ČESKÉ VYSOKÉ
UČENÍ TECHNICKÉ
V PRAZE

FAKULTA
BIOMEDICÍNSKÉHO
INŽENÝRSTVÍ

DISERTAČNÍ PRÁCE 2024

LUKÁŠ
MIKLAS

České vysoké učení technické v Praze
Fakulta biomedicínského inženýrství

Katedra zdravotnických oborů a ochrany obyvatelstva

BEZPEČNOST HOSPITALIZOVANÝCH CHRÁNĚNÝCH OSOB

Disertační práce

PhDr. Lukáš MIKLAS, MBA

Kladno, *září, 2024*

Doktorský studijní program: *P1032D020001 Civilní nouzová připravenost*

Školitel: ***doc. JUDr. Jan KOLOUCH, Ph.D.***
Školitel specialista: ***doc. PhDr. Barbora Vegrichtová, Ph.D., MBA***

Czech Technical University in Prague
Faculty of Biomedical Engineering

Department of Health Sciences and Population Protection

THE SAFETY OF HOSPITALISED PROTECTED PERSONS

Doctoral Thesis

PhDr. Lukáš MIKLAS, MBA

Kladno, *September, 2024*

Ph.D. Programme: *P1032D020001 Civil Emergency Preparedness*

Supervisor: ***doc. JUDr. Jan KOLOUCH, Ph.D.***

Supervisor-Specialist: ***doc. PhDr. Barbora Vegrichtová, Ph.D., MBA***

PROHLÁŠENÍ

Prohlašuji, že jsem disertační práci s názvem *Bezpečnost hospitalizovaných chráněných osob* vypracoval samostatně pouze s použitím pramenů, které uvádím v seznamu použitých pramenů.

Nemám závažný důvod proti užití tohoto školního díla ve smyslu § 60 zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů.

V Kladně dne 30. 9. 2024 .....…….

PhDr. Lukáš Miklas, MBA

PODĚKOVÁNÍ

Rád bych tímto vyjádřil své hluboké poděkování vedoucímu své disertační práce, doc. JUDr. Janu Kolouchovi, Ph.D., za jeho neustálou podporu, cenné rady a konzultace, které mi poskytoval po celou dobu mého studia. Jeho odborné vedení, ochota a motivace mi byly neocenitelnou oporou při zpracovávání této práce. Děkuji také doc. PhDr. Barboře Vegrichtové, Ph.D., MBA, za cenné rady a podporu, které mi poskytovala v prvních třech letech mého studia.

Dále děkuji všem neformálním konzultantům, kteří mi pomohli rozkrývat taje vědy a poskytovali mi cenné vhledy a rady. Mé největší poděkování patří mé rodině za jejich neustálou podporu, trpělivost a pochopení, a to i v časech, kdy má práce vyžadovala jejich oběti. Bez jejich důvěry a obrovské podpory by tato práce nevznikla. V neposlední řadě děkuji svým blízkým, kteří mě provázejí životem a poskytují mi oporu ve všech mých snahách.

ABSTRAKT

Disertační práce se komplexně zabývá problematikou poskytování zdravotní péče chráněným osobám, se zaměřením na fyzickou a kybernetickou bezpečnost ve zdravotnických zařízeních v České republice. Hlavním cílem práce je, na základě empirických dat a poznatků, důkladně identifikovat klíčová riziková místa v oblasti bezpečnosti a ochrany osobních a zdravotních informací chráněných osob během jejich hospitalizace, přenosu a zpracování. Cílem je formulovat konkrétní a prakticky využitelná doporučení, která přispějí k posílení ochrany citlivých údajů a zvýšení úrovně zabezpečení informací ve zdravotnických zařízeních. Tato opatření mají být v souladu s nejlepšími mezinárodními standardy a implementovatelná v českém zdravotnickém systému.

V rámci práce jsou využívány kvalitativní a kvantitativní výzkumné metody. Kvalitativní část zahrnuje hloubkové rozhovory s odborníky v oblasti zdravotnictví a bezpečnosti, zatímco kvantitativní část se opírá o dotazníková šetření mezi pracovníky ve zdravotnictví a chráněnými osobami. Součástí výzkumu je také analýza existujících bezpečnostních protokolů ve zdravotnických zařízeních a jejich efektivity, přičemž zvláštní pozornost je věnována aplikaci cloudových technologií a vybraných moderních technologií pro bezpečný přenos a uchovávání zdravotních informací. Cílem této analýzy je identifikovat hlavní technologické výzvy a navrhnout modely a bezpečnostní opatření, které zajistí lepší ochranu osobních údajů.

Tato práce se zabývá také legislativním rámcem ochrany osobních údajů ve zdravotnictví, přičemž se zaměřuje na etické a právní aspekty, které ovlivňují sdílení informací o zdravotním stavu chráněných osob vůči veřejnosti. Zároveň rozebírá specifika péče o chráněné osoby, včetně těch, které vyžadují zvláštní fyzickou a virtuální bezpečnost v souvislosti s jejich ochranou.

Další významná část práce se věnuje analýze přenosu zdravotních informací prostřednictvím cloudových řešení, která představují nové technologické výzvy. Práce navrhuje konkrétní technická opatření, která zahrnují zavedení robustních bezpečnostních protokolů, aby se zabránilo neoprávněnému přístupu a zneužití informací. Navržené modely a doporučení pro praxi zahrnují kombinaci existujících technologií s vývojem autonomních systémů specifických pro potřeby jednotlivých států. Výsledky výzkumu rovněž ukazují, že zavedení standardizovaných bezpečnostních opatření, spolu s posílením vzdělávání zdravotnického

personálu v oblasti ochrany informací, může významně přispět ke zvýšení bezpečnosti a kvality péče o chráněné osoby.

Závěry práce poskytují doporučení pro zavedení jednotných standardů ochrany osobních údajů chráněných osob, jak na úrovni technologií, tak legislativy. Tato doporučení mohou být klíčová pro zajištění dlouhodobé ochrany zdravotních informací ve zdravotnických zařízeních v České republice. Práce tak přispívá nejen k lepšímu porozumění této problematiky, ale i k posílení důvěry veřejnosti v bezpečnost zdravotní péče.

KLÍČOVÁ SLOVA: Bezpečnost dat * Ochrana osobních údajů * Zdravotnická zařízení * Kybernetická bezpečnost * Chráněné osoby * Přenos dat * VIP pacient * Virtuální hospitalizace

ABSTRACT

This dissertation comprehensively addresses the issue of healthcare provision for protected persons, with a focus on physical and cyber security in healthcare facilities in the Czech Republic. The main objective of the work is to thoroughly identify key risk areas in the security and protection of personal and health data of protected persons during their hospitalization, transmission, and processing, based on empirical data and findings. The aim is to formulate concrete and practically applicable recommendations that will contribute to strengthening the protection of sensitive information and enhancing data security in healthcare facilities. These measures are intended to align with the best international standards and be implementable within the Czech healthcare system.

The work employs both qualitative and quantitative research methods. The qualitative part includes in-depth interviews with experts in healthcare and security, while the quantitative part is based on surveys conducted among healthcare workers and protected persons. The research also involves analyzing existing security protocols in healthcare facilities and their effectiveness, with special attention given to the application of cloud technologies and selected modern technologies for the secure transmission and storage of health data. The goal of this analysis is to identify the main technological challenges and propose models and security measures that will ensure better protection of personal data.

This dissertation also addresses the legislative framework for data protection in healthcare, focusing on the ethical and legal aspects that influence the sharing of information about the health status of protected persons with the public. It further examines the specifics of care for protected persons, including those requiring special physical and virtual security in connection with their protection.

Another significant part of the work is devoted to analyzing the transmission of health data through cloud solutions, which present new technological challenges. The dissertation proposes specific technical measures, including the implementation of robust security protocols to prevent unauthorized access and misuse of data. The proposed models combine existing technologies with the development of autonomous systems specific to the needs of individual countries. The research results also indicate that the implementation of standardized security measures, along with enhanced education for healthcare personnel in data protection, can significantly contribute to improving the security and quality of care for protected persons.

The conclusions of the dissertation provide recommendations for the introduction of unified standards for the protection of personal data of protected persons, both at the technological and legislative levels. These recommendations may be crucial for ensuring the long-term protection of health information in healthcare facilities in the Czech Republic. The work contributes not only to a better understanding of this issue but also to strengthening public confidence in the security of healthcare services.

KEYWORDS: Data security * Personal data protection * Healthcare facilities * Cybersecurity * Protected individuals * Data transfer * Data processing * VIP Patient * Virtual hospitalisation

Obsah

Úvod do problematiky

Bezpečnost ve zdravotnických zařízeních představuje komplexní výzvu, která zahrnuje jak fyzickou ochranu pacientů, personálu a návštěvníků, tak zabezpečení citlivých osobních a zdravotních informací. Zejména s rostoucí digitalizací zdravotnických systémů a využíváním různých služeb navázaných na zdravotnická zařízení se zvyšuje riziko ztráty či poškození dat, a to jak z nedbalosti, tak zejména úmyslně (např. pomocí kybernetického útoku). Výše uvedené významně ohrožuje integritu a důvěrnost těchto informací.

Cílem této disertační práce je identifikovat klíčová rizika v oblasti bezpečnosti a ochrany informací při hospitalizaci **chráněných osob**[1] během jejich přenosu a zpracování ve zdravotnických zařízeních v České republice. Na základě získaných informací budou formulována konkrétní doporučení, která mohou pomoci se zvýšením úrovně bezpečnosti a ochrany citlivých informací chráněných osob, a to jak v souladu s národními, tak mezinárodními standardy.

Současné globální události, jako je válka na Ukrajině a teroristické útoky v Izraeli, zdůrazňují nutnost efektivních bezpečnostních opatření, která chrání jak fyzickou, tak kybernetickou integritu zdravotnických zařízení a zejména pak chráněných osob. Tyto konflikty ukazují na potřebu rychlé a spolehlivé výměny informací v krizových situacích a na důležitost zabezpečení informací chráněných osob, které mohou být zneužity pro strategické nebo politické účely. Bezpečnostní výzkumy v řadě zemí se proto mimo jiné zaměřují i na pokročilé bezpečnostní technologie, jako je šifrování, biometrická autentizace a geolokační údaje, které zajišťují bezpečný přenos a uchování informací i v těch nejnáročnějších podmínkách.

Obsah této disertační práce je rozdělen primárně na část **teoretickou a výzkumnou**. **Teoretická část** se zaměřuje na systém zdravotní péče a specifika poskytování služeb chráněným osobám. Zabývá se nejen právními a etickými aspekty poskytování zdravotní péče, ale také aktuálními trendy v oblasti fyzické a virtuální bezpečnosti těchto osob. Důležitým tématem je vymezení právního rámce poskytování zdravotní péče chráněným osobám, včetně rozboru právní ochrany těchto osob[2], které vyžadují specifický přístup v oblasti bezpečnosti a zachování jejich práv na ochranu osobních údajů. Tato část analyzuje způsoby, jak jsou

[1] Definice pojmu *chráněné osoby* viz kapitola 2.3.5

[2] V práci je též uváděn pojem *VIP pacient* a *VIP návštěva.* Blíže viz kapitola 2.3

aplikována fyzická i virtuální bezpečnostní opatření ve zdravotnických zařízeních a jaké trendy a inovace jsou využívány v oblasti hospitalizace chráněných osob.

Významná část práce se zaměřuje na přenos zdravotních informací chráněných osob, což představuje, zejména s ohledem na narůstající kybernetické hrozby a požadavky na ochranu osobních údajů, stále větší výzvu. Práce se v této části zabývá i možným využitím cloudových technologií a prvků *Internet of Things*[3] pro bezpečný přenos a uchovávání přenášených dat a informací. V této souvislosti se rozebírá také otázka, zda by státy měly vyvíjet vlastní autonomní systémy pro zajištění ještě vyšší úrovně bezpečnosti. Klíčovou výzvou je nastavení účinných bezpečnostních protokolů, aby byla zaručena bezpečnost informací, a zároveň byla zajištěna flexibilita a rychlost v poskytování akutní zdravotní péče.

Dále se práce věnuje otázce legitimnosti a rozsahu sdílení informací o zdravotním stavu chráněných osob vůči veřejnosti, což je téma, které se týká jak právní, tak etické roviny. Práce podrobně rozebírá specifika poskytování zdravotní péče chráněným osobám s ohledem na ochranu jejich soukromí a bezpečnost jak fyzickou, tak virtuální.

Významnou součástí teoretické části je analýza právních a etických aspektů ochrany osobních údajů ve zdravotnictví. Tato část se zaměřuje na formulaci interních právních předpisů a regulací, které mají za úkol chránit osobní údaje pacientů, aniž by narušovaly efektivitu zdravotnických zařízení. V kontextu dříve popsaných hrozeb, se zde rozebírá proces hledání rovnováhy mezi ochranou informací a zajištěním kvalitní zdravotní péče pro chráněné osoby i běžné pacienty.

Druhá část práce je zaměřena na výzkum, který se zabývá analýzou současných přístupů k procesu zpracování a přenosu dat chráněných osob. V této části jsou představeny metody kvalitativního a kvantitativního výzkumu, které sloužily k identifikaci slabin a nedostatků v současných postupech. Výzkum definuje klíčové oblasti, jako jsou metody sběru a analýzy dat, a poskytuje konkrétní návrhy opatření ke zlepšení bezpečnosti a kvality poskytované

[3] Dále jen „IoT“ (Internet of Things, překlad autora: Internet věcí), je vědecky definován jako síť fyzických objektů (věcí) vybavených senzory, softwarovými aplikacemi a dalšími technologiemi, které jsou propojeny prostřednictvím internetu, a umožňují tak sběr a výměnu dat s jinými zařízeními a systémy. Tyto objekty mohou být cokoli od běžných spotřebičů a průmyslových zařízení po nositelnou elektroniku a chytrou infrastrukturu. IoT integruje digitální a fyzický svět, umožňuje automatizaci, monitorování a optimalizaci procesů a poskytuje reálná data pro analýzy a rozhodování.[265]

zdravotní péče chráněným osobám. Tato část práce také zahrnuje vytvoření modelů pro zvýšení ochrany pacientských informací, zejména v oblasti virtuální hospitalizace a přenosu informací.

Výzkumná část zahrnuje i interpretaci kvalitativních a kvantitativních dat, která byla shromážděna v rámci dotazníkových šetření mezi pracovníky ve zdravotnictví a samotnými chráněnými osobami. Tyto analýzy přinášejí nové poznatky o vnímání bezpečnosti péče chráněných osob a přenosu citlivých informací v reálných podmínkách, včetně specifických výzev při péči o tyto osoby, a to jak z fyzického, tak kybernetického hlediska.

Autor disertační práce se věnuje jednomu hlavnímu tématu, přičemž toto téma rozpracovává z pohledu několika klíčových aspektů. Primární důraz je kladen na virtuální bezpečnost, tedy ochranu citlivých zdravotních dat a informací chráněných osob během jejich přenosu a zpracování. Vedle toho se práce zaměřuje také na principy poskytování zdravotní péče a jejich fyzickou bezpečnost. V praktické části jsou představena konkrétní doporučení a postupy využitelné v praxi, včetně modelu zabezpečení zdravotních dat chráněných osob, který reflektuje specifické výzvy vyplývající ze zkušeností z konfliktů na Ukrajině a v Izraeli. Autor provedl i rozsáhlou rešerši odborné literatury a dalších zdrojů, aby identifikoval aktuální klíčové trendy a výzvy v oblasti ochrany chráněných osob, které jsou následně podrobně analyzovány v teoretické části práce. Všechny popsané oblasti se v práci logicky prolínají a jsou finálně rozpracovány v rámci diskuse v jejím závěru, která obsahuje zásadní výstupy a přínosy využitelné v praxi, jež zohledňují nejmodernější technologie a trendy v oblasti kybernetické i fyzické bezpečnosti ve zdravotní péči.

1 Řešená problematika disertační práce

1.1 Motivace a bližší popis řešené problematiky

Komplexní pohled na bezpečnostní opatření zdravotnických zařízení v České republice zahrnuje celou řadu oblastí, které je pro optimální zajištění bezpečnosti personálu, pacientů a návštěvníků nezbytné zabezpečit. Vzhledem k enormnímu rozsahu těchto opatření, diferentním podmínkám jednotlivých zdravotnických zařízení, nejednotnosti pohledu na jejich implementaci a jejich turbulentnímu vývoji, není možné všechny výše uvedené oblasti a bezpečností opatření v rámci jedné disertační práce postihnout.

Zejména vzhledem ke skutečnosti, že autor práce je služebně zařazen v rámci Ústřední vojenské nemocnice – Vojenské fakultní nemocnice Praha[4], která se, mimo jiné, specializuje na poskytování zdravotní péče příslušníkům ozbrojených sil, bezpečnostních sborů a ústavních činitelů[1], **je disertační práce zacílena na procesy a vazby vybraných skupin bezpečnostních opatření týkajících se chráněných osob.**

Hospitalizace chráněných osob vyžaduje zvýšenou úroveň zabezpečení nejen z hlediska fyzické ochrany, ale i ochrany kybernetické. Zdravotnická zařízení by měla být vybavena moderními technologiemi a zejména postupy, které umožňují efektivní ochranu informací před neoprávněným přístupem, kybernetickými útoky, ale i fyzickým únikem informací. Tento úkol je komplikován rozdílnými podmínkami v jednotlivých zdravotnických zařízeních a nejednotnými přístupy k implementaci bezpečnostních opatření.

Zajištění bezpečnosti informací pacientů ve zdravotnických zařízeních je v současné době zásadním prvkem bezpečnostních systémů. Tento problém nabývá na významu zejména v případě hospitalizace chráněných osob, jako jsou političtí představitelé, celebrity, svědci ve svědecké ochraně nebo členové ozbrojených sil a bezpečnostních složek. Chráněné osoby tvoří specifickou skupinu pacientů, u nichž mají osobní a zdravotní informace vysokou hodnotu a jejichž ochrana vyžaduje zvláštní přístup.

Práce se zabývá rozborem technických, organizačních a právních aspektů bezpečnosti a ochrany informací při hospitalizaci chráněných osob ve zdravotnických zařízeních vybraného typu.

---

[4] Dále jen „ÚVN“.

Při hospitalizaci chráněných osob se obvykle uplatňují, mimo standardní bezpečnostní opatření, také bezpečnostní opatření dodatečná či specifická. Tato opatření mají za cíl zajistit bezpečnost a soukromí zmíněných osob. Přesná opatření se však opět mohou lišit v závislosti na zdravotnickém zařízení, zemi, situaci a stupni ohrožení aj. Primárně je z pohledu fyzické bezpečnosti třeba chránit místo, kde je takovýto pacient hospitalizován. Konkrétně se může jednat o zajištění pomocí zvýšené fyzické ochrany, například pomocí bezpečnostních strážců, monitorovacích systémů, kamer či přístupových omezení. Stejně tak se vyžaduje omezený přístup, který může být přísně kontrolován, k hospitalizované chráněné osobě. V mnoha případech dochází ke vzniku týmu pro zajištění bezpečnosti chráněné osoby. Ve zvláštních případech mohou být přítomni zkušení bezpečnostní experti nebo členové výkonných složek státu pro zajištění bezpečnosti chráněné osoby. Mohou spolupracovat s personálem zdravotnického zařízení a pomáhat s ochranou chráněné osoby. Rovněž jsou přijímána opatření směřující k zajištění určité míry soukromí a důvěrnosti chráněných osob, včetně zajištění jejich kybernetické bezpečnosti. To zahrnuje zejména dodatečné zabezpečení osobních informací chráněné osoby a omezení přístupu k nim.

Popsaná situace vede zdravotnická zařízení zabývající se hospitalizací chráněných osob k tvorbě vnitřní dokumentace, metodik a postupů pro optimální zvládání případné hospitalizace tohoto druhu pacientů. Lze doporučit, aby zdravotnické zařízení mělo vytvořené samostatné vnitřní postupy, metodiky či obecně vnitřní předpisy pro řešení možných nouzových situací, jako jsou případné útoky, hrozby nebo únik informací. Přesná bezpečnostní opatření a postupy se mohou lišit v závislosti na konkrétních okolnostech a požadavcích dané bezpečnostní situace.

Dalším aspektem je sdílení pacientských informací chráněných osob, zejména příslušníků ozbrojených sil a bezpečnostních sborů. V kontextu současných vojenských operací a dynamicky se vyvíjejících konfliktů, kde je evakuace zraněných komplikovaná, je nezbytné okamžitě přenášet zdravotní data zraněných do zdravotnických zařízení vyšší úrovně péče. Tento proces by měl být zajištěn prostřednictvím moderních technologií, které umožňují sledování zdravotního stavu pacienta na dálku, poskytování rady první pomoci a přípravu na přijetí pacienta do zdravotnického zařízení. Významnou roli v tomto procesu hraje telemedicína, virtuální konsilia, včetně tzv. virtuální hospitalizace, které má potenciál zajišťovat kontinuitu péče od okamžiku zranění až po kompletní zotavení pacienta. To vše přináší nové požadavky na přenos, sdílení a zejména zabezpečení pacientských dat chráněných

osob, na které musí poskytovatelé zdravotních služeb efektivně reagovat, neboť hrozba úniku zdravotních dat může mít zásadní vliv na další vývoj konfliktu.

Výsledky předložené disertační práce mohou významně přispět k zajištění vyšší úrovně bezpečnosti a ochrany citlivých informací ve zdravotnických zařízeních. Implementace navržených opatření může nejen zvýšit bezpečnost hospitalizovaných chráněných osob, ale také posílit důvěru veřejnosti ve zdravotnická zařízení a jejich schopnost efektivně chránit informace o pacientech. Navíc mohou výsledky této práce sloužit jako základ pro tvorbu centrální metodiky a jednotných postupů v oblasti ochrany zdravotnických informací.

Autor práce byl a stále je v rámci své funkce zodpovědný za koordinaci bezpečnostních opatření týkajících se hospitalizace chráněných osob, což mu umožnilo získat řadu cenných praktických zkušeností. Tyto zkušenosti zároveň odhalily mnoho problémů, jejichž řešení vyžaduje hlubší vědecké zkoumání této specifické oblasti. Motivací pro volbu tématu disertační práce byla zejména nutnost reagovat na zmíněné problémy a navrhnout konkrétní postupy a opatření pro optimalizaci hospitalizace chráněných osob, ať už fyzicky nebo virtuálně, v rámci poskytování zdravotních služeb, se zvláštním důrazem na bezpečnost zdravotních dat a ochranu osobních údajů.

Je třeba uvést, že autor je striktním zastáncem demokratických principů a zejména rovnosti všech lidí. Ačkoliv se v práci se objevují pojmy jako „společensky významný“, „VIP“ atd., je tyto třeba v kontextu práce vnímat pouze jako označení vybrané skupiny osob či vlastnosti přiznané na základě různých kritérií (právními předpisy, popularitou, veřejným míněním aj.). V žádném z ohledů nelze legitimizovat určité výsostné postavení některé ze skupin osob, kterým je poskytována zdravotní péče, ba právě naopak, s pojmy „VIP“ a „VIP pacient“ pracuje autor v kontextu bezpečnosti a ustanovení zdravotního práva a rovněž podrobuje kritice vybrané instituty poskytování zdravotní péče z hlediska požadavku na jejich rovné a nediskriminační aplikování všem osobám bez rozdílů.[5]

[5] Blíže viz kap. 2.3.

1.2 Cíle práce

Hlavním cílem disertační práce je na základě získaných empirických dat a poznatků identifikovat klíčová rizika v oblasti bezpečnosti a ochrany osobních a zdravotních dat a informací při hospitalizaci chráněných osob během jejich přenosu a zpracování ve zdravotnických zařízeních v České republice. Na základě této analýzy bude práce směřovat k formulaci konkrétních a prakticky využitelných doporučení, která přispějí k posílení ochrany citlivých údajů a zvýšení úrovně zabezpečení informací v těchto zařízeních. Cílem práce je také zajistit, aby navržená opatření byla v souladu s mezinárodními standardy, a aby mohla být efektivně implementována v rámci českého zdravotnického systému.

Uvedené cíle zahrnují komplexní analýzu současného stavu fyzické i kybernetické bezpečnosti, identifikaci nejčastějších slabých míst a specifických rizik, zhodnocení existujících technických a organizačních opatření a návrh efektivních řešení pro zlepšení bezpečnostních postupů a ochrany dat chráněných osob. Výstupy disertační práce by měly přispět ke zvýšení bezpečnosti a kvality péče o chráněné osoby a poskytnout doporučení pro zdravotnická zařízení, která se mohou stát základem pro tvorbu centrální metodiky a jednotných postupů v oblasti kybernetické bezpečnosti.

Uvedených cílů práce by autor práce chtěl dosáhnout, mimo jiné, i díky realizovaným zahraničním stážím, získaným zkušenostem od vybraných zahraničních poskytovatelů zdravotních služeb a zkušenostem získaným v rámci jeho aktuálního služebního zařazení.

Přínosem práce pak může být i její případné využití poskytovateli zdravotních služeb, ale také širokou akademickou, odbornou i laickou veřejností. Díky výzkumné části práce lze předpokládat i možný vznik několika dalších odborných příspěvků týkajících se tématu práce, včetně pokusu o vytvoření metodických doporučení pro poskytovatele zdravotních služeb fakultního typu.

K naplnění primárního cíle práce bude zapotřebí učinit řadu postupných kroků. Došlo proto ke stanovení následujících dílčích cílů:

Prvním dílčím cílem disertační práce bude provedení analýzy širokého spektra odborných pramenů týkajících se sféry bezpečnosti zdravotnických zařízení se zaměřením na hospitalizace chráněných osob. Současná teorie poznání v oblasti práva a managementu zdravotnických zařízení je natolik široká, že pro potřeby práce a tvorbu vlastních tvůrčích východisek bude

zapotřebí sestavit rozsáhlou platformu vycházející z dostupných odborných pramenů. Částečným pozitivním limitem pro tento dílčí cíl práce je skutečnost, že většina pramenů je zahraničních.

- Význam prvního dílčího cíle:

Splnění uvedeného cíle bude zásadní pro vytvoření logické struktury různých teoretických a právních vnímání otázek hospitalizace chráněných osob. Dále jeho splněním bude možné zaujmout vlastní hodnotící postoje, jež budou promítány do jednotlivých teoretických postupů a východisek realizovaných v rámci výzkumné části práce. V neposlední řadě bude poté možné zmíněným cílem přispět k rozvoji oblasti zdravotního práva jako takové.

Druhým dílčím cílem disertační práce bude identifikace problémových míst zpracování osobních údajů chráněných osob včetně navržení opatření a postupů pro zvýšení jejich bezpečnosti v rámci hospitalizace chráněných osob.

- Význam druhého dílčího cíle:

Komplexní zaměření práce umožní rovněž rozbor jednotlivých organizačních, technických a právních aspektů bezpečnosti a ochrany informací, které je možné realizovat v prostředí vybraného poskytovatele zdravotních služeb. Budou analyzovány právní, technické a organizační aspekty ochrany dat a kybernetické bezpečnosti v kontextu jejich správné aplikace. Tato analýza zahrne také specifika postupů zdravotnických zařízení a jejich spolupráci s dalšími subjekty za účelem zefektivnění ochrany citlivých informací chráněných osob. Zejména pak ryze právní pohled na ochranu subjektu osobních údajů bude velkým přínosem, neboť zkoumaným subjektem bude pacient se statutem chráněné osoby.

Problematika bezpečnosti a ochrany dat a informací při hospitalizaci chráněných osob je dosud teoreticky málo popsaná. Zejména zmíněný výzkumný problém je značně otevřený a neprobádaný. V ČR do současné doby neexistuje jednotný pohled na danou problematiku včetně centrální metodiky či stanovených postupů ve vztahu k ochraně dat a informací o chráněných osobách při jejich hospitalizaci. V této oblasti proto lze spatřovat významný potenciál pro vědecké a výzkumné úsilí této disertační práce.

Lze předpokládat, že zmíněný dílčí výzkumný cíl může být přínosný pro praxi také z hlediska samotných dílčích závěrů plynoucích z použitých vědecko-výzkumných postupů, ale

i samotných metod. Rovněž může přispět k odhalení příčin problémových míst v oblasti fyzické a kybernetické bezpečnosti a ochrany informací a k jejich samotné identifikaci.

Samotné poznatky získané v rámci plnění zmíněného dílčího cíle práce lze prezentovat vybraným zdravotnickým zařízením za účelem zkvalitnění jejich činnosti v oblasti hospitalizace chráněných osob a jejich ochrany. Zmíněné poznatky mohou být využity pro jejich činnosti spojené s nastavováním interních procesů a jejich optimalizací v oblasti ochrany dat, informací a kybernetické bezpečnosti.

Třetím dílčím cílem je navržení konkrétních opatření a postupů pro poskytování zdravotní péče chráněným osobám v rámci jejich hospitalizace, s důrazem na identifikaci specifik a odlišností oproti běžným pacientům, včetně řešení otázky fyzické bezpečnosti. Tento cíl se zaměřuje na analýzu, jak status chráněných osob ovlivňuje běžně nastavené zdravotnické procesy a organizační struktury ve zdravotnických zařízeních, a jak lze optimalizovat poskytování péče tak, aby bylo efektivní a zároveň zajišťovalo bezpečnost těchto pacientů a současně nenarušilo poskytování běžné zdravotní péče.

- Význam třetího dílčího cíle:

Poskytování zdravotní péče chráněným osobám přináší řadu výzev, které se liší od péče o běžné pacienty, zejména v kontextu zajištění soukromí, prioritizace péče a zvýšené bezpečnosti. Tento cíl umožní podrobné zkoumání, jak přítomnost chráněných osob ovlivňuje provozní procesy a pracovní prostředí ve zdravotnických zařízeních. Význam tohoto cíle spočívá v návrhu opatření, která by usnadnila integraci specifických potřeb chráněných osob do každodenního provozu zdravotnických zařízení, aniž by došlo ke zhoršení péče pro ostatní pacienty. Analýza zahrne také aspekty fyzické bezpečnosti, které jsou s poskytováním péče těmto osobám neoddělitelně spojeny, a navrhne protokoly pro zajištění jejich ochrany v různých scénářích. Výsledky mohou přispět k formulaci politik a postupů, které zajistí efektivní a bezpečnou péči o chráněné osoby, aniž by to nepříznivě ovlivnilo celkovou kvalitu zdravotní péče v českých zdravotnických zařízeních.

Čtvrtým dílčím cílem disertační práce bude vytvoření práce, která může být využita jako podklad či inspirace pro další vědecko-výzkumné bádaní samotného autora práce, širokou kurii studentskou, ale také pro ostatní akademickou a odbornou veřejnost, především pro samotná zdravotnická zařízení a výzkumníky zabývající se bezpečností zdravotnických zařízení.

- Význam čtvrtého dílčího cíle:

Autor při zpracování disertační práce bude postupovat v souladu s potřebami participace při řešení vědecko-výzkumných projektů Fakulty biomedicínského inženýrství Českého vysokého učení technického v Praze, ale také v souladu s potřebami praxe zdravotnických zařízení. Výstupy této práce budou poskytnuty pro jejich další využití jak samotným studentům a akademickým pracovníkům zabývajícím se oblastí bezpečnosti zdravotnických zařízení a zdravotním právem, tak samotným zdravotnickým zařízením, včetně Ministerstva zdravotnictví a Ministerstva obrany, na které je problematika této disertační práce zaměřena. Dále pak v případě zjištění nedostatků na ně poukázat, aby mohlo dojít k navržení efektivních opatření k jejich odstranění.

1.3 Výzkumné problémy a hypotézy

Hospitalizace chráněných osob je proces, který vyžaduje zvýšenou úroveň zabezpečení nejen z hlediska fyzické ochrany, ale zejména ochrany jejich pacientských dat. Zdravotnická zařízení musí být vybavena moderními technologiemi a postupy, které umožňují efektivní ochranu dat a informací před neoprávněným přístupem, kybernetickými útoky a únikem informací. Tento úkol je komplikován rozdílnými podmínkami v jednotlivých zdravotnických zařízeních, nejednotností přístupů k implementaci opatření a jejich turbulentním vývojem.

V současné době se zdravotnická zařízení v České republice potýkají s řadou výzev v oblasti fyzické a kybernetické bezpečnosti. Tyto výzvy zahrnují nejen technické aspekty, jako je zabezpečení vybraných prostor, IT infrastruktury, ale také organizační a právní aspekty. Specifická rizika spojená s hospitalizací chráněných osob zahrnují zejména cílené kybernetické útoky zaměřené na získání citlivých informací ze strany Ruska, Číny nebo teroristických organizací, které mohou být zneužity pro různé účely, včetně vydírání, špionáže nebo veřejné diskreditace.[2, 266]

Výzkumy ukazují, že současný systém zdravotnictví často není dostatečně připraven čelit novým hrozbám v oblasti fyzické a virtuální bezpečnosti pacientů se statutem chráněné osoby. Analýzy a studie zaměřené na připravenost zdravotnických systémů na různé mimořádné situace, včetně pandemických hrozeb a válečných konfliktů, odhalují významné mezery, které je třeba řešit. Tyto problémy zahrnují nedostatečnou připravenost na krizové situace, omezené schopnosti systému absorbovat šoky, nedostatečnou komunikaci a koordinaci mezi

zdravotnickými zařízeními a nedostatek standardizovaných postupů pro ochranu citlivých informací.[3]

Pokud jde o přístup k pacientům se statutem chráněné osoby, výzkumy potvrzují, že tito pacienti vyžadují specifická bezpečnostní opatření, která se liší od běžných pacientů. Tento rozdílný přístup je nezbytný k zajištění jejich bezpečnosti a ochraně osobních údajů.[4]

Na základě výše uvedeného, zejména pak v části bližší řešené problematiky a po zkušenostech autora práce s hospitalizací několika prezidentů, včetně kontextu válek na Ukrajině a Izraeli byly na počátku vyřčeny dvě výzkumné otázky:

1. **Je současný systém zdravotnictví připraven čelit novým hrozbám v oblasti fyzické a zejména virtuální bezpečnosti pacientů se statutem chráněné osoby?**
2. **Je k pacientům se statutem chráněné osoby přistupováno stejně jako k pacientům bez tohoto statusu?**

Na obě otázky zní odpověď ne, což je doloženo mnohými výzkumy[3, 4]. S ohledem na služební zařazení autora pak logicky následovala další výzkumná otázka:

3. **Jakým konkrétním způsobem se uvedené otázky projevují v praxi poskytovatelů zdravotních služeb ve vztahu ke všem skupinám chráněných osob?**

Uvedené problematické oblasti jsou předmětem zájmu autora práce, díky čemuž je možné pro kvalitativní a kvantitativní část výzkumu vymezit následující výzkumné problémy a pracovní hypotézy:

Výzkumný problém č. 1: **Jaká jsou nejčastější slabá místa a specifická rizika v oblasti bezpečnosti pacientských dat anebo informací o chráněných osobách při jejich fyzické anebo virtuální hospitalizaci?**

Lze předpokládat, že nejčastější slabá místa a specifická rizika v oblasti bezpečnosti pacientských dat anebo informací o chráněných osobách při jejich fyzické nebo virtuální hospitalizaci jsou způsobena nedostatečnou implementací moderních bezpečnostních technologií a postupů. Tato slabá místa mohou vést k narušení soukromí a bezpečnosti pacientů, což může mít vážné důsledky pro jejich zdraví a bezpečnost. Slabá místa mohou zahrnovat nedostatečné šifrování informací, neaktuální bezpečnostní software nebo špatně definované bezpečnostní politiky. Identifikace a analýza těchto rizik bude prováděna prostřednictvím

rozhovorů s odborníky a dotazníkových šetření mezi zdravotnickým personálem a bezpečnostními experty.

Hypotéza č. 1: Nejčastější slabá místa v oblasti bezpečnosti pacientských dat anebo informací při hospitalizaci chráněných osob jsou způsobena nedostatečnou implementací aktuálních bezpečnostních technologií a postupů.

Ověření této hypotézy bude založeno na kombinaci kvalitativní a kvantitativní analýzy aktuálních bezpečnostních opatření a technologií používaných ve zdravotnických zařízeních. Tento přístup zahrnuje provedení rozhovorů s odborníky v oblasti kybernetické bezpečnosti, zdravotnictví a dotazníkových šetření mezi zdravotnickým personálem a bezpečnostními experty. Identifikace hlavních slabin a rizik umožní navrhnout účinná řešení pro jejich minimalizaci a zlepšení celkové úrovně bezpečnosti pacientských dat a informací o nich. Tento výzkum povede k vypracování doporučení, která budou zahrnovat implementaci moderních bezpečnostních technologií a postupů, zajištění pravidelné aktualizace bezpečnostního softwaru a posílení šifrování informací.

Výzkumný problém č. 2: **Jaká jsou specifická rizika virtuální bezpečnosti pacientů se statutem chráněné osoby ve srovnání s běžnými pacienty?**

Pacienti se statutem chráněné osoby, jako jsou političtí činitelé, celebrity, příslušníci ozbrojených sil nebo bezpečnostních sborů, čelí specifickým rizikům kvůli vysoké hodnotě a citlivosti jejich osobních a zdravotních dat. Tato rizika zahrnují cílené fyzické, ale i kybernetické útoky, které se zaměřují na získání nebo zneužití jejich informací za účelem vydírání, špionáže nebo veřejné diskreditace. Analýza těchto specifických rizik bude prováděna prostřednictvím komparativní analýzy rizikových faktorů získaných prostřednictvím rozhovorů s odborníky a dotazníkových šetření mezi zdravotnickým personálem a bezpečnostními experty z různých zdravotnických zařízen v rámci celého světa.

Hypotéza č. 2: Pacienti se statutem chráněné osoby čelí vyššímu riziku zneužití jejich osobních údajů anebo zdravotních dat ve srovnání s běžnými pacienty, zejména kvůli jejich zvýšené hodnotě.

Tato hypotéza bude testována prostřednictvím analýzy dat slabých míst bezpečnostních systémů poskytovatelů zdravotních služeb a srovnáním míry a závažnosti útoků na chráněné osoby a běžné pacienty. Výsledky této analýzy pomohou vytvořit specifické bezpečnostní protokoly a doporučení pro ochranu citlivých informací o chráněných osobách. Identifikace

těchto rizik a návrh opatření umožní posílit bezpečnostní systémy a snížit pravděpodobnost úspěšných kybernetických útoků na tuto zranitelnou skupinu pacientů.

Výzkumný problém č. 3: Jaká technická a organizační opatření jsou aktuálně implementována pro ochranu citlivých informací o pacientech se statutem chráněné osoby ve vybraných zdravotnických zařízeních při jejich hospitalizaci nebo vyšetření?

Cílem tohoto problému je zjistit, jaká technická a organizační opatření jsou již implementována a jak efektivní jsou tato opatření při ochraně citlivých informací chráněných osob. Důkladná analýza těchto opatření umožní identifikovat mezery a navrhnout vylepšení. Analýza bude zahrnovat hodnocení informací o bezpečnostních opatřeních (např. šifrovacích metod, přístupových kontrol, pravidel pro uchovávání informací a bezpečnostních politik) získaných na základě rozhovorů s odborníky a dotazníkových šetření mezi zdravotnickým personálem a bezpečnostními experty z různých zdravotnických zařízen v rámci celého světa.

Hypotéza č. 3: Technická a organizační opatření aktuálně implementovaná ve zdravotnických zařízeních nejsou dostatečná k efektivní ochraně citlivých informací o pacientech se statutem chráněné osoby.

Tato hypotéza bude testována prostřednictvím detailního zhodnocení současných bezpečnostních opatření, včetně technických řešení a organizačních procesů, aby se zjistilo, zda splňují požadované standardy ochrany dat. Identifikace nedostatků a návrh konkrétních zlepšení budou klíčovými výstupy této analýzy.

Dílčí shrnutí

Komplexní pohled na bezpečnostní opatření zdravotnických zařízení v České republice zahrnuje technické, organizační a právní aspekty ochrany informací při hospitalizaci chráněných osob. Výzkumné otázky a hypotézy této práce se zaměřují na identifikaci slabých míst a rizik v oblasti bezpečnosti pacientských dat chráněných osob, hodnocení současných opatření a analýzu vlivu nedostatečné bezpečnosti na kvalitu a bezpečnost péče. Výstupy disertační práce by měly přispět ke zvýšení bezpečnosti a kvality péče o chráněné osoby a poskytnout doporučení pro zdravotnická zařízení, chráněné osoby i zaměstnance zdravotnických zařízení, která se mohou stát základem pro tvorbu centrální metodiky a jednotných postupů v oblasti bezpečnosti pacientských dat a informací o nich samotných.

1.4 Metody vědecké práce

Pro úspěšné dosažení cílů disertační práce je zásadní přesné vymezení a implementace metodologických východisek a přístupů. Věda jako disciplína představuje komplexní myšlenkový proces, který je založen na metodologii, teorii a systému utříděných poznatků. Realizuje se prostřednictvím různých, vzájemně propojených aktivit, jejichž cílem je popis a vysvětlení zákonitostí specifických jevů. Vědu lze chápat jako rozvětvenou síť tvořivých a komunikujících osobností, podporovanou strukturovanými institucemi, kde se systematický výzkum provádí v souladu s poznávacími potřebami vědy a jejími aplikačními požadavky. Tento přístup je přirozeně doplněn různými koncepty jednotlivých vědních oborů.

Každá vědecká disciplína má svůj vlastní teoretický systém, který je dále členěn do teoretických subsystémů s různou úrovní obecnosti. Tyto subsystémy lze podle daného přístupu efektivněji kategorizovat. Základním stavebním prvkem těchto systémů a subsystémů je tzv. teoretický výrok. Teoretický výrok slouží vědě jako elementární jednotka, z níž vycházejí různé teorie, ať už jednoduché nebo složité. Pojem teorie se používá pro označení vědeckých myšlenkových konstrukcí na všech úrovních. Teorie, které zkoumá obecná metodologie, mohou být rozděleny do čtyř hlavních skupin:

1) *Analytické teorie*, do kterých spadají především matematické a logické myšlenkové systémy, které nemají přímý vztah k reálnému světu. Tyto systémy jsou tvořeny souborem axiomatických výroků, jež jsou pravdivé na základě definice a z nichž jsou ostatní výroky deduktivně odvozeny. Mezi pravdivé definice patří například Euklidova věta, Archimédův zákon či Ludolfovo číslo.[5]
2) *Normativní teorie* se zaměřují na formulování idejí o žádoucích stavech pozorovatelné reality, stanovují konečná uspořádání a definují ideální stavy. Tyto teorie následně popisují pozorované jevy v kontextu těchto ideálních stavů a hodnotí je podle několika kritérií. Tento typ teorií tvoří základ vědních oborů, jako je estetika, etika a další.[6]
3) *Metateorie* jsou teorie, které vznikají při zkoumání, analýze a popisu samotných teorií. Můžeme je také chápat jako filozofický základ dané teorie. Metateorie představují soubor základních myšlenek o tom, jak nahlížet a zkoumat určité jevy v konkrétní oblasti zájmu. Tento termín se nepoužívá příliš často, ale nejčastěji se s ním setkáváme v humanitních a přírodovědných oborech.[7]

4) *Vědecké teorie*, které v užším slova smyslu zahrnují teorie, které se vytvářejí na základě pravidel obecné vědecké metodologie v jejím základním stavu. Obecná vědecká metodologie byla primárně vyvinuta jako nástroj pro rozvoj přírodních věd, na které je také nejlépe aplikovatelná.[8, 9]

Pojem metodologie je sám o sobě značně komplexní a bývá různě interpretován. Etymologicky je termín „metodologie“ odvozen ze dvou řeckých slov: *„methodos“* (způsob, cesta) a *„logos“* (učení, věda, slovo). Metodologie obecně představuje teorii metod, tedy nauku o metodách, které lze využívat při tvorbě vědecké práce. Zahrnuje studium metod a vědeckých postupů, které představují selekci výzkumných metod a postup, jak tyto metody používat při vědeckém bádání. Je teorií zaměřenou na výběr výzkumných metod a poskytuje návod, jak vybrané metody aplikovat ve vědeckém zkoumání.[10]

V širším smyslu se metodologie vědy neboli nauka o metodách zabývá nejen samotnými metodami, ale i procesy a principy jejich aplikace. To zahrnuje analýzu jednotlivých vědeckých metod na základě jejich využití, což směřuje k dosažení specifických vědeckých a teoretických cílů. Metodologie je tedy souhrnem metod určité vědy a představuje teorii metod, která je v širším pojetí ekvivalentní s teorií vědy. Důležitým aspektem metodologie je způsob, jakým dochází k rozboru jednotlivých vědeckých metod, což vede k optimalizaci jejich využití v rámci vědeckého výzkumu.[11]

Na pojem metodologie lze v současné době nahlížet ve třech úrovních:

1) *V nejširším pojetí:* Metodologie vědy jako takové, neboli věda o vědě, se zabývá obecnými principy a metodami, které jsou aplikovány napříč různými vědními obory. Tento přístup se zaměřuje na pochopení a analýzu vědeckých procesů jako celku.
2) *V užším pojetí:* Metodologie konkrétního vědního oboru nebo skupiny věd. Toto pojetí zahrnuje speciální metodologie, například metodologii managementu, metodologii psychologie atd. Každá z těchto metodologií se zaměřuje na specifické metody a postupy, které jsou relevantní pro daný obor.
3) *V nejužším pojetí:* Metodologie jako věda o metodách vědeckého poznání. Tento přístup se soustředí na konkrétní metody, které jsou používány při získávání vědeckých poznatků, a zahrnuje jejich analýzu, hodnocení a aplikaci.[11]

Mezi jednotlivými skupinami existují vzájemné obecné či konkrétní vztahy a vazby vyplývající z jejich společné provázanosti a měření.

Metodou rozumíme nástroj ke zkoumání daného výzkumného předmětu. Jedná se o způsob a aplikaci postupu tak, aby bylo možné dosáhnout zvolený výzkumný cíl. Samotné použití metody při vědeckém zkoumání ovšem podmiňuje znalost postupu využití metody. Tento postup má rysy záměrnosti (vztahuje se k výzkumnému cíli) a systematičnosti (metoda je uplatňovaná v rámci teoreticky zdůvodněného postupu). Jednotlivá východiska pro zdůvodnění postupu dává metodologie. Zmíněná metodologie má tedy klíčovou úlohu pro zaměření vědeckého zkoumání a pro volbu vědecko-výzkumných metod.[12, 13]

Metoda obecně je způsob, jak dosáhnout stanoveného cíle, systematický postup uplatňovaný při poznávání předmětu zkoumání, který má určitý teoretický základ. Obecnými metodami jsou například: analogie, analýza, dedukce, experiment, indukce, pozorování, syntéza. Metoda je tedy systém určitých vědeckých pravidel a postupů umožňujících získávání poznatků.

Metoda představuje systematický postup určitého konání směřující do konkrétního cíle. Metodou tedy rozumíme:

1) určitý uspořádaný operační postup nebo systém,
2) systém pravidel určujících třídu operačních systémů,
3) postup nebo způsob, kterým se lze z konkrétního výchozího místa dospět k plánovanému stavu.[14]

V disertační práci je pracováno rovněž s **metodikou**. Metodika nepatří do oblasti metodologie. Metodikou výzkumné práce rozumíme postup (návod, „recept“), jak v praxi postupně realizovat výzkumné procedury vztahující se k realizaci výzkumného cíle. Metodika je soubor doporučených a vybraných metod a postupů sloužících k úspěšnému řešení stanovených cílů výzkumné práce.[14]

Technika je poté, dle pojetí autora práce, určitý konkrétní způsob, kterým probíhá například sběr dat. Jedná se o propracované a sofistikované postupy specifických operací směřujících k získání empirických informací v rámci daného výzkumu. Mezi významné a rovněž známé techniky sběru dat patří například dotazník, rozhovor či pozorování.

Výzkum je obecnější způsob zkoumání s určitým vyšším stupněm představy o zkoumaném jevu a s konkrétními vědeckými cíli. Jedná se o pomůcku, díky které je možné odhalit širší souvislosti. Jedná se o úmyslné systematické jednání či činnost využívající určité techniky sběru dat. V uvedeném konceptu je vhodné začlenit rovněž pojem průzkum, který na rozdíl od výzkumu neobsahuje vědecké cíle. Průzkum je zaměřen na řešení daného úkolu a poté na

bezprostřední aplikaci získaných poznatků.

Kromě výše uvedených termínů je nutné dále pojednat o možnosti stanovení kvality a relevance určitého výzkumu, který byl v daném čase realizován. Zmíněnou kvalitu a relevanci je možné prověřit z hlediska dvou základních kritérií – validity a reliability.

Validita je jiný výraz pro pravdivost. Při výzkumu zejména v psychologii, sociologii a dalších společenských vědách (stejně jako při statistickém hodnocení technologických procesů, například dodržení standardů kvality služeb) je velmi důležité zkoumat validitu neboli platnost získaných výsledků vzhledem ke skutečnosti. Samotný proces zajištění validity se nazývá validace. Kvalitativní anebo nezávislá kvantitativní validace je důležitá zejména tam, kde zkoumaný jev nelze úplně oddělit od dalších vlivů a kde je interpretace výsledků složitá. Validace se používá při kvantitativním i kvalitativním výzkumu a existují také různé postupy jejího vyčíslení.[12]

Validita tedy primárně vyjadřuje požadavek relevance mezi předem stanoveným cílem výzkumu a skutečně dosaženými výsledky. Lze konstatovat, že je-li výzkum validní, znamená to, že skutečně měří to, co měřit má. V rámci provádění výzkumu a činností, které s provedením výzkumu bezprostředně souvisí, je třeba postupovat tak, aby uvedené činnosti a výzkum byly co nejvíce validní. Je totiž velmi podstatné, aby výsledky uvedeného bádání co nejvíce odpovídaly skutečné realitě.[15]

Výzkum není validní, jestliže se v rámci daného procesu hovoří jen o několika exemplárních případech, nejsou poskytnuta kritéria nebo důvody pro zařazení určitých případů na úkor jiných a v neposlední řadě rovněž proto, že není k dispozici materiál v původní podobě, jak byl předložen na začátku výzkumu.

Absolutní validity je velmi obtížné dosáhnout, ba dokonce je otázkou, zdali je skutečně možné jí vůbec dosáhnout. Existuje však několik způsobů, jak je možné validitu v rámci výzkumu ověřit:

1) validita je založená na členství v určité známé skupině (testován je nástroj na skupině, o níž víme, že má vlastnost, kterou má nástroj mířit),
2) prediktivní validita (pro replikační výzkum porovnává předpověď založenou na testovaném míření se skutečnými výsledky),
3) souběžná validita (dochází k použití dvou a více postupů pro míření téže vlastnosti),
4) validita založená na mínění skupiny soudců (shoda výroků mezi soudci),

5) zjevná validita (intuitivně spoléháme na to, že existuje dostatečná spojitost mezi zkoumaným jevem a naším měřením).[16]

V daném kontextu je ovšem nutné podotknout, že validita jako taková se vždy vztahuje ke konkrétní sféře či oblasti, z čehož vyplývá, že s takovou oblastí či sférou úzce souvisí. Není proto většinou možné, aby došlo k obecné aplikaci validity i na jiné oblasti, nežli ty, které primárně postihuje. Proto je zapotřebí vždy postupovat v určité metodologické kontinuitě ve vztahu k ověření validity.

Míra validity zodpovídá, zda dochází skutečně ke zkoumání toho, co má býti zkoumáno, a je jedním z předpokladů objektivity. Dalším předpokladem objektivity výzkumu v sociálních vědách je rovněž níže zmíněná **reliabilita**, která odpovídá na otázku, jak přesné je toto zkoumání. Reliabilita je proto logicky podmínkou validity. Může existovat reliabilní, ale nevalidní test, avšak test s nízkou reliabilitou validní být nemůže. Podle Helmstadera dokonce platí, že maximální možná validita se rovná odmocnině z reliability.[17]

Reliabilita vyjadřuje opakovatelnost se stejnými výsledky. O reliabilním výzkumu hovoříme tehdy, když můžeme zaznamenat stupeň shody, s jakou různí pozorovatelé nebo ten samý pozorovatel v rozdílných situacích případy zařadí do té samé kategorie. Jedná se o vlastní požadavek na formální přesnost měřícího nástroje použitého v daném empirickém výzkumu. Velmi důležitou otázkou jsou poté samotné výsledky výzkumu či měření v primární linii, které ovlivňují různé chyby jako např. přítomnost nebo nepřítomnost pozorovatele, vliv okolí, osobní rozpoložení výzkumníků, změna instrukcí k testu atd. Zmíněná spolehlivost, stálost neboli reliabilita nástroje pro dané měření je pro výzkumníka nesmírně důležitá. Je pro něj zárukou, že variabilita v jeho datech neboli proměnné výsledky míření různých objektů, není způsobena špatným měřicím prostředkem, nýbrž skutečnou variabilitou intenzity mířené vlastnosti.[18]

Mezi validitou a reliabilitou vzniká určitá forma závislosti, kdy validní nástroj zahrnuje i reliabilitu. To znamená, že jestliže lze o nějakém nástroji tvrdit, že je validní, je poté i spolehlivý. Naopak to z logiky věci neplatí. Pokud je vědecký nástroj spolehlivý, samotné měření nemusí být vždy validní.[14]

Pod pojmem reliabilita rozumíme přesnost a spolehlivost výzkumného nástroje. Každý výzkumný nástroj může být do určité míry přesný a spolehlivý, ale žádný nástroj nedosahuje dokonalé přesnosti a spolehlivosti. Při jeho použití se projevují určité vlastnosti, které jeho reliabilitu snižují. Úlohou výzkumníka je získat nebo vytvořit nástroj s co nejvyšší možnou

mírou reliability. To je jednou ze záruk, že jeho výsledky budou následně hodnotné a dobře interpretovatelné.

V teorii je možné se setkat se třemi základními faktory, které ovlivňují reliabilitu:

1) **Rozsah výzkumného nástroje (počet položek).**
   Delší výzkumné nástroje obvykle vykazují vyšší spolehlivost než kratší. To je dáno tím, že respondenti v delším dotazníku dostanou více příležitostí k odpovědi, což vede k přesnějším výsledkům. Náhoda zde hraje menší roli, než by tomu bylo u kratších nástrojů. Dlouhé výzkumy zpravidla přinášejí větší variabilitu výsledků, což pozitivně ovlivňuje celkovou spolehlivost měření.
2) **Homogenita výzkumného nástroje.**
   Homogenita znamená sourodost nástroje. Nástroj musí měřit jednu vlastnost a položky nástroje si musí být svým obsahem blízké. Pokud například test obsahuje úlohy týkající se oblasti „A“ a oblasti „B“, nejde o homogenní test, protože měří dvě odlišné oblasti. Proto bude jeho reliabilita nízká.
3) **Obtížnost otázek či úloh výzkumného nástroje.**
   U vědomostních testů, testů schopností atd., jestliže je test velmi lehký, skóre v rámci skupiny bude mít nízkou variabilitu a test bude mít rovněž nízkou reliabilitu. Velmi těžký test však může způsobit, že respondenti odpovědi neznají a budou je hádat nebo si je vymýšlet. To způsobí náhodné chyby, čímž se reliabilita sníží.[19]

1.4.1 Logické vědecké metody práce

V rámci teoretické části disertační práce byly použity vědecké metody označované jako metody **logické.** Jednotlivé logické metody se vzájemně doplňují a překrývají, čímž v konečném důsledku dochází k synergickému efektu ve vztahu k vědeckému bádání.

Mezi zmíněné metody patří:

1) **Analýza – syntéza**

Vědecké metody jako jsou analýza a syntéza jsou obecné vědecké metody, bez kterých se neobejde žádný vědecký výzkum. Proto se tyto metody používají ve všech etapách a na všech stupních řešení daného vědeckého problému.

Analýza (z řeckého *analysis* – rozbor, uvolnění) je základní metodou poznávání objektů, jevů a procesů, kterou se poznávaný objekt rozkládá (dekomponuje) na jeho jednotlivé části

(prvky, znaky, složky apod.) a zjišťují se vzájemné vztahy (souvislosti) mezi nimi, dále mezi částmi a celkem, mezi celkem a okolím, mezi celky, které jsou ve vzájemném vztahu atp. Analýza umožňuje poznání podstatných rysů zkoumaného jevu, odkrytí jeho struktury a vztahů. Základní operace: rozložení na komponenty, jejich rozlišení, uspořádání, kombinace, tvoření tříd, zjištění vztahů, interpretace výsledků. Po analýze následuje syntéza, umožňující vytvoření závěrů. Podle zaměření můžeme a. členit na faktorovou, interakční, textovou, obsahovou, strukturální, významovou, vztahovou apod.[20]

Analýzu lze vnímat jako určité myšlenkové a metodické rozčlenění zkoumaného objektu na jeho jednotlivé části. Mohou to být konkrétní aspekty, roviny, vrstvy, vazby a podobně. Do této úrovně vnímání lze zakomponovat proces spočívající v aplikaci oblastí specifických pro každé výše uvedené rozčlenění a rovněž uplatnění postupů či metod, které umožňují vždy v daném kontextu vyslovit specifickou dílčí charakteristiku zkoumané části.

Spolu s tím se analýza zabývá také vztahy mezi zmíněným vymezováním i jednotlivými částmi. Hledání společného významu částí navzájem je však již obratem od analýzy k syntéze. Produktem analýzy je popis skutečnosti, syntéza podává její vysvětlení. Při analýze jednotlivá fakta konstatujeme, syntézou docházíme k jejich pochopení.[21]

Syntéza je proces nebo myšlenkový postup skládání jednotlivých částí do celku. Na rozdíl od analýzy, při které se postupuje od celku k částem, syntéza umožňuje poznávat zkoumaný předmět či systém jako jediný celek. Syntéza tvoří základní platformu pro tvorbu správných rozhodnutí. Vědeckou metodu syntézy můžeme charakterizovat jako proces zjišťování souvislostí mezi vyčleněnými prvky, znaky, protiklady a jejich propojení a následnou reprodukci zkoumané události s jejich podstatnými znaky a vztahy. Syntéza umožňuje sledovat vztahy mezi fakty, charakter vzájemných souvislostí mezi nimi, odhalovat příčiny konkrétních jevů, funkční závislost vybraných prvků, návaznost jednotlivých etap či tendenci vývoje zkoumaného vědeckého jevu.[16]

Analýzu a syntézu lze tedy označit jako protichůdně orientované metody využívané při výzkumu určitého problému. Analýza směřuje od celku k části, kdežto syntéza naopak od jednotlivé části ke konečnému celku. Syntéza tvoří spolu s analýzou primární myšlenkové pochody při odhalování nových vztahů a zákonitostí.[22]

2) Indukce – dedukce

Indukce (lat. *in-ducere* – vyvozovat) je proces logického vyvozování obecného závěru na

základě poznatků a úsudku o jednotlivostech. Indukce je úsudek směřující od zvláštních případů k obecné poučce. Je myšlenkovým postupem od konkrétního, daného k abstraktnímu, zobecňujícímu. Napomáhá formulovat všeobecně platná pravidla, principy či zákonitosti. V konečném důsledku umožňuje využít dostupné informace k vytvoření vědeckých teorií – induktivní závěry překračují informaci získanou v původních datech. Induktivní závěr lze považovat za hypotézu, protože nabízí vysvětlení, i když těchto vysvětlení může být v praxi více. Tato hypotéza je přijatelná, jestliže nám vysvětlí, proč daný jev nastal.[21]

Závěry induktivních myšlenkových pochodů jsou vždy doprovázeny kontinuitou se subjektivními postoji vědce či osoby, která danou metodu aplikuje (zkušenostmi, znalostmi), a lze na ně tedy nahlížet pouze s omezenou platností. Indukce se zaměřuje jen na ověření toho, zda sledovaný jev dopadne tak, jak je předpokládáno. Výsledek konečné pravděpodobnosti určitého případu nelze odvozovat od pravděpodobnosti dílčího jevu.

Reichenbach zastává názor, že samotný induktivní postup nevede ke spolehlivému výsledku. Velmi silným nástrojem je naopak vytvoření vzájemně propojené sestavy induktivních procesů, které jsou zařazeny v rámci určitého vědního oboru. Uvedené pojetí znamená, že jedna indukce koriguje jinou indukci.[23]

Indukce jako taková se ověřuje dedukcí.

Dedukce je způsob vyvozování nových, logicky opodstatněných závěrů na základě již obecných, známých tvrzení či předpokladů. Dedukcí vyvozené závěry bývají méně známé, zvláštní či nové, nežli tomu bylo před použitím dedukce. Nejedná se pouze o pravděpodobné závěry. Spolu s indukcí patří dedukce mezi základní myšlenkové pochody při odhalování nových zákonitostí a vztahů. Dedukce má své zásadní místo v oblasti vědy a výzkumu, při zkoumání zákonitostí a testování obecných hypotéz. Dedukce je nápomocná při celé řadě metod v řízení rizik, řízení kvality či řízení bezpečnosti, neboť samotné vyšetřování skutečností je založeno mnohdy na deduktivním přístupu. Pomocí dedukce je možné testovat, jestli vyslovená hypotéza je schopna objasnit zkoumanou skutečnost, zda má obecnou platnost. Jedná se o jeden z článků myšlenkového řetězce, a je tedy zapotřebí ji používat zároveň s jinými typy myšlení nebo vyvozování.[24]

Deduktivně lze postupovat od obecného k obecnému nebo od jedinečného k jedinečnému, vždy v určité rovině obecnosti. Deduktivní přístup vychází z pozitivismu, kdy nejprve na

základě teorie formuluje hypotézy a poté za pomoci logického uvažování a již známých faktů testuje uvedenou hypotézu. K tomu využívá především kvantitativní data, která lze získat různými způsoby. Deduktivní přístup bývá často realizován průzkumem pro odhalování kauzálních vztahů mezi jednotlivými proměnnými.

Dedukce je proces myšlení, při kterém od obecných závěrů, tvrzení a soudů přecházíme k méně známým či zvláštním. Vycházíme tedy ze známých, ověřených a obecně platných závěrů a aplikujeme je na jednotlivé dosud neprozkoumané případy. Dedukce je jeden z procesů, díky kterému můžeme vysvětlit, zda testovaná hypotéza může skutečně vysvětlit daný jev. Bohužel lze konstatovat, že imponující nezvratnost deduktivních důkazů je však dosahována za cenu toho, že většinou nic nevypovídají o reálném světě. Proto má dedukce význam jen jako článek určitého myšlenkového řetězce, ve kterém lze uplatnit i jiné typy myšlení.[21]

3) Abdukce

Abdukce je vedle indukce a dedukce dalším typem úsudků. Jde o takový typ úsudků, při nichž se vytváří hypotézy pro pozorované jevy. Při tom jde většinou o redukci z několika možných vysvětlení. Tento typ abdukce je většinou nazván selektivní abdukcí. Vedle selektivní abdukce je známa také kreativní abdukce, která vytváří možná vysvětlení.

Jak při selektivní, tak i při kreativní abdukci však dochází k různým typům úsudkových zkreslení, která ne vždy umožňují vytvářet oprávněnou domněnku nebo hypotézu. V zásadě lze říci, že abdukce je založena na modelech, které lze rozdělit na modely zahrnující smyslové aktivity (např. analogická vizuální úvaha) a na modely, které mají idealizační formu (např. myšlenkový experiment). Magnani o tom referuje a Thagard tuto myšlenku zpřesňuje tím, že hovoří o schématech nebo o scénářích, z nichž pochází vysvětlení faktů. V obou případech je však nutné vyhnout se zatížení mysli.[25]

4) Abstrakce a konkretizace

Abstrakce je vnímána jako jakýsi myšlenkový proces našeho vědomí, v jehož rámci se z různých dílčích objektů vyčleňují jen určité specifické charakteristiky, díky čemuž se v našem vědomí vytváří určitý model konkrétní věci či objektu. Taková představa poté obsahuje jen takové znaky či rysy, jejichž zkoumání a vnímání samotné umožňuje získávat odpovědi na konkrétní otázky v rámci našeho vědomí.[26]

Často využívanou vědeckou metodou ve společenském i technickém prostředí je metoda abstrakce. Tuto metodu lze blíže charakterizovat jako myšlenkové odlučování určitých vlastností, souvislostí a vztahů, které ztěžují pronikání do zkoumaného problému. Danou frázi lze přetlumočit tak, že každý zkoumaný problém má nekonečné množství znaků, souvislostí a vztahů a při zkoumání konkrétního procesu se ponechávají mnohotvárné podrobnosti, které vzhledem k stanovenému cíli nepřinášejí podstatné informace. K poznání konkrétního jevu je potřebné ho studovat krok za krokem, jednu stránku za druhou a dočasně ponechávat stranou ostatní stránky.[27]

Je tedy logické, že naše vědomí si vytváří samo jen takový model objektu, který mu díky určitým charakteristikám či objektům klademe k posouzení. Abstrakce tedy umožňuje zobecnění neboli přechod od konkrétní myšlenky k obecnějšímu, které sice vykazuje méně znaků, ale tyto znaky jsou společné.

Za protikladnou metodu abstrakce lze označit metodu zevšeobecňování, která je charakterizována myšlenkovým přechodem od jedinečného ke všeobecnému pomocí zjednodušení údajů na základě jednoho nebo více shodných znaků. Základem takové metody je všeobecnost souvislostí reálných předmětů a jevů, vzájemná souvislost jedinečného a všeobecného ve všech reálně existujících oblastech či událostech.[21]

Konkretizace je myšlenkový postup od všeobecného k jednotlivému, tj. od skupiny k jejím jednotlivým fragmentům. Při konkretizaci se vyhledává konkrétní výskyt určitého objektu z určité utříděné množiny objektů, na který je následně zapotřebí aplikovat charakteristiky platné pro celou takovou skupinu objektů.[28]

Ve výzkumné části disertační práce byly použity uvedené metody kvalitativního a kvantitativního výzkumu, které jsou blíže uvedeny v kapitole 3.3 této práce.

1.5 Metodologie a metodika disertační práce

Výzkum prezentovaný v disertační práci bude realizován v několika fázích s cílem získat komplexní pohled na zkoumanou problematiku. Vlastní výzkum je rozčleněn do následujících fází a v této části prezentuje základní rámec výběru vzorků a sběru dat:

- **Fáze 1: Kvalitativní výzkum prostřednictvím polostrukturovaných rozhovorů**
    - **Účel:** Získání detailních a hlubokých poznatků od expertů v oblasti zdravotnictví, fyzické a kybernetické bezpečnosti.

- **Metoda:** Polostrukturované rozhovory analyzované pomocí interpretativní fenomenologické analýzy (dále jen „IPA“) s lékaři, IT specialisty a manažery.
- **Výstup:** Kvalitativní data, která poskytnou základ pro identifikaci klíčových témat a problémových míst bezpečnosti chráněných osob.

- **Fáze 2: Kvantitativní výzkum formou dotazníkového šetření**
  - **Účel:** Shromáždit rozsáhlé a reprezentativní údaje od zaměstnanců zdravotnických zařízení a chráněných osob („VIP pacientů“).
  - **Metoda:** Strukturované dotazníky distribuované mezi zaměstnance zdravotnických zařízení (lékaře, sestry, administrativní pracovníky, vedoucí atd.) v rámci České republiky, celého světa a mezi chráněné osoby („VIP pacienty“) v rámci České republiky.
  - **Výstup:** Kvantitativní data, která umožní statistickou analýzu a identifikaci vztahů mezi různými proměnnými včetně komparace se zahraničními přístupy.
- **Fáze 3: Sestavení aktuálního stavu a analýza sekundárních dat**
  - **Účel:** Získání širšího kontextu a doplnění primárních dat.
  - **Metoda:** Přezkum legislativních dokumentů, interních předpisů a bezpečnostních protokolů/standardů ve zdravotnických zařízeních.
  - **Výstup:** Sekundární data, která pomohou identifikovat nesrovnalosti a mezery v aktuálních opatřeních a sestavit aktuální stav kybernetické bezpečnosti ve zdravotnických zařízeních.
- **Fáze 4: Analýza a interpretace dat**
  - **Kvalitativní analýza:** Analýza rozhovorů za účelem identifikace klíčových témat a problémových míst. Získaná data budou vyhodnocena pomocí kvalitativní obsahové analýzy.
  - **Kvantitativní analýza:** Statistická analýza dotazníkových dat pro určení četnosti a vztahů mezi různými proměnnými včetně zapojení kvalitativní obsahové analýzy a komparace se zahraničím.

- **Sekundární analýza:** Přezkoumání a syntéza legislativních a interních dokumentů, aby byly identifikovány nesrovnalosti a mezery v aktuálních opatřeních.

- **Fáze 5: Vývoj návrhů, modelů a doporučení pro praxi**

  Na základě analýzy dat budou vypracovány konkrétní návrhy a doporučení pro zlepšení poskytování zdravotní péče a zvýšení fyzické a kybernetické bezpečnosti, včetně ochrany osobních a zdravotních dat chráněných osob během jejich hospitalizace nebo vyšetření ve zdravotnických zařízeních. Tyto návrhy budou zahrnovat:

  - **Technická opatření:** Doporučení pro implementaci moderních bezpečnostních technologií a nástrojů, které zajistí ochranu dat a zabrání neoprávněnému přístupu.
  - **Organizační opatření:** Návrhy na efektivní tvorbu a aktualizaci vnitřních postupů a metodik, které zahrnují specifické procesy zaměřené na zvýšení ochrany dat a bezpečnosti chráněných osob, s důrazem na interoperabilitu s existujícími systémy.
  - **Právní aspekty:** Doporučení pro legislativní úpravy, které zajistí soulad s ochranou osobních údajů a dalšími relevantními předpisy, s cílem vytvořit jednotný rámec pro obecně poskytování zdravotní péče chráněných osob ve zdravotnických zařízeních.

- **Fáze 6: Validace a implementace**

  Doporučení budou konzultována s odborníky a nabídnuta k testování do pilotních projektů ve vybraných zdravotnických zařízeních. Výsledky pilotních projektů budou analyzovány a případně zapracovány do finálních doporučení.

Pro dosažení jednotlivých cílů disertační práce bylo zapotřebí provést následující kroky:

1) formulace problému,
2) stanovení cílů disertační práce,
3) stanovení hypotéz,
4) literární rešerše,

5) sběr dat,
6) zpracování dat,
7) interpretace a shrnutí poznatků získaných sběrem dat,
8) formulace doporučení a tvorba modelů,
9) vyvození závěrů včetně dosažení cílů práce,
10) vyvrácení či potvrzení hypotéz.

V rámci disertační práce, a to zejména její praktické části, se autor zaměřil na empirický výzkum, jehož cílem bude stanovit postupy a opatření pro realizaci optimální hospitalizace chráněné osoby v podmínkách vybraného poskytovatele zdravotních služeb, včetně navržení konkrétních legislativních změn. Nedílnou součástí praktické části je také její provázanost s teoretickými základy představenými v teoretické části práce. Ta poslouží zejména jako teoretický základ, ze kterého bude následně čerpáno pro analýzu získaných dat a jejich komparaci, jakožto dat osvětlujících skutečnou praxi s teoretickým základem.

Na základě zaměření tématu práce její autor dospěl k závěru, že pro účely výzkumu se jako nejlepší jeví kombinace kvalitativních a kvantitativních výzkumných metod, a to hned z několika důvodů. Za prvé, cílem praktické části této práce nebude vytvořit relevantní data využitelné pro statistické účely, případně statistiku ohledně podmínek hospitalizace chráněných osob, ale definovat konkrétní opatření a postupy zjištěné, mimo jiné, komparací mezi praxí a právem *de lege lata*, případně porovnat praxi jednotlivých subjektů. V tomto případě by tedy ryze kvantitativní výzkum nemohl přinést kýžené výsledky, byť by data získaná jeho prostřednictvím mohla být pro účely této či jiné práce zajímavá. Kvalitativní výzkum s prvky výzkumu kvantitativního však pro účely této práce přinese informace, které bude možné dále zpracovat, vyhodnotit konkrétní postupy jednotlivých subjektů a následně navrhnout odpovídající opatření a postupy týkající se hospitalizace chráněných osob.

To se v kontextu provedeného výzkumu projeví například ve skutečnosti, že soulad praxe a platného práva (tzv. „*compliance*“) nebude do hloubky zjišťován u jediného subjektu, ale místo toho dojde k ověření souladu s platným právem u většího množství subjektů způsobem, který umožní zobecnění získaných výsledků.

V rámci výzkumu autor práce využije kombinaci dotazníkového průzkumu a uzavřených polostrukturovaných rozhovorů se zaměstnanci zdravotnických zařízení, kteří mají praktickou

zkušenost s hospitalizací chráněných osob („VIP pacientů“). Dotazníkové šetření i rozhovory budou upraveny pro specifické individuální potřeby výzkumu. Dotazníkové šetření bude zaměřeno rovněž na ostatní zdravotnické zaměstnance z celého světa a také na samotné chráněné osoby v rámci České republiky.

Získaná data budou následně vyhodnocena pomocí obecně teoretických explanačních metod (analýza, syntéza, indukce, dedukce, srovnání, analogie). Tento komplexní přístup a analýza získaných dat umožní v konečném důsledku splnění stanoveného cíle.

1.6 Očekávaná omezení

Při tvorbě disertační práce se autor setká s řadou omezení, která budou vyžadovat specifické řešení v obou hlavních oblastech, teoretické i praktické. Jedním z hlavních omezení v teoretické části je rozsáhlost tématu kybernetické bezpečnosti ve zdravotnických zařízeních. Oblast kybernetické bezpečnosti se neustále vyvíjí, což způsobuje rychlé změny v přístupech a technologiích. Autor si je vědom toho, že nelze pokrýt všechny aspekty této problematiky do hloubky. Proto bude nutné se zaměřit na vybrané klíčové oblasti, které jsou relevantní pro zdravotnická zařízení v České republice, se zvláštním důrazem na ochranu dat chráněných osob. Další omezení spočívá ve specifické odborné náročnosti zdrojů, především těch zahraničních, které bude nutné překládat. Překlad odborných textů může vést k nepřesnostem, které mohou ovlivnit správné pochopení a interpretaci klíčových pojmů. Aby se minimalizovalo riziko chyb, autor plánuje konzultovat sporné termíny s odborníky v dané oblasti.

Hlavní praktické omezení disertační práce je identifikováno v oblasti neochoty některých zdravotnických zařízení a jejich statutárních orgánů spolupracovat při realizaci výzkumu s konkurenčními zdravotnickými zařízeními. Získání potřebných informací může být komplikované, zejména pokud jde o citlivé informace týkající se fyzické a kybernetické bezpečnosti a ochrany osobních údajů. Toto omezení bude vyžadovat strategický přístup ke sběru dat, včetně využití anonymizovaných dotazníků a případných osobních konzultací s odborníky. Dalším významným omezením je specifická povaha kvalitativního výzkumu, který bude použit k definování hlavních bezpečnostních rizik a doporučení. Kvalitativní výzkum je časově náročný a vyžaduje pečlivé plánování a provádění, aby byly získané výsledky co nejpřesnější a nejrelevantnější pro následnou kvantitativní analýzu.

V rámci výzkumné části práce bude jedním z hlavních omezení zajištění vysoké úrovně bezpečnosti a důvěrnosti získaných dat. Při práci s citlivými informacemi o chráněných osobách

je nezbytné dodržovat přísné bezpečnostní protokoly, aby nedošlo k úniku informací. Tento aspekt bude vyžadovat pečlivé plánování a implementaci technických a organizačních opatření. Další omezení se týká samotné definice hrozeb a jejich prevence ve zdravotnických zařízeních. Zejména kybernetické hrozby jsou dynamické a neustále se vyvíjejí, což znamená, že doporučení a opatření musí být flexibilní a schopné rychle reagovat na nové typy hrozeb.

Mezi možná omezení výzkumu lze zařadit i možnou neochotu zahraničních zdravotnických zařízení spolupracovat na výzkumu pocházejícím z jiného státu. Různá zdravotnická zařízení mohou mít odlišné bezpečnostní protokoly a kulturu ochrany dat, což může vést k obtížím při získávání přístupu k relevantním informacím a datům. Nedostatek spolupráce ze strany zahraničních institucí může omezit rozsah a generalizovatelnost výzkumných závěrů, což by mohlo ovlivnit celkovou validitu studie.

Kromě toho, plánované použití platformy Google formulářů pro sběr dat může představovat další výzvu, jelikož tato platforma není ve všech zdravotnických zařízeních vnímána jako bezpečná a může vyvolat obavy týkající se ochrany osobních údajů. Některá zdravotnická zařízení mohou mít přísné interní politiky, které zakazují používání externích online nástrojů pro sběr citlivých informací, což by mohlo omezit míru participace respondentů a tím i objem a kvalitu získaných dat. Tato omezení si vyžádají dodatečné úsilí při navrhování alternativních metod sběru dat, které budou respektovat bezpečnostní požadavky jednotlivých zařízení. Jako alternativa byla zvažována platforma Survio, i tato je však vnímána jako externí online nástroj představující potencionální riziko pro zdravotnické zařízení.

Autor si uvědomuje, že omezení spojená s touto disertační prací jsou značná a budou vyžadovat pečlivý a systematický přístup. Přes všechna tato omezení je cílem vytvořit hodnotnou a prakticky využitelnou práci, která přispěje k lepší ochraně osobních údajů a zajištění kybernetické bezpečnosti ve zdravotnických zařízeních v České republice. Uvedené postupy a konkrétní způsoby řešení budou detailně rozpracovány v rámci jednotlivých kapitol této disertační práce.

2 Současný stav řešené problematiky a její teoretické souvislosti

V rámci poskytování zdravotní péče chráněným osobám může docházet k vyvolání střetu několika odvětví práva v závislosti na konkrétních okolnostech a specifických situacích. Právo na soukromí a ochranu osobních údajů chráněné osoby často vyžadují zvýšenou ochranu. Zdravotnické zařízení musí dodržovat příslušné zákony a předpisy týkající se ochrany soukromí a správy osobních údajů, jako je například Nařízení EU 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)[6], či zákon č. 110/2019 Sb., o zpracování osobních údajů, ve znění pozdějších předpisů[7], aby zajistilo, že informace o pacientech jsou řádně chráněny. Zároveň má zdravotnický personál povinnost poskytovat péči v souladu s nejvyššími standardy etiky a dbát na zájmy pacienta.[29] V případě chráněných osob mohou být vynaloženy dodatečné opatření na zajištění jejich bezpečnosti, důvěrnosti a komfortu, a to v souladu s etickými směrnicemi a předpisy.

Rovněž mají dle GDPR chráněné osoby také právo na svobodu projevu a na informovaný souhlas se zdravotní péčí. Je důležité zajistit, aby tato práva nebyla narušena a že chráněné osoby mají možnost vyjádřit svou vůli a rozhodovat o svém lékařském ošetření. V případě osob, které jsou vystaveny vysokému stupni bezpečnostního ohrožení, může dojít ke střetu s právem na bezpečnost a ochranou její bezpečnosti[8]. Zdravotnické zařízení musí najít rovnováhu mezi poskytováním nezbytné péče a ochranou bezpečnosti chráněné osoby a případně také dalších osob ve zdravotnickém zařízení se nacházejících. Rovněž tak čelí veřejně známé osobnosti nebo političtí činitelé specifickým výzvám při zajišťování spravedlivého přístupu ke kvalitní zdravotní péči. Zdravotnické zařízení by mělo zajistit, aby tyto osoby nebyly diskriminovány nebo znevýhodněny v přístupu ke zdravotní péči kvůli svému statusu nebo veřejnému obrazu.[30]

Je nezbytné, aby zdravotnická zařízení a odpovědný zdravotnický personál byli obeznámeni s relevantními právními předpisy, etickými směrnicemi a postupy, které se týkají poskytování

---

6 Dále jen „GDPR“.

7 Dále jen „zákon o zpracování osobních údajů“.

8 Popsaný střet lze pozorovat mezi nařízením GDPR, Usnesením předsednictva České národní rady ze dne 16. prosince 1992 o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky (dále jen „Listina“) a zákonem č. 372/2011 Sb., o zdravotních službách, ve znění pozdějších předpisů (dále jen „zákon o zdravotních službách“ nebo „ZZS“).

zdravotní péče chráněným osobám. Tím se zajistí dodržování práv a ochrana zájmů jak těchto jedinců, tak zdravotnického zařízení, při současném poskytování nezbytné zdravotní péče.

V posledních letech se objevila řada medializovaných případů, které se týkaly poskytování zdravotní péče ústavním činitelům nejen naší země, ale i jiných států. Současná globální bezpečnostní situace, jež vyvolává zvýšené nároky na ochranu členů ozbrojených sil a bezpečnostních složek během jejich hospitalizace, tyto otázky jen posiluje. Tyto situace otevírají prostor pro diskuzi o možných změnách v legislativě týkající se zdravotní péče pro chráněné osoby, a také pro jasnější vymezení tohoto pojmu.

2.1 Systém zdravotní péče

Nežli budou předloženy argumenty týkající se vymezení limitů a možností hospitalizace chráněné osoby včetně samotné její definice z pohledu zdravotního práva, je vhodné v krátkosti nastínit princip fungování zdravotního systému České republiky a legislativní rámec, v němž zdravotní systém funguje.

Na systém zdravotní péče je třeba pohlížet jako na komplexní množinu vzájemně interagujících prvků. V rámci této množiny lze rozlišit tři základní systémové úrovně:

1) mikro úroveň – úroveň interakce pacienta s lékařem,
2) meso úroveň – úroveň zdravotnických organizací,
3) makro úroveň – úroveň politiky zdravotní péče.[31]

Tambuyzer a kol. dále doplňují meta úroveň, do níž zařazují vzdělávání profesionálů a výzkum.[32]

Na těchto úrovních je pacient zapojován do systému zdravotnictví a může ovlivňovat jeho podobu. Dle názoru autora práce lze systém zdravotní péče chápat jako víceúrovňové pole, jehož aktuální podoba je potenciálně dialogicky vyjednávána klíčovými aktéry, mezi něž kromě pacientů patří zejména ministerstvo zdravotnictví a úřady veřejné správy, poskytovatelé zdravotnických služeb, zdravotní pojišťovny, odborné společnosti a komerční subjekty (farmaceutické firmy a výrobci či distributoři zdravotnických prostředků). Samostatná zdravotnická struktura přitom neleží ve vzduchoprázdnu, nýbrž je pevně formována společensko-politickým systémem naší země a s ním souvisejícími sociálními vlivy, kdy na uvedené formování významnou měrou působí aktuální evropské trendy v oblasti poskytování

zdravotní péče (nedostatek kvalifikovaného zdravotnického personálu; migrace zdravotnických pracovníků; platová politika jednotlivých členských zemí atd.).

Zdraví pozitivně přispívá k životní spokojenosti a hospodářskému růstu.[33] Efektivní systém zdravotní péče zajišťující kvalitní péči a rovný přístup zároveň přispívá k vyšší životní spokojenosti obyvatel. Z typologického hlediska je systém zdravotní péče České republiky obdobný jako systémy v Lucembursku, Rakousku, Řecku, Japonsku či Jižní Koreji. Systém zdravotní péče České republiky je postaven na principu veřejného základního pojistného krytí a do určité míry využívajícího tržní mechanismy na úrovni poskytovatelů zdravotní péče.[34] Široká nabídka poskytovatelů zdravotní péče zajišťuje uživatelům široký výběr mezi poskytovateli, neexistuje žádný *gate-keeping*, tedy funkce ve zdravotním systému, bez jehož doporučení se s výjimkou vyjmenovaných případů nemůže pacient obrátit přímo na specialistu či zdravotnické zařízení.[35] Hlavní prvky zdravotního systému České republiky spočívají v zásadě svobodného výběru poskytovatele zdravotních služeb, kdy došlo ke zrušení tzv. spádového systému poskytování zdravotní péče. S nástupem demokratického právního sytému došlo k privatizaci většiny poskytovatelů primární péče, specializované ambulantní péče mimo zdravotnická zařízení, farmaceutického průmyslu, lékáren a lázeňských zařízení. Lékařská péče má charakter veřejné služby a je poskytována různými typy poskytovatelů, kteří jsou financováni primárně zdravotními pojišťovnami.

Za zcela esenciální lze považovat již zmíněné poskytování kvalitní péče a rovný přístup. Bez garance těchto dvou hodnot ze strany státu není možné hovořit o společnosti jako o demokratické, založené na rovném postavení všech jejich členů. Samotný systém zdravotního pojištění je totiž založen na principu solidarity, který je prezentován faktem, že čerpání lékařské péče ani zdravotní stav pacienta nesouvisí s poskytnutou výší příspěvku do zdravotního systému. Finanční krytí zdravotního systému je tvořeno povinnými příspěvky všech ekonomicky aktivních obyvatel (zaměstnanci a OSVČ[9]), které jsou založeny na mzdě (platu) či příjmu. Ekonomicky neaktivní obyvatelé (děti, studenti, osoby na rodičovské dovolené, senioři, nezaměstnaní, vězni a žadatelé o azyl atd.) jsou pojištěni prostřednictvím státních příspěvků. Povinné příspěvky zdravotní péče odváděné z příjmů činí cca 75 % příjmů zdravotních pojišťoven a 54 % celkových příjmů zdravotního systému. Zbývající podíl pochází ze státního

[9] Osoba samostatně výdělečně činná (dále jen „OSVČ“).

rozpočtu jako příspěvek za ekonomicky neaktivní obyvatele a z finanční spoluúčasti pacientů. Z hlediska rozsahu poskytování zdravotní péče je českou právní úpravou stanoveno, že pojištěnci mají nárok na veškeré zdravotní ošetření poskytované s cílem zachovat nebo zlepšit zdravotní stav pacientů. V praxi je objem péče stanoven právními předpisy, seznamy, každoročním procesem vyjednávání mezi zdravotními pojišťovnami a poskytovateli s cílem definovat konkrétní podmínky úhrady a seznam zdravotních výkonů. Pro představu výdaje na zdravotnictví, které si občané hradí přímo, vyjádřené jako podíl z celkových výdajů na zdravotnictví, jsou nízké, například v roce 2022 představovaly v České republice 15 %, byly tedy pod průměrem OECD[10], jenž byl 20 %, a byly také nižší než v sousedních zemích (Rakousku, Maďarsku a Slovenské republice). Oproti průměru v zemích EU, které jsou součástí OECD, bylo v ČR také méně občanů, u kterých nebylo po vypuknutí pandemie postaráno o zdravotní péči. V roce 2023 byly náklady obdobné, přibližně 14.7 % z celkových výdajů na zdravotnictví. Průměrem OECD činil 19.6 %.[34]

Dle článku 31 Listiny má každý právo na ochranu zdraví.[36] Občané mají na základě veřejného pojištění právo na bezplatnou zdravotní péči a na zdravotní pomůcky za podmínek, které stanoví zákon. Zákon č. 48/1997 Sb., o veřejném zdravotním pojištění a o změně a doplnění některých souvisejících zákonů, ve znění pozdějších přepisů,[11] v § 13 odst. 1) stanoví, že: *„ze zdravotního pojištění se hradí zdravotní služby poskytnuté pojištěnci s cílem zlepšit nebo zachovat jeho zdravotní stav nebo zmírnit jeho utrpení, pokud*

a) odpovídají zdravotnímu stavu pojištěnce a účelu, jehož má být jejich poskytnutím dosaženo, a jsou pro pojištěnce přiměřeně bezpečné,

b) jsou v souladu se současnými dostupnými poznatky lékařské vědy,

c) existují důkazy o jejich účinnosti vzhledem k účelu jejich poskytování.“[37]

Znění § 13 odst. 1) ZVZP je v souladu s utilitaristickým přístupem k systému poskytování zdravotní péče obecně. Lze tedy konstatovat, že je kladen důraz na maximalizaci užitku a minimalizace utrpení pacientů. V kontextu rovného a nediskriminačního poskytování

[10] Dále jen „OECD“ (Organisation for Economic Co-operation and Development, český překlad autora: Organizace pro hospodářskou spolupráci a rozvoj).
[11] Dále jen „zákon o veřejném zdravotním pojištění“ či „ZVZP“.

zdravotní péče všem bez rozdílu, lze uvedené ustanovení považovat za jakýsi štít chránící právě ono základní právo pacientů na jim poskytovanou zdravotní péči.

2.2 Významný kontext právní úpravy poskytování zdravotní péče

Princip rovného postavení všech osob v jejich důstojnosti a právech hierarchicky dopadá také na principy poskytování zdravotní péče, která je poskytována všem osobám stejně, bez rozdílů. Z nastíněného pohledu ovšem plyne otázka, jak lze takového cíle ze strany státu dosáhnout. Nutně musí dojít k pokusu o definici určitého *„slušného minima zdravotní péče“*, které je skutečně možné ze strany státu garantovat všem bez rozdílů. Aby poté bylo možné tvrdit, že na slušné minimum zdravotní péče existuje právní nárok, je nutné uvést rozdílné právní pohledy na poskytování zdravotní péče a zejména zodpovědět esenciální otázku, zda má člověk obecně právo na zdravotní péči. Pokud je možné předjímat pozitivní odpověď, lze poté uvést, že i státem garantované slušné minimum zdravotní péče má být předmětem lidského práva.

Přístup k poskytování zdravotní péče lze rozlišit na dvě základní skupiny:

1) liberálně egalitářský přístup, který zdravotní péči vnímá z hlediska sociální odpovědnosti jako základní životně důležitou potřebu pro všechny bez ohledu na jejich socioekonomický status, a
2) libertariánský přístup, který z hlediska zdravotní péče klade důraz na odpovědnost jednotlivce.[38]

Dle prvního přístupu je zdravotní péče vnímána jako právo. Všechny činnosti a řešení související s poskytováním zdravotní péče musí začít základním plněním tohoto práva. Druhý přístup deklaruje naopak fakt, že společnost není povinna poskytnout základní zdravotní péči všem, což vychází z libertariánského předpokladu, že pouze taková práva, která zakazují jednání proti další osobě, jsou legitimní práva.

Zastánci libertariánského přístupu se obecně domnívají, že jakýkoliv právní nárok, který vyžaduje něco jiného než nečinnost poskytovatele služeb, není opravdovým právem. Z právního hlediska se v prvním případě jedná o tzv. pozitivní právo založené na principu, že pokud A má právo vůči B činit x, má B povinnost vůči A asistovat při této činnosti.[39] V druhém případě se jedná o tzv. negativní právo, které spočívá v tom, že pokud A má právo vůči B činit x, B má povinnost zdržet se bránění A činit x. Hlavní problém mají zastánci libertariánského přístupu s tím, že každé pozitivní právo zahrnuje určitou míru porušení svobody jednotlivce. Tento předpoklad vychází z následující premisy: aby B splnil svoji

povinnost vůči A s pomocí x, je vyžadováno, aby B získal y od C, což znamená, že B bude mít zdroj potřebný pro asistenci A s x. Narveson dále uvádí, že důkazní břemeno spočívá na zastáncích pozitivního práva v tom smyslu, že pro obhajobu pozitivního práva musí specifikovat, co a v jakém množství musí A poskytnout B.[39]

Odpovídající filosofický pohled na nastíněnou otázku přinesl Randa, který ve svém článku *„Slušné minimum zdravotní péče"*[40] nazírá z filosofického hlediska na svobodu jednotlivce z pohledu libertariánů jako na nedotknutelnou, a proto jakékoliv pozitivní právo, v tomto konkrétním případě právo na slušné minimum zdravotní péče, by bylo v rozporu s jejich pojetím individuální svobody jako nedotknutelného práva. Dle libertariánského pohledu je právo na zdravotní péči vnímáno jako negativní právo, tedy že je nepřípustné, aby bylo komukoliv bráněno, aby mu byla poskytnuta zdravotní péče. Tento libertariánský právní pohled je však např. dle Shuea[41] příliš zjednodušující, protože nebere v úvahu morální závazky, které s negativním právem souvisí. Shue vnímá pozitivní právo jako právo, které vyžaduje činnost, zatímco u negativního práva je princip založen na zdržení se činnosti. Libertariáni se domnívají, že vymahatelnost negativního práva je levnější než v případě pozitivního práva, protože nevyžaduje činnost.

Tento předpoklad je však dle Shuea chybný, protože opomíjí fakt, že vymahatelnost a zaručení negativního práva zahrnuje pozitivní činnost – zajištění infrastruktury nutné k vymahatelnosti negativních práv.[41] Z pohledu zastánců pozitivního práva je nutné uvést argumenty, které vedou k názoru, že je zdravotní péče pozitivním právem. Dle Randy je nezbytné jít ještě dále a dokázat, že zdraví a s ní spojená zdravotní péče je pro fungování lidského těla natolik fundamentální, že slušné minimum zdravotní péče, které je předpokladem zajištění normálního druhově typického fungování, je nejen pozitivním právem, ale i lidským právem.[42]

S nastíněným pohledem Randy lze souhlasit. Přijetí této teze je totiž esenciálně důležité pro vymezení právních mantinelů tzv. „VIP pacienta" v oblasti zdravotního práva. Konstatování, že určité minimum zdravotní péče je lidským právem, nás totiž v této sféře katapultuje do ústavního rámce Listiny, neboť zejména čl. 31 Listiny dává každému občanovi právo na ochranu zdraví se zmocněním dalších zákonů pro úpravu podmínek poskytování bezplatné zdravotní péče pro občany na základě veřejného zdravotního pojištění. Rozsah a podmínky veřejného zdravotního pojištění pak upravuje zákon o veřejném zdravotním pojištění. Jinými slovy je opět vyzdvihován princip rovnosti všech osob bez rozdílů.

Za zmínku stojí slovenský přístup, dle kterého existuje veřejná minimální síť poskytovatelů zdravotních služeb. Tato minimální síť poskytovatelů představuje uspořádání nejmenšího počtu veřejně dostupných poskytovatelů na území Slovenské republiky, kraje nebo okresu v takovém počtu a složení, aby došlo k zabezpečení efektivně dostupné, plynulé, soustavné a odborné zdravotní péče, a to s přihlédnutím k taxativně vybraným kritériím.[43]

Dle názoru autora práce je současný právní rámec upravující poskytování zdravotních služeb v celé jejich šíři koncipován systémově a logickým způsobem vychází, v kontextu tématu disertační práce, právě ze základních ústavních a lidsko-právních principů zakotvených v Listině. Tento rámec je nesmírně důležitý pro aplikační praxi zejména jednotlivých poskytovatelů zdravotních služeb, kdy z jejich pohledu nelze vycházet pouze z ustanovení zákona o zdravotních službách či jiných doplňujících právních předpisů a podzákonných norem, ale právě primárně z roviny ústavní.

2.3 Chráněná osoba

Konkrétní definici pojmu chráněné osoby v širším společenském vnímání předchází pojem „VIP osoba“, kterou je nezbytné vymezit v kontextu současné právní úpravy. Dění například kolem zdravotního stavu bývalého prezidenta České republiky Ing. Miloše Zemana (dále v této podkapitole jen „prezident republiky“) v průběhu posledních několika let, zejména v roce 2021, nutí zamyslet se nejen nad otázkou poskytování zdravotní péče tzv. „VIP osobám“, ale obecně nad rovným a nediskriminačním přístupem ke všem pacientům. Mnohdy se s pojmem „VIP osoba“ lze setkat v médiích, ale také na nejrůznějších společenských akcích.

Zkratka „VIP“ je vychází z anglického sousloví *„Very Important Person“*, volně přeloženo jako velmi důležitá osoba. Bývají tak označováni prominentní účastníci různých společenských akcí a často je zmíněná zkratka používána v souvislosti s celebritami. Jedná se o pojem, který ovšem není zakotven v žádném právním předpise. Například v Cambridgeském slovníku je „VIP osoba“ popsána takto: *„A very important person; a person who is treated better than ordinary people because they are famous or influential (= they have a lot of influence) in some way.”*[44] Českým překladem se jedná o velmi důležitou osobu; člověka, se kterým se zachází lépe než s běžnými lidmi, protože je nějakým způsobem slavný nebo vlivný (má velký vliv).

2.3.1 Právní rámec specifického postavení určité skupiny osob

Je nutné připomenout, že již čl. 1 Listiny, stanoví, že „*Lidé jsou svobodní a rovní v důstojnosti i v právech. Základní práva a svobody jsou nezadatelné, nezcizitelné, nepromlčitelné*

a nezrušitelné.“[42] Rovněž Ústavní soud v jeho nálezu IV. ÚS 412/04 zdůraznil, že těžištěm ústavního pořádku je jednotlivec a jeho práva garantovaná tímto pořádkem. Proto je nutné vycházet z priority občana jako jednotlivce nad státem, a tím i z priority základních občanských a lidských práv a svobod.[46] Je to právě koncept lidské důstojnosti, který zakládá prioritu lidské bytosti nad kolektivitou, a proto vévodí komplexu základních práv obsažených v ústavním pořádku.[47]

V daném kontextu lze doplnit rovněž nález Ústavního soudu II. ÚS 1191/08, dle kterého při výkonu veřejné moci, lhostejno v jaké formě, je třeba respektovat takto vyložená základní práva, jinak se totiž člověk může stát objektem práva. Tak se děje zpravidla tehdy, když nejsou vůbec zohledňována základní práva, přičemž právě k ochraně a šetření práv jednotlivce jsou všechny orgány veřejné moci ústavně zavázány.[48] Pakliže tedy zákonodárce nepřepokládá, že by existovali lidé rovní a rovnější, nelze formálně přisuzovat ani některým skupinám osob či jednotlivcům více práv, či méně povinností, které by pro ně mohly přirozeně plynout z titulu jejich postavení. To lze pouze na základě jasného legislativního vymezení, kterým jsou myšleny například výhody beztrestnosti plynoucí z titulu diplomatického postavení, politického postavení, exekutivního úřadu či jiných charakteristik.[49]

Z pohledu zdravotního práva a právních předpisů upravujících tuto oblast rovněž nelze nalézt osoby, kterým by z titulu jejich postavení či funkce vyplývala nějaká výhoda. Dle § 3 odst. 1 zákona o zdravotních službách, se pacientem rozumí „*fyzická osoba, které jsou poskytovány zdravotní služby“*.[29] Tato strohá, leč velmi důmyslná definice vystihuje podstatu rovnosti všech osob zakotvenou v Listině, tedy, že není více druhů pacientů, ale existuje v legislativním vymezení pouze jeden pacient (tj. fyzická osoba – člověk).

Možným „rozdělovníkem“ jednotlivých pacientů je pak časová závažnost jejich zdravotního stavu a charakter jim poskytované zdravotní péče. V této rovině, z pohledu zdravotního práva, autor definuje několik přednostních skupin pacientů. Jsou jimi například pacienti v akutním stavu ohrožení jejich života a zdraví, pacienti trpící nakažlivou infekční nemocí a obdobné skupiny pacientů[50]. Společným jmenovatelem těchto skupin je tedy potřeba neodkladnosti nebo akutnosti při jim poskytované zdravotní péči.

Jedním z hlavních problémů spojených s hospitalizací chráněných osob je etický aspekt péče. Existuje riziko, že tito pacienti budou mít přístup k lepším službám na úkor ostatních pacientů, což může vést k nerovnostem ve zdravotní péči. Jak uvádí studie publikovaná v *Journal*

of Ethics American Medical Association, „VIP služby“ mohou vést k nadměrnému využívání zdrojů a tlaku na lékaře, aby poskytovali péči, která není vždy nezbytná.[78] Další studie ukazuje, že většina lékařů necítí rozdíl v kvalitě péče mezi chráněnými osobami a běžnými pacienty, což naznačuje, že nadstandardní služby nemusí nutně vést ke zlepšení zdravotních výsledků[49]. Tento fakt zpochybňuje oprávněnost „VIP služeb“, pokud jejich existence vede k nerovnoměrnému rozdělení zdrojů bez prokazatelného přínosu.[79]

2.3.2 VIP osoba

Pomineme-li tzv. celebrity, tedy osoby mediálně známé (herce, modelky, vědce, sportovce, politiky, influencery atd.), existuje další skupina osob, které se poněkud vymykají z výše nastíněné definice. I přesto je k nim ovšem v praxi přistupováno odlišně, mnohdy s vyšší mírou důležitosti, která sice není nikde formálně zakotvena, ale může být, dle názoru autora, veřejností takto vnímána. Optikou poskytovatele zdravotních služeb či obecně státních institucí a orgánů, se dle autora jedná o osoby spadající do režimu tzv. „chráněných osob“, kterým je poskytována osobní či epizodická ochrana. Do zmíněné skupiny lze obecně z hlediska platné právní úpravy zařadit například trvale chráněné ústavní činitele České republiky a osoby, kterým je po dobu jejich pobytu na území České republiky poskytována ochrana podle mezinárodních dohod.[12] Zákonné znění tedy tyto osoby jmenuje jako chráněné osoby.

Oblastí, ve které se lze tedy nejčastěji setkat (částečně legitimně), s pojmem „*VIP osoby*“, je bezpečnost. Obecně lze deklarovat, že bezpečnost ČR je založena na principu zajištění bezpečnosti jednotlivce. Východiska bezpečnostní politiky se zakládají na trvalých demokratických hodnotách a principech. V jejich středu zůstává bezpečnost jednotlivce a ochrana jeho lidských práv a základních svobod.[51] Tento princip plynoucí z Bezpečnostní strategie ČR je odrazem demokratických principů plynoucích z ústavního pořádku naší země, neboť pro státní aparát je prioritní zajištění bezpečnosti v kontextu zajištění bezpečnosti

[12] Zejména **Vídeňská úmluva o diplomatických stycích z roku 1961**, která definuje status diplomatů a zajišťuje jejich ochranu a imunity na území přijímajících států. Tato dohoda upravuje ochranu diplomatických zástupců a členů jejich rodin po dobu jejich pobytu v zahraničí. Diplomatičtí zástupci jsou tedy považováni za chráněné osoby podle této úmluvy.
Dalším významným právním předpisem je **Úmluva o předcházení a trestání zločinů proti osobám požívajícím mezinárodní ochrany, včetně diplomatických zástupců z roku 1973**. Tato úmluva zavazuje státy k ochraně mezinárodně chráněných osob, jako jsou hlavy států, diplomaté a jiné důležité osoby, a stanovuje postihy pro osoby, které se dopustí zločinů vůči nim.

jednotlivce. Jinými slovy již není při normotvorbě využíváno ideologie, která by v zájmu blaha celku jednotlivce bezmyšlenkovitě obětovala.

2.3.3 Chráněná osoba

V daném kontextu ovšem z opačného pohledu existují jednotlivci, kteří mají určitým způsobem „výjimečné“ postavení a jsou chráněni více, nežli ostatní členové společnosti – je jim *de lege lata* přiřazeno určité „VIP postavení“ tzv. chráněné osoby.

Chráněná osoba je jedinec anebo rovněž skupina vyžadující osobní ochranu. Chráněná osoba může být označena jako „VIP“ – „very important person“.[52] Jde o veřejně známou, vlivnou osobu, kdy s ní může být zacházeno oproti běžné populaci nadstandardně. **Z pohledu zajištění její bezpečnosti se jedná o osobu, u které je vyšší riziko ohrožení na zdraví a životě.** Může se jednat například o umělce, politika, člena významné královské rodiny, podnikatele, milionáře, osoby zastávající pozici vládního činitele, mající vysokou pozici v obchodní společnosti, podnikatele, veřejně vystupující a pronášející politické názory, členy politických stran, veřejně vystupující a pronášející náboženské názory, členy náboženských církví, celebrity vystupující v médiích, příslušníky ozbrojených sil nebo bezpečnostních sborů nebo ale také osoby doprovázející „VIP osobu“ či její osoby blízké.[53]

Z pohledu *ultima ratio* lze potenciálního „VIP pacienta“ nalézt i v oblasti trestního práva, a to v situacích, kdy nelze bezpečnost ohrožené osoby zajistit jiným způsobem. Trestně právní instituty zasahující do práv a svobod ostatních osob v daný okamžik nepodléhajících ochraně prostředků trestního práva, lze totiž využít až v krajních situacích, kdy již nelze využít jiné instituty ostatních (mírnějších) oblastní práva.[54] Dle zákona č. 137/2001 Sb., o zvláštní ochraně svědka a dalších osob v souvislosti s trestním řízením a o změně zákona č. 99/1963 Sb., občanský soudní řád, ve znění pozdějších předpisů[13] totiž v souvislosti s trestním řízením definuje v § 2 odst. 1 „ohroženou a chráněnou osobu“ následovně:

„Za ohroženou osobu se pro účely tohoto zákona považuje osoba, která

a) *podala nebo má podat vysvětlení, svědeckou výpověď nebo vypovídala či má vypovídat jako obviněný anebo jinak pomáhala nebo má pomoci podle ustanovení trestního řádu k dosažení účelu trestního řízení, nebo*

[13] Dále jen „zákon o zvláštní ochraně svědka“ či „ZVOS“.

b) *je znalcem nebo tlumočníkem anebo obhájcem, pokud obviněný, kterého jako obhájce zastupuje, vypovídal nebo má vypovídat, aby pomohl k dosažení účelu trestního řízení, anebo*

c) *je osobou blízkou osobě uvedené v písmenu a) nebo b).”*[55]

Chráněnou osobou pak dle ustanovení § 2 odst. 2 ZVOS rozumí ohroženou osobu uvedenou v odstavci 1, které je poskytována zvláštní ochrana a pomoc.

Z hlediska ústavních činitelů lze nalézt jejich „VIP bezpečnostní postavení“ v ustanovení § 1 odst. 1 nařízení vlády č. 468/2008 Sb., o zajišťování bezpečnosti určených ústavních činitelů České republiky, ve znění pozdějších novel[14], podle kterého náleží ochrana následujícím státním činitelům:

*„**Zajištění bezpečnosti se trvale poskytuje ústavnímu činiteli České republiky, který vykonává funkci**:*

a) ***prezidenta republiky**, a to i po skončení výkonu jeho funkce,*

b) ***předsedy Poslanecké sněmovny** Parlamentu České republiky,*

c) ***předsedy Senátu** Parlamentu České republiky,*

d) ***předsedy vlády**.“*[45]

Dle § 1 odst. 2 NvZBUČ však náleží zákonná ochrana rovněž vybraným členům Vlády České republiky: „*Zajištění bezpečnosti se trvale poskytuje rovněž těmto členům vlády:*

a) ***ministru financí**,*

b) ***ministru zahraničních věcí**,*

c) ***ministru vnitra**,*

d) ***ministru spravedlnosti**,*

e) ***ministru průmyslu a obchodu**.“*[45]

Dle § 2 odst. 1 NvZBUČ se zajištěním bezpečnosti rozumí „*souhrn ochranných a bezpečnostních opatření prováděných Policií České republiky k nerušenému výkonu funkce ústavního činitele České republiky.“*[45]

Zmíněnou ochranu zajišťuje Útvar pro ochranu prezidenta a Ochranná služba Policie České republiky (Ptáček a kol, n. d.). Byť je zákon o zajišťování bezpečnosti ústavních činitelů

[14] Dále jen „nařízení vlády o zajišťování bezpečnosti ústavních činitelů“ či „NvZBUČ“.

podzákonný právní předpis, definuje v § 2 odst. 2 zcela zásadní charakteristiku zajištění bezpečnosti ústavních činitelů v podobě následujícího ustanovení: ***„Rozsah zajištění bezpečnosti závisí na bezpečnostní situaci a možné míře ohrožení.“***[45]

Ona bezpečnostní situace a zejména pak míra ohrožení podmiňuje totiž nejen adekvátní použití ochranných prostředků ze strany Policie České republiky[15], ale **zejména předurčuje i míru legitimního zásahu do práv a svobod osob přímo nebo nepřímo dotčených činnostmi souvisejícími s ochranou ústavního činitele. Popsanou míru zásahu do práv a svobod je možné analogicky aplikovat také do jiných, specifických oblastí práva. Explicitně se může jednat také o právo zdravotní či ústavní, kde je při aplikaci vybraných právních institutů poskytování zdravotní péče chráněným osobám nezbytné nalézt optimální hranici střetu obou zmíněných právních rovin.**

Mimo PČR se ochranou chráněných osob zabývá rovněž Vojenská policie, která dle zákona č. 300/2013 Sb., o Vojenské policii a o změně některých zákonů (zákon o Vojenské policii), ve znění pozdějších předpisů[16], chrání ministra obrany a vysoce postavené příslušníky Armády České republiky. Obecně je úlohou vojenské policie zajišťovat bezpečnost a ochranu v rámci vojenského prostředí. Mezi jejich zodpovědnosti může patřit ochrana a zabezpečení významných osob nebo objektů, vyšetřování trestných činů, řízení dopravního provozu na vojenských objektech, udržování pořádku a disciplíny v rámci vojenského prostoru a další. Popsanou úpravu vztahující se k chráněným osobám lze nalézt v ustanovení § 4 odst. 1 písm. k) ZoVP, dle kterého Vojenská policie ***„zajišťuje ochranu a doprovod ministra obrany a jím určených osob (dále jen „chráněná osoba“)“.***[57] Uvedenou ochranou je pověřeno Velitelství ochranné služby Vojenské policie.

Explicitně pak Vojenská policie postupuje dle ustanovení § 36 ZoVP, které obsahuje oprávnění pro konkrétní úkony vojenského policisty ve vztahu k zabezpečení bezpečnosti chráněné osoby. Úlohou Vojenské policie je poskytovat ochranu, dohled a zabezpečení těchto osob v souladu se zákony a předpisy, které upravují jejich činnost. Vojenská policie může mít speciální protokoly a postupy pro zajištění bezpečnosti chráněných osob. Tyto osoby mohou zahrnovat významné politické činitele, vojenské velitelské důstojníky, vysoké představitele vlády nebo jiné jedince,

[15] Dále jen „PČR“.
[16] Dále jen „zákon o Vojenské policii“ či „ZoVP“.

kteří jsou vystaveni zvýšenému riziku bezpečnosti. K zajištění jejich bezpečnosti Vojenská policie může provádět následující činnosti:

- Fyzická ochrana: Vojenská policie může poskytovat fyzickou ochranu chráněných osob a zajišťovat jejich bezpečnost prostřednictvím dohledu, eskorty nebo ochranky.
- Omezování přístupu: Vstup na určité místo, kde se chráněné osoby nacházejí, může být omezen a kontrolován. Vojenská policie může provádět kontrolu totožnosti, monitorovat přístupové body a sledovat pohyb osob v daném prostoru.
- Vyhodnocování rizik: Vojenská policie může provádět analýzu a hodnocení bezpečnostních rizik spojených s chráněnými osobami. Na základě těchto informací mohou být přijata opatření ke zvýšení jejich ochrany.
- Vyšetřování a prevence: Vojenská policie může provádět vyšetřování potenciálních hrozeb nebo trestných činů, které by mohly ohrozit bezpečnost chráněných osob. Dále mohou podnikat preventivní opatření ke snížení rizika vystavení těchto osob bezpečnostním hrozbám.[57]

Dle Šarbochové[58] spadají do skupiny chráněných osob, jež mají právo na poskytnutí ochrany státem zřízenými útvary, i zahraniční návštěvy v rámci ČR: *„Bezpečnostní doprovod zajišťuje Ochranná služba, případně Vojenská policie Armády České republiky. Rozsah opatření stanoví Ochranná služba podle momentální bezpečnostní situace a možné míry ohrožení. Ze strany České republiky je poskytována ochrana těmto chráněným osobám:*

- ***hlava státu,***
- ***předsedové obou komor parlamentu,***
- ***předseda vlády,***
- ***ministr zahraničních věcí,***
- ***ministr vnitra,***
- ***ministr spravedlnosti,***
- ***ministr obrany*** *(ochranu zajišťuje Vojenská policie Armády České republiky),*
- ***nejvyšší představitelé některých mezinárodních organizací.*** *"*[58]

Šarbochová rovněž uvádí, že *„Při přípravě návštěvy musí diplomatická mise oficiálně požádat o zabezpečení ochrany protokolární pracoviště příslušné státní instituce. V případě shora uvedených chráněných osob je to Diplomatický protokol Ministerstva zahraničních věcí ČR. Žádá-li diplomatická mise o ochranu osob mimo shora uvedený výčet, musí se s žádostí obrátit*

přímo na protokolární nebo jiné příslušné pracoviště té instituce, která je odpovědná za organizaci návštěvy. Detaily a zvláštní požadavky pak mise projednává přímo s Ochrannou službou a protokolem příslušné státní instituce.“[58]

2.3.4 Chráněná osoba v soukromoprávním režimu

Mimo zmíněnou skupinu „veřejně“ chráněných osob je nutné poukázat taktéž na druhou velmi významnou skupinu – chráněné osoby v tzv. „soukromoprávním režimu“. Popularita nebo jakýkoliv jiný společenský úspěch (podnikatelský, mediální, sportovní atd.) s sebou v mnoha případech nutně přináší požadavek na ochranu života a zdraví dané osoby, tedy její zařazení do skupiny chráněných osob. Tato skupina osob ovšem nepodléhá veřejnoprávní ochraně placené z peněz daňových poplatníků, tak jak tomu bylo u skupiny osob uvedených v předchozí subkapitole, nicméně je odkázána na sféru soukromou a činnost tzv. soukromých agentur či jiných subjektů poskytujících ochranu osob za úplatu. Schneider[59] v této oblasti definuje v rámci poskytování osobní ochrany na poli soukromých agentur dva pojmy. Klienta, přičemž klientem může být člověk, článek či organizace, která financuje ochranná opatření a ochranný tým. Chráněnou osobou je pak ten, komu je osobní ochrana poskytována.[59]

Základní rozdíl mezi ochranou poskytovanou státními složkami a soukromoprávními subjekty je ten, že státem poskytnutá ochrana má vícero možností a prostředků, může si dovolit rozsáhlejší ochranný tým, má větší pravomoci a často může vyžádat spolupráci u jiných složek státu (např. PČR, armádu apod.). Soukromé subjekty jsou naopak limitovány prostředky a finanční částkou, kterou je klient ochoten zaplatit. Navíc, soukromý subjekt je státem „omezován“ v povinnosti dodržování platných zákonů a nemožnosti využití tolika práv, kterými disponují v této oblasti státní orgány.

V daném kontextu všech kategorií chráněných osob, ať už veřejným či soukromým sektorem, je nutné zdůraznit, že ačkoli tedy požívají výše popsaných legislativních či jiných „výhod“, z pohledu zdravotnického práva jim tyto výhody žádné benefity nepřináší, pokud se nejedná o pacienta v přímém ohrožení života. *De lege* by takovým skupinám potenciálních pacientů měla být poskytována zdravotní péče v naprosto stejné míře kvality, jako komukoliv jinému a neexistuje žádný oprávněný nárok, který by tyto osoby v nastíněném kontextu zvýhodňoval.[60] Privilegia osob plynoucích z norem ústavního práva či výše finančních prostředků určených k zajištění bezpečnosti dané osoby totiž v normách zdravotního práva nenalézá pochopení.[61]

2.3.5 Vlastní definice pojmu chráněná osoba, VIP pacient a VIP návštěva

Na základě výše uvedených komparací a analýz je možné definovat následující východiska pro pojem chráněné osoby, „VIP pacienta“ a „VIP návštěvy“ v kontextu poskytování zdravotní péče, přičemž tato východiska zahrnují několik klíčových aspektů:

- **Chráněná osoba** je jedinec nebo skupina osob, které je na základě platné právní úpravy, nebo rozhodnutí oprávněného subjektu, poskytována zvýšená míra ochrany. Tato ochrana může zahrnovat fyzickou, virtuální i kybernetickou bezpečnost. Do kategorie chráněných osob spadají nejen ústavní činitelé nebo veřejně známé osobnosti, ale také vojáci, příslušníci PČR, členové bezpečnostních složek a další osoby, jejichž povaha činnosti či postavení vyžadují v daném čase zvláštní bezpečnostní opatření.
- **VIP pacientem** se rozumí pacient se statutem chráněné osoby státním nebo soukromým subjektem.[258] Tento pacient vyžaduje specifická opatření zajišťující nejen standardní kvalitní zdravotní péči, ale také zvýšenou bezpečnost jak z hlediska fyzické ochrany, tak i v oblasti ochrany citlivých dat.
- **VIP návštěvou** se rozumí fyzická osoba se statutem chráněné osoby státním nebo soukromým subjektem, která se nachází v prostředí poskytovatele zdravotních služeb za účelem návštěvy některého z pacientů. I v tomto případě je nutné zajistit odpovídající bezpečnostní opatření, aby nedošlo k ohrožení jak návštěvníka, tak dalších osob v prostředí zdravotnického zařízení.

V dalším textu tedy pro označení všech zmíněných kategorií osob autor používá souhrnný termín chráněná osoba, s výjimkou empirické části výzkumu, kde mohou být definovány specifické podkategorie.

Tato rozšířená definice zahrnuje nejen právní rámec, ale také praktické příklady poskytování zdravotní péče v kontextu současné bezpečnostní situace a zvýšených požadavků na ochranu zdravotnických zařízení.

2.4 Aplikace fyzických a virtuálních bezpečnostních opatření v rámci ochrany chráněných osob

V návaznosti na dosavadní pojednání o chráněných osobách, pacientech a chráněných osobách a zajištění jejich bezpečnosti je nutné reflektovat, že bezpečnostní opatření a právní předpisy, které chrání tyto osoby, musí být aplikovány jak v oblasti fyzické, tak virtuální bezpečnosti.

Kybernetická bezpečnost je v současném digitálním věku nezbytnou součástí komplexní ochrany, kterou stát poskytuje těmto zvlášť důležitým jedincům. Bezpečnostní opatření, která byla dříve zaměřena především na fyzickou ochranu, musí být nyní rozšířena tak, aby zahrnovala i ochranu proti kybernetickým hrozbám, které jsou čím dál tím více sofistikované a nebezpečné.[62]

Analogická aplikace právních předpisů je důležitým nástrojem v právní vědě, zejména tam, kde konkrétní právní úprava chybí nebo není dostatečně rozvinutá. Analogii lze definovat jako proces, při kterém se aplikují pravidla a principy jednoho právního institutu na jiný, podobný případ, který není výslovně upraven zákonem. Tento přístup je zakotven v právní teorii a praxi a umožňuje soudům a jiným právním institucím vyplnit mezery v právních předpisech a zajistit tak spravedlnost a právní jistotu. V kontextu kybernetické bezpečnosti chráněných osob je analogická aplikace právních předpisů nezbytná, protože právní úprava v této oblasti často zaostává za technologickým vývojem a aktuálními potřebami ochrany.[63]

Mezi právními teoretiky nepanuje shoda na tom, kam analogii zařadit a zda ji lze aplikovat obecně na všechny oblasti práva. Někteří autoři ji považují za jeden z argumentů (*argumentum per analogiam*) používaných při standardní metodě logického výkladu[64], jiní mají za to, že je spíše součástí nadstandardní metody teleologické.[65]

Analogie má obecně pomoci vyplnit mezery v právu. Ty můžeme rozlišovat na vědomé či nevědomé. Vědomé mezery jsou případy, kdy zákonodárce cíleně situaci zákonem neupravil. Oproti tomu mezery nevědomé vznikají neúmyslně nedokonalostí právní úpravy. Použitím analogie tak dochází k dotváření práva v oblastech, které ještě právem upraveny nejsou.

Někdy bývají za analogii označovány i případy, kdy k jejímu použití vyzývá sám zákon.[66] Nejvíce uváděným příkladem, který ve své podstatě do jisté míry analogii shrnuje, je § 10 odst. 1 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů[17], který uvádí, že *„nelze-li právní případ rozhodnout na základě výslovného ustanovení, posoudí se podle ustanovení, které se týká právního případu co do obsahu a účelu posuzovanému právnímu případu nejbližšího.“*[67] Ustanovení § 10 odst. 2 OZ dodává *„není-li takové ustanovení, posoudí se právní případ podle principů spravedlnosti a zásad, na nichž spočívá tento zákon,*

[17] Dále jen „občanský zákoník“ či „OZ“.

tak, aby se dospělo se zřetelem k zvyklostem soukromého života a s přihlédnutím k stavu právní nauky i ustálené rozhodovací praxi k dobrému uspořádání práv a povinností."[67]

Dále se jedná také o případy, kdy ustanovení odkazuje na jiné upravující podobnou situaci za použití slov „obdobně" či „přiměřeně." Takové odkazy ale nejsou příliš žádoucí a zákonodárce by je měl používat spíše výjimečně a skutečně tam, kde jsou vhodné.

Analogie se tradičně rozlišuje na analogii *legis* (*per analogiam legis*) a analogii *iuris (per analogiam iuris)*. Při použití analogie *legis* se aplikuje nejvíce podobný právem upravený případ. Analogie *iuris* aplikuje obecné právní principy, případně odvětvové zásady, avšak přichází na řadu až poté, kdy není nalezeno vhodné ustanovení, které by bylo možné na situaci vztáhnout.[68]

Použití analogie však není bezbřehé a je nutné, aby při použití byly naplněny určité předpoklady. **Analogie nesmí být v daném případě nepřípustná**. Jedná se zejména o situace v trestním právu, kdy by použití analogie bylo k tíži pachatele, obdobně je tomu ve správním přestupkovém právu. Dále je analogie zcela vyloučena při posuzování kompetencí a pravomocí či při stanovení daní a poplatků. Tyto zákazy lze vyvodit mimo jiné i z ústavního pořádku (např. čl. 39 a čl. 11 odst. 5 Listiny).[69] Někdy bývá zahrnován i judikaturně dovozený názor zákazu vydat konstitutivní rozhodnutí na základě použití analogie[18].[70]

Klíčovým aspektem je vhodnost aplikace analogie. Zejména při použití analogie *legis* musí být přítomna dostatečná podobnost relevantních prvků porovnávaných případů a v potaz musí být brán i účel aplikovaného zákona či ustanovení. Použití analogie také nesmí odporovat zásadám právní logiky.

V oblasti kybernetické bezpečnosti může být analogie použita k aplikaci existujících právních norem, které upravují fyzickou bezpečnost a ochranu osobních údajů, na nové digitální prostředí a kybernetické hrozby. Například, principy stanovené v zákoně o zvláštní ochraně svědka mohou být aplikovány na ochranu dat a komunikace chráněných osob. Tento zákon poskytuje rámec pro ochranu osob v nebezpečí a analogicky může být použit i pro zajištění jejich kybernetické bezpečnosti. Stejně tak nařízení GDPR, které chrání osobní údaje,

[18] Blíže viz např. rozhodnutí Nejvyššího soudu ze dne 16. května 2005, sp. zn. 22 Cdo 1438/2004.

lze aplikovat na ochranu digitálních identit a citlivých informací chráněných osob v online prostředí.[55]

Tento přístup je podpořen nejen teoreticky, ale i prakticky. V rámci mezinárodních organizací, jako je ENISA[19], je analogická aplikace právních předpisů často doporučována jako způsob, jak efektivně reagovat na nové výzvy v oblasti kybernetické bezpečnosti. ENISA ve svých publikacích zdůrazňuje, že principy ochrany osobních údajů a fyzické bezpečnosti mohou a měly by být rozšířeny na digitální prostředí, aby byla zajištěna komplexní ochrana všech aspektů života chráněných osob[71]. Rovněž NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)[20] doporučuje využití analogie při tvorbě strategií kybernetické bezpečnosti pro kritickou infrastrukturu, což zahrnuje i ochranu chráněných osob.[72]

V kontextu zajištění virtuální bezpečnosti chráněných osob je důležité zmínit, že právní rámec České republiky zahrnuje zákony a nařízení, která mohou být aplikována analogicky, pokud přímá právní opora není explicitně definována. Například, ochrana osobních údajů a citlivých informací je zajištěna dle nařízení GDPR a zákona č. 110/2019 Sb., o zpracování osobních údajů, ve znění pozdějších předpisů. Tato legislativa poskytuje robustní rámec pro ochranu dat, který lze efektivně aplikovat i na chráněné osoby, zejména pokud jde o jejich zdravotní údaje a další citlivé informace.[73]

V praxi to znamená, že všechny opatření týkající se fyzické bezpečnosti chráněných osob je vhodné analogicky rozšířit tak, aby pokrývala i digitální prostředí. To zahrnuje šifrování komunikace, zabezpečení datových úložišť, ochranu proti malwaru a jiným kybernetickým útokům. Zvláštní důraz je kladen na ochranu zdravotních dat, které jsou mimořádně citlivé a mohou být cílem útoků s cílem získat výkupné nebo poškodit reputaci chráněné osoby.[74]

Stát musí logicky chránit virtuální bezpečnost těchto osob s ohledem na jejich zvláštní postavení. Pokud konkrétní právní úprava chybí, musí být postupováno analogicky dle

---

[19] ENISA (European Union Agency for Cybersecurity) je agentura Evropské unie, která se zaměřuje na zajištění kybernetické bezpečnosti v rámci EU. Byla založena v roce 2004 a její hlavním cílem je podporovat členské státy EU v prevenci, řešení a zvládání kybernetických hrozeb a incidentů. ENISA poskytuje odborné poradenství, podporuje výzkum v oblasti kybernetické bezpečnosti a koordinuje spolupráci mezi členskými státy a dalšími organizacemi, aby posílila odolnost proti kybernetickým útokům.

[20] NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) je výzkumné a vzdělávací centrum zaměřené na kybernetickou obranu, které podporuje NATO. Bylo založeno v roce 2008 v Tallinnu, Estonsko. Jeho hlavním cílem je poskytovat odborné analýzy, výzkum, výcvik a vzdělávání v oblasti kybernetické bezpečnosti pro členské státy NATO a partnery. CCDCOE se zabývá strategickými, technickými, právními a operačními aspekty kybernetické obrany a podporuje sdílení znalostí a spolupráci mezi spojenci.

existujících předpisů, které zajišťují ochranu citlivých informací. Tato analogie vychází z principu právní jistoty a ochrany práv jednotlivců, jak je definováno například Listinou, kde je zdůrazněno, že každý má právo na ochranu svého soukromí a osobních údajů.[75]

Speciálním právním odvětvím je zdravotnické právo, které lze považovat za velmi specifickou oblast nejen proto, že se dotýká života a zdraví, ale i proto, že prostupuje celou řadou jiných právních odvětví, včetně kybernetické bezpečnosti a ochrany osobních údajů. Nejen soudy (např. rozhodnutí Nejvyššího soudu ze dne 28. dubna 2016, sp. zn. 23 Cdo 1988/2014, ve kterém bylo dovozeno použití tzv. úhradové vyhlášky pro rok 2012 (vyhláška č. 425/2011 Sb.) i pro úhrady za poskytnutou zdravotní péči v pobytových zařízeních sociálních služeb), ale i poskytovatelé zdravotních služeb jsou někdy nuceni zaplňovat situace, na které zákonodárce nepomyslel, nebo je neupravil dostačujícím způsobem. Jednou z takových oblastí je otázka bezpečnosti se stále se zrychlujícím technickým rozvojem zejména problematiky kyberbezpečnosti. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů[21] totiž pokládá pouze obecný rámec a neřeší některé specifické situace, které mohou nastat při poskytování zdravotních služeb.

Analogická aplikace právní úpravy je nezbytná i v rámci specifických situací, jako je ochrana svědků dle zmíněného zákona o zvláštní ochraně svědka. Tento zákon poskytuje rámec pro ochranu osob, které jsou v nebezpečí kvůli jejich účasti v trestním řízení. Tento princip ochrany by měl být přenesen i do oblasti kybernetické bezpečnosti, aby byla zajištěna komplexní ochrana všech aspektů jejich života.[55] Jinými slovy **není možné se zaměřovat pouze na bezpečnost fyzickou, ale také virtuální a právní ochranu osobních údajů**.

Zajištění virtuální bezpečnosti chráněných osob ovšem vyžaduje spolupráci různých státních a soukromých subjektů. Například Útvar pro ochranu prezidenta a Ochranná služba Policie České republiky by měly spolupracovat s Národním úřadem pro kybernetickou a informační bezpečnost[22] při zajištění kybernetické ochrany těchto osob. Soukromé agentury poskytující ochranu chráněným osobám musí rovněž investovat do moderních technologií a školení svých zaměstnanců v oblasti kybernetické bezpečnosti.[76]

---

[21] Dále „zákon o kybernetické bezpečnosti“ nebo „ZoKB“.
[22] Dále jen „NÚKIB“.

V neposlední řadě je důležité zdůraznit, že efektivní ochrana virtuální bezpečnosti vyžaduje také neustálé vzdělávání a osvětu samotných chráněných osob. Tyto osoby by měly být informovány o rizicích, která jim hrozí v digitálním prostředí, a měly by být vybaveny znalostmi a nástroji, jak se těmto rizikům bránit. To zahrnuje používání silných hesel, pravidelnou aktualizaci softwaru a uvědomělý přístup k používání sociálních médií.[71]

Je také nutné brát v potaz dynamický vývoj kybernetických hrozeb, který vyžaduje flexibilní a adaptabilní přístup k zabezpečení. Právní rámec by měl být pravidelně aktualizován, aby odpovídal aktuálním technologiím a metodám útoků. Tento proces by měl zahrnovat jak preventivní opatření, tak i mechanismy pro rychlou reakci na incidenty a zmírnění jejich dopadů.[77]

Efektivní spolupráce mezi veřejným a soukromým sektorem je klíčová. Stát by měl poskytovat metodickou podporu a nastavovat standardy, zatímco soukromé subjekty by měly implementovat technologická řešení a postupy na operativní úrovni. Taková synergická spolupráce může výrazně zvýšit úroveň ochrany chráněných osob v digitálním prostoru.[72]

Dílčí shrnutí

V rámci dílčího závěru této kapitoly lze konstatovat, že **zabezpečení virtuální bezpečnosti chráněných osob je nezbytným a logickým rozšířením jejich fyzické ochrany**. Vzhledem k absenci právní úpravy virtuálních bezpečnostních opatření je nezbytné, aby poskytovatelé zdravotních služeb analogicky využívali současné znění právní úpravy a dokázali tak *lege artis* zajistit optimální míru zabezpečení nejen fyzické, ale zejména pak virtuální bezpečnosti chráněných osob. Stát a soukromé subjekty musí společně pracovat na vytvoření komplexního systému ochrany, který zahrnuje jak právní, tak technické a organizační aspekty, aby byly tyto osoby chráněny před všemi typy hrozeb, kterým mohou čelit. Tento přístup nejenže zajistí jejich bezpečnost, ale také posílí důvěru veřejnosti ve schopnost státu nediskriminačně chránit své občany v digitálním věku.[15]

2.5 Aktuální trendy v oblasti hospitalizace chráněné osoby

Hospitalizace chráněných osob představuje specifickou oblast zdravotní péče, která vyžaduje zvláštní přístup jak z hlediska medicínského, tak etického, organizačního, ale zejména bezpečnostního. Jak bylo zmíněno dříve, chráněné osoby mohou zahrnovat široké spektrum jedinců od politických činitelů, celebrit, významných podnikatelů až po další osoby s významným veřejným profilem. V kontextu války na Ukrajině a Izraeli se ovšem okruh

chráněných osob rozšiřuje o celou řadu dalších skupin pacientů, zejména pak vojáků z povolání. Poskytování zdravotní péče těmto pacientům se často setkává s unikátními výzvami, které zahrnují zvýšené nároky na soukromí, bezpečnost a také specifická očekávání ohledně kvality péče.

Hospitalizace chráněných osob také vyžaduje zvláštní organizační a bezpečnostní opatření. Chráněné osoby zpravidla vyžadují zvýšenou míru soukromí a bezpečnosti, aby byla chráněna jejich identita a osobní údaje. To může zahrnovat například oddělené pokoje, speciální vstupní a výstupní protokoly a zvýšenou přítomnost bezpečnostního personálu. V moderním zdravotnictví je kladen důraz na kybernetickou bezpečnost, která je nezbytná pro ochranu citlivých zdravotních údajů chráněných osob. Podle ENISA je nezbytné, aby principy ochrany osobních údajů a fyzické bezpečnosti byly rozšířeny i na digitální prostředí.[71] Hospitalizace chráněných osob je proto komplexní téma, které vyžaduje pečlivé zvážení jak praktických, tak etických aspektů. Vyvážení potřeb chráněných osob s potřebami široké veřejnosti je klíčové pro udržení rovnosti a spravedlnosti ve zdravotní péči.

Výsledkem střetu popsaných právních stran zdravotního a ústavního práva na poli poskytování neodkladné či akutní zdravotní péče je dle autora práce zjištění, že mají naprosto stejné postavení. Jinými slovy **chráněná osoba nemá z hlediska poskytování zdravotních služeb přednostní postavení před ostatními fyzickými osobami.**[80] Nemůže tomu býti ani jinak, neboť bychom poté o naší společnosti nemohli hovořit jako o demokratické garantující rovné postavení všech jejích členů.

Postup *lege artis* se v kritických stavech vztahuje na všechny fyzické osoby jednotně. Postupy a opatření se neliší podle věku, etnika, pohlaví, sociálního postavení postiženého, podle jeho intelektuální, mentální či celkové životní úrovně. V této sféře je zdůrazňován optimální, ovšem totožný zájem pacienta jak pro tzv. speciálního „chráněného“ jedince, tak pro příslušníka minoritní a vulnerabilní kategorie občanů.[81] Teprve podle klinického průběhu a reakce na akutní léčbu či intenzivní péči se připojí k požadavkům a zásadám *lege artis* jednání lékařů zpracováním etapové epikrízy. Její závěr stanoví viabilitu pacienta – jeho celkovou rezervu zvládnout akutní inzult a maximálně pravděpodobnou prognózu přežití. Vyjádří se k rozsahu poskytované péče. Nutno dodat, že u tzv. racionálního pacienta, který o sobě dokáže v daném čase rozhodnout, se respektují jeho zjištěná přání a rozhodnutí.[82]

Dle tacitních zkušeností autora práce se samotná hospitalizace tohoto typu pacienta z lékařského pohledu řídí standardně shodnými pravidly, jako hospitalizace kohokoliv jiného. Existuje ovšem celá řada specifických oblastí, které mohou být vlivem společenského statusu pacienta brány do úvahu při jeho umístění na konkrétní budovu, pokoj, lůžko nebo naopak mohou být zvažovány při aplikaci některých postupů, ať už lékařských, logistických, bezpečnostních či provozních. Jednou z těchto oblastí je i zajištění intimity a soukromí chráněné osoby.[83]

Obzvláště ve sféře zachování soukromí chráněné osoby je v případě jeho hospitalizace obvykle vyvíjen enormní mediální tlak na dané zdravotní zařízení. Nevědomky tím dochází k důslednějšímu přezkumu jeho postupu veřejným sektorem, který má, mnohdy kontinuální, informace o jeho činnosti ve vztahu k danému pacientu.[84] O to více obtížnější je poté ze strany daného poskytovatele zdravotních služeb zachovat maximálně intimitu a soukromí každého ošetřovaného a tedy postupovat *lege artis*. Jedná se o silně etický a estetický požadavek každého ošetřovaného, nejen chráněné osoby, neboť zdravotní služby je nezbytné *de lege* poskytovat v souladu s ustanovením § 4 odst. 5 zákona o zdravotních službách *„při respektování individuality pacienta“*.[29]

Speciální metodická doporučení i společenského rázu v těchto případech jsou v *lege artis* akutních postupech vypracována pro péči o pacienty zařazované do některé z kategorií chráněných osob, nemají nicméně vyčleněné legislativní znění. Snad jen pokud jde o diplomatické pracovníky, lze čerpat v obecné rovině, aplikovatelné jistě i na poskytování zdravotních služeb, z mezinárodně-právních dokumentů upravujících tzv. diplomatické právo; svůj význam pak v tomto kontextu mají též diplomatické protokoly, jež sice nemají povahu právních předpisů, nicméně důraz na jejich dodržování je kladen ve zvýšené míře.[56]

Oblast poskytování zdravotní péče členům diplomatických misí lze upravit i smluvně, a to přímo s daným poskytovatelem zdravotních služeb. Předmětem takové smlouvy pak mohou být, dle zkušeností autora práce, právě konkrétní provozní, organizační, technické, finanční či personální podmínky zabezpečení zdravotní péče ze strany poskytovatele zdravotních služeb. **V žádném z ohledů však není možné ošetřit smluvně určité přednostní či výsadní právo v rámci poskytování zdravotních služeb**.[85]

V případě, že se chráněná osoba rozhodne využít služeb některého z poskytovatelů zdravotních služeb nebo se ocitne ve stavu, který vyžaduje poskytnutí neodkladné nebo akutní zdravotní

péče, dochází tedy téměř vždy ke střetu dvou právních rovin. Tou první je rovné postavení všech pacientů a práva na poskytování stejné zdravotní péče v určité standardní kvalitě a tou druhou je zájem státu na ochraně života a zdraví „společensky významné“ osoby (chráněné osoby). Popsaný boj právních rovin lze dle názoru autora práce spatřovat jak v areálu či budovách poskytovatelů zdravotních služeb (zdravotnických zařízení), tak kdekoliv na území našeho státu.

Demonstrativním případem výše uvedeného může být mediálně známá hospitalizace prezidenta republiky v ÚVN na podzim roku 2021. „Běžný“ občan České republiky nedisponující ústavními privilegii by jen stěží měl nastaven tak přísný režim jeho fyzické ochrany zasahující do provozu zdravotnického zařízení natolik, že je mu věnována zvýšená péče. Přítomnost policistů útvaru Ochranné služby PČR přímo na jednotce intenzivní péče je totiž sama o sobě velkým zásahem do každodenních činností lékařského a nelékařského zdravotnického personálu působícího na daném oddělení, které lze definovat jako oddělení *sui generis*. Hospitalizace prezidenta republiky a permanentní dohled jeho ochranky ovlivňuje celou řadu procesů nejen na úrovni lékařské, ale také provozní. Práce či služba na zmíněném typu oddělení již sama o sobě vybočuje svou náročností, charakterem a požadavky mimo standardy ostatních oddělení poskytovatele zdravotních služeb, neboť se jedná o oddělení s pacienty, kterým je poskytována neodkladná nebo akutní zdravotní péče a mnohdy jsou v přímém ohrožení života. Dle názoru autora plynoucího z vlastních praktických zkušeností vzniká vlivem faktické přítomnosti zmíněných osob enormní tlak na celý zdravotnický i ostatní personál takového oddělení, což v konečném důsledku může ovlivnit míru kvality poskytovaných zdravotních služeb.

Není například zcela běžné, aby na návštěvy k chráněné osobě chodili přední ústavní činitelé bez vědomí ošetřujícího lékaře za účelem podepisování významných ústavních dokumentů.[86] Poprvé v novodobé historii České republiky se tak místem realizace *„projevu vůle“* prezidenta republiky svolat zasedání nového složení Poslanecké sněmovny Parlamentu České republiky stalo prostředí oddělení jednotky intenzivní péče poskytovatele zdravotních služeb.

Pomineme-li skutečnost, že veřejnost nebyla obeznámena se zdravotním stavem prezidenta republiky, kdy vyvstávaly tehdy legitimní úvahy o jeho způsobilosti vyjádřit svou vlastní vůli, je v období po parlamentních volbách velmi významným subjektem. I tato jeho významnost ovšem nemá z pohledu ústavního práva potenciál přisuzovat mu, oproti jiným pacientům, nadstandardní privilegia v oblasti poskytování zdravotní péče.[87] Z obecných mediálních

výstupů lze mylně vnímat, že tak dochází k jeho určitému nadřazení nad ostatní pacienty, neboť jeho role z hlediska budoucího povolebního vývoje byla v danou chvíli nesmírně významná. Lze se dokonce mylně domnívat, že tato jemu propůjčená konkrétní ústavní důležitost předjímá i jeho „VIP postavení“ mezi ostatními pacienty. **Z pohledu platné právní úpravy ovšem nemá, byť v této pozici, jiné, výsostní postavení oproti ostatním pacientům a stále je nutné k němu z pohledu poskytování zdravotní péče přistupovat standardním způsobem.**[88]

Ačkoliv je prezident České republiky vrchním velitelem ozbrojených sil, není samozřejmostí, že případný požadavek na jeho hospitalizaci bude realizován v prostředí některého z tzv. vojenských poskytovatelů zdravotních služeb. I přes tento fakt je prezident republiky stále občanem se všemi jeho právy a povinnostmi, tedy i s právem svobodně si zvolit poskytovatele zdravotních služeb tak, jak mu to garantuje zákon o zdravotních službách. Tak tomu jistě bylo i v případech jeho hospitalizací v ÚVN. ÚVN poskytuje komplexní zdravotnickou péči o dospělé pacienty, založenou na nejmodernějších léčebných metodách a postupech ve všech oborech s výjimkou kardiochirurgie, porodnictví a léčby popálenin. Jako jediná vojenská fakultní nemocnice v ČR je výcvikovým, vzdělávacím a odborným zdravotnickým zařízením Armády České republiky. Komplexně dlouhodobě pečuje o válečné veterány.[89]

Přestože lze historicky vnímat ÚVN jako primární zdravotnické zařízení určené pro poskytování zdravotní péče prezidentům republiky, její předmět činnosti to jistě není a nelze ani tvrdit, že by se jednalo o vyčleněné pracoviště pro potřeby ústavních činitelů (mimo úkoly plynoucí pro ÚVN z jejího postavení v systému IZS nebo krizového řízení). Na příkladu ÚVN lze ovšem demonstrovat současnou připravenost zdravotnického zařízení na hospitalizaci chráněných osob.

Pro srovnání například v USA existuje tzv. Vojenská kancelář Bílého domu, která, mimo kompletní logistické zabezpečení chodu úřadu prezidenta, zabezpečuje rovněž zdravotnický servis přímo prezidentovi USA: *„Vojenský úřad Bílého domu (WHMO) poskytuje vojenskou podporu funkcím Bílého domu, včetně stravovacích služeb, prezidentské dopravy, lékařské podpory, akutní lékařské péče a pohostinských služeb.“*[90] V rámci České republiky sice existuje Kancelář prezidenta České republiky, ta ovšem není určena k zabezpečení zdravotních služeb hlavy státu. Rovněž neexistuje ani přímo určený poskytovatel zdravotních služeb, který by byl vyčleněn pro prezidenta republiky, případně pro ostatní ústavní činitele. Existují samozřejmě tzv. závodní lékaři, ti ovšem nejsou určeni pro konkrétní jednotlivce, nýbrž pro skupinu zaměstnanců daného úřadu či instituce.

Jak bylo nastíněno výše, v současné době nelze nalézt jakýkoliv legislativní rámec určující alespoň minimální pravidla a standardy při hospitalizaci chráněných osob. Dle zjištění autora rovněž ani ÚVN nedisponovala kodifikovaným vnitřním předpisem či metodikou, která by její zaměstnance na takovou hospitalizaci připravila. Mimo zdravotní péči poskytovanou příslušníkům zpravodajských služeb, jejichž mateřské organizační složky jim samy ze zákona zabezpečují skrytí jejich pravé totožnosti[91], neexistuje žádný formální systém, který by popsanou hospitalizaci reflektoval.

Každá hospitalizace chráněné osoby, která disponuje vlastní ochrankou, je tedy řešena operativně s danou organizační složkou státu, ústředním správním úřadem či ministerstvem, kdy jsou přijata vedením zdravotnického zařízení konkrétní opatření a jsou nastavena specifická pravidla. Tato opatření a pravidla v legitimní míře reflektují zejména požadavek fyzické ochrany chráněné osoby. S tím souvisí zejména přítomnost členů ochranky, kterou nelze zakázat. Lze ji omezit pouze na situace zachování soukromí chráněné osoby například při jejím ošetřování, při poskytování lékařské péče nebo při jeho návštěvách osobami blízkými, kdy je žádoucí poskytnout chráněné osobě soukromí a určitou míru intimity. Stále ovšem musí být fyzická přítomnost ochranky chráněné osoby zajištěna, a to do takové míry, aby mohla zasáhnout i v případě ohrožení chráněné osoby například osobou jemu blízkou.

Realizace hospitalizace chráněné osoby z pohledu skloubení zajištění jeho bezpečnosti a patřičné úrovně jemu poskytovaných zdravotních služeb dle autora práce tkví v následujícím základním schématu. Ať již se jedná o hospitalizaci s nutností umístění na jednotce intenzivní péče nebo na standardním pokoji, je nezbytné jasně vymezit přístupová práva konkrétních osob k chráněné osobě, a to jak z pohledu zdravotnického zařízení, tak z pohledu ochranky chráněné osoby.

V případě zdravotnického zařízení je toto vymezení realizováno cestou vedoucího zaměstnance daného oddělení, který vymezí okruh zdravotnických zaměstnanců vyčleněných pro poskytování zdravotní péče chráněné osobě. Mnohdy se může jednat o všechny zaměstnance daného oddělení, kdy je stanoven pouze jeden hlavní ošetřující lékař. Samotný režim vstupu těchto zdravotnických pracovníků na dané oddělení je řešen zpravidla systémově, tedy standardním způsobem (například autorizovanou čipovou kartou atd.). Tato kontrola je ovšem „dublována“ kontrolou ze strany ochranky chráněné osoby, která kontroluje vpuštění oprávněných zdravotnických pracovníků. Jinými slovy ochranka dohlíží na to, aby některá z osob nebyla vpuštěna na oddělení neoprávněně. Mimo kmenové zdravotnické pracovníky

daného oddělení je možné vpustit i ostatní zaměstnance, je-li jejich přítomnost nezbytná. Může se jednat o ostatní lékaře (např. konziliární vyšetření), nelékařský zdravotnický personál, technický personál aj. Jejich vpuštění ovšem musí být odsouhlaseno ošetřujícím lékařem nebo smí být uskutečněno pouze s jeho vědomím. Vše závisí na charakteru případného vstupu na dané pracoviště. V daném kontextu se lze domnívat, že mimo onu „dublovanou" kontrolu se jedná o standardní postup, ovšem, není tomu tak.

Chráněné osoby je, mimo popsaná režimová opatření, nutné umístit nejlépe na samostatný pokoj bez možnosti hospitalizace jiného pacienta, a to právě z důvodu zajištění maximální možné míry jeho bezpečí. Lze předpokládat, že se bude jednat o pokoj s uzavíratelnými dveřmi s průhlednou výplní. V takovém případě, stejně jako tomu bylo u prezidenta republiky při jeho hospitalizaci na jednotce intenzivní péče na Klinice anesteziologie a resuscitace 1. Lékařské fakulty Univerzity Karlovy a ÚVN, je možné umístit ochranku chráněné osoby bezprostředně před vstup do jeho pokoje s tím, že je zachována přijatelná míra jeho soukromí a intimity při poskytování zdravotní péče a rovněž při jeho návštěvách. Pakliže by dveře od takového pokoje nebyly průhledné, jen stěží by bylo možné ponechat chráněnou osobu samotnou v přítomnosti jiné osoby, byť osoby blízké, bez jejího permanentního dohledu.

Zmíněné dveře a analogicky i ostatní průhledné bariéry (okna, stěny apod.), konkrétně u pokoje prezidenta republiky na jednotce intenzivní péče, lze vnímat nejen jako fyzickou bariéru oddělující dva prostory, ale také jako onu pomyslnou hranici mezi ústavním a zdravotním právem. Na jedné straně na lůžku leží nejvyšší ústavní činitel nesoucí na bedrech stěžejní rozhodovací pravomoci mající bezprostřední dopad na chod naší země, ale na straně druhé, na tomtéž lůžku, leží člověk, pacient, který má svá osobnostní práva, zejména právo na soukromí. Za dveřmi, u lůžka pacienta zcela jasně vítězí právo zdravotní, a to jak z pohledu způsobu poskytování zdravotní péče, tak z pohledu práv pacienta. Z praktického pohledu je tedy po průchodu těmito dveřmi ke chráněné osobě přistupováno zcela standardním způsobem.

Dle názoru autora práce se totiž z pohledu zdravotnického zařízení stále primárně jedná o pacienta, tj. fyzickou osobu s tím rozdílem, že jeho přítomnost sama o sobě vyvíjí systémový tlak na způsob a kvalitu jemu poskytované zdravotní péče. Popsané tvrzení vychází z autorovi vlastní tacitní zkušenosti a není tím myšleno poskytování vyšší kvality zdravotní péče, takový pojem je zavádějící, neboť každé chráněné osobě je poskytována ta nejvyšší možná úroveň kvality zdravotní péče. Naopak, autor práce tím podněcuje vznik úvahy o potenciálně vyšší

míře kontroly kvality poskytované zdravotní péče chráněné osobě plynoucí například i z přítomnosti sdělovacích prostředků.

2.6 Aktuální trendy v oblasti návštěv chráněné osoby

Stejně, jako je tomu v případě hospitalizace chráněné osoby, platí obecně závazná pravidla plynoucí z právních předpisů i pro tzv. návštěvy této osoby. Hospitalizace chráněné osoby s sebou přináší střet dvou pomyslných právních rovin ústavního a zdravotního práva nejen z pohledu poskytování zdravotní péče takovému pacientu, ale také z pohledu výkonu jeho funkcí. Ať už je návštěvou významný ústavní činitel, blízký spolupracovník, celebrita či „běžný občan“, zákon nepředpokládá existenci „VIP skupin návštěv“, které se nemusí řídit obecně platnými pravidly a příslušným vnitřním řádem poskytovatele zdravotních služeb. Pro všechny osoby, bez rozdílu jejich společenské významnosti či jiného skupinového odlišení, platí stejná pravidla.

V daném kontextu lze konfrontovat současnou právní úpravu návštěv pacientů na praktickém příkladu návštěvy bývalého prezidenta republiky na lůžku jednotky intenzivní péče ÚVN dne 14.10.2021 předsedou Poslanecké sněmovny Parlamentu České republiky, kancléřem Kanceláře prezidenta České republiky a 4 dalšími osobami, bez vědomí ošetřujícího lékaře. V nastíněném kontextu a ve světle již veřejně známých informací[92] lze onu návštěvu hodnotit nejen jako porušení platných hygienicko-epidemiologických opatření, ale také jako porušení rovného přístupu k právům pacientů. Je otázkou, do jaké míry by za toto porušení a diskriminaci bylo systémově odpovědné zdravotnické zařízení, pakliže by zmíněné osoby navštívili prezidenta díky vpuštění příslušníkem Ochranné služby PČR pod tíhou jejich významnosti nebo dokonce na základě jejich pokynu. Taková situace by byla flagrantním porušením demokratických práv a svobod zakotvených v ústavním pořádku České republiky inklinující k naplnění skutkové podstaty některého z trestných činů. Jelikož se tato úvaha nepodařila prokázat a nebyla nikterak potvrzena, jedná se pouze o hypotetickou domněnku podněcující možné další vědecké úvahy a dále jde o ilustrativní příklad rozšiřující oblasti možných scénářů chování „VIP návštěvy“, na které by personál poskytovatele zdravotních služeb měl být ovšem také připraven a vyškolen.

Zmíněná konkrétní návštěva však podnítila vznik právní otázky automatického umožnění přístupu „VIP návštěvy“ k lůžku pacienta. Dojde-li k pominutí faktu, že byl prezident hospitalizován na tzv. JIP lůžku, kde je již sám o sobě nastaven přísný režim návštěv, v době

trvající tzv. „covidové“ pandemie, je zcela standardní, že při návštěvě jakéhokoliv pacienta je primárně respektováno přání a vůle pacienta. Standardně se tedy jakákoliv návštěva ohlásí nejprve službu konajícímu lékaři, případně jinému odpovědnému zdravotnímu pracovníkovi, který se poté dotáže pacienta, zdali si přeje návštěvu vidět a setkat se s ní. Teprve po vyjádření jeho souhlasu je návštěva vpuštěna na dané oddělení, pokud je to ale vůbec možné například s ohledem na aktuálně platná protiepidemiologická opatření daného poskytovatele zdravotních služeb či jeho vnitřní řád.

Dle mediálních výstupů ovšem dne 14.10.2021 nastala situace, kdy jeden z členů zmíněné návštěvy využil již dříve uděleného souhlasu navštěvovat prezidenta a v době, kdy neměl souhlas ošetřujícího lékaře, zorganizoval návštěvu ostatních výše zmíněných osob. Je otázkou, zda prezident dokázal v té době vnímat naplno jejich přítomnost a zda vyslovil předem souhlas s jejich návštěvou, nicméně se jedná o situaci, na kterou měla efektivně zareagovat ochranka prezidenta a tyto osoby zde bez formálního potvrzení oprávněnosti návštěvy ošetřujícím lékařem nevpustit.

Žádná osoba v postavení „VIP návštěvy“, byť vysoký ústavní činitel, nemá právo postupovat mimo rámec vymezených pravidel daného zdravotnického zařízení, či si dokonce vynucovat návštěvu, byť je účel jeho návštěvy pracovní a může mít dopad na chod celého státu, fungování vlády, podniků atd. Pro daný postup totiž, dle názoru autora práce, neexistuje v demokratickém právním státu legitimní oprávnění.[85]

Z opačného úhlu pohledu může být dalším specifikem „VIP návštěvy“ rovněž její ochranka, a to v několika směrech. Tím prvním je její samotná přítomnost ve zdravotnickém zařízení, obdobně, jako je tomu při jejím působení při ochraně hospitalizované chráněné osoby. Ačkoliv má každý poskytovatel zdravotních služeb jasně vymezena pravidla pro poskytování návštěv opírající se o právní předpisy, svou samotnou přítomností a doprovodem „VIP návštěvy“ narušují členové ochranky chod daného zdravotnického zařízení, potažmo konkrétního oddělení.

Z pozice zdravotnického zařízení by měla být vyžadována naprosto stejná režimová a bezpečnostní opatření vůči každému z členů ochranky, stejně tak, jako by měla být vyžadována vůči „VIP návštěvě“. V daném případu se může jednat například o prokázání se negativním testem na přítomnost onemocnění COVID-19, očkovacím certifikátem, ale také požadavek na nasazení osobních ochranných prostředků či zvláště problematické vypnutí

mobilních telefonů a ostatních elektronických zařízení, která by mohla rušit provoz zdravotnické techniky. Záleží tedy na každé jednotlivé návštěvě, jejím charakteru, potřebnosti, významu chráněné osoby v podobě „VIP návštěvy“, kdy je nezbytné, aby výše nastíněné otázky byly opět předem konzultovány jak s ošetřujícím lékařem pacienta, tak ale s managementem zdravotnického zařízení či jeho bezpečnostním ředitelem.

Lze se domnívat, že správnou koordinací poskytování zdravotní péče zdravotnického zařízení a činností ochranky lze „VIP návštěvu“ uskutečnit. Tento pohled není ryze provozní, ale rovněž právní, kdy za zmíněného předpokladu akceptace vzájemných pravidel a při souhlasu pacienta s uskutečněním návštěvy, se na půdě zdravotnického zařízení opět snoubí několik právních rovin. Toto jejich souznění ovšem vytvoří tzv. průsečík *lege artis*, ve kterém se mohou jejich jednotliví představitelé pohybovat bez nutnosti porušení právních předpisů či vnitřních předpisů. Samotný střed průsečíku pak dle názoru autora práce legitimním způsobem umožňuje uskutečnit „VIP návštěvu“ i za situace, která může navenek mylně evokovat porušení některého z pravidel.

Nastíněná legitimnost lze ovšem dle autora práce zdůvodnit vždy pouze nutností ochrany života a zdraví „VIP návštěvy“ ze strany její ochranky, a nikoliv jakýmikoliv partikulárními zájmy chráněné osoby nebo navštěvované chráněné osoby. Mimo rámec zachování neporušenosti života a zdraví „VIP návštěvy“ nelze ze strany zdravotnického zařízení přistoupit na odklonění se od systémových pravidel, či dokonce k jejich porušení.[93] Jednalo by se do jisté míry o upřednostnění daného pacienta či jeho „VIP návštěvy“ a diskriminaci všech ostatních pacientů a jejich návštěv. Stejná úvaha je zcela jistě aplikovatelná opačně ve vztahu chráněné osoby a jeho návštěv.

Poskytovateli zdravotních služeb, ať už se jedná o státní příspěvkovou organizaci či akciovou společnost zřízenou krajem, totiž nepřísluší jakkoliv hodnotit například významnost pacienta či jeho návštěvy, jejich ústavní povinnosti atd. Nejedná se o orgán veřejné moci či naopak soukromý subjekt, který by byl povinován určitými povinnostmi vůči představitelům státní moci. Naopak, jeho činnost *de lege* vždy směřuje k poskytování kvalitní zdravotní péče pacientovi tedy určitého slušného minima zdravotní péče[23].

[23] Blíže viz kap. 2.2.

2.7 Virtuální hospitalizace

Proces hospitalizace chráněných osob, zejména v kontextu současných vojenských operací, začíná již na bojišti v okamžiku zranění vojáka. V moderních konfliktech, kde je bojiště dynamické a evakuace často komplikovaná, je nezbytné okamžitě přenášet zdravotní data zraněného do zdravotnického zařízení vyšší úrovně péče (tzv. Role 4[24]). Toto zdravotnické zařízení musí být připraveno na jeho hospitalizaci a na poskytování potřebné péče v reálném čase prostřednictvím telemedicíny nebo virtuálních konsilií. Moderní technologie umožňuje, aby zdravotnický personál na dálku sledoval zdravotní stav pacienta, poskytoval rady první pomoci a připravoval vše potřebné pro přijetí pacienta do zdravotnického zařízení, jakmile bude jeho evakuace možná. Virtuální hospitalizace tak zajišťuje kontinuitu péče od okamžiku zranění až po kompletní zotavení pacienta.

Virtuální hospitalizace představuje revoluční přístup k poskytování zdravotní péče, který využívá moderní technologie k poskytování lékařských služeb na dálku. Tento model zdravotní péče se stává stále více rozšířeným, zejména díky pokrokům v telemedicíně, IoT, umělé inteligenci[25] a zabezpečeném přenosu dat. Virtuální hospitalizace umožňuje pacientům zůstat nejen v pohodlí domova, zatímco jsou monitorováni a léčeni zdravotnickými profesionály prostřednictvím digitálních platforem, ale naopak je možné její využití i v podmínkách bojiště, kdy raněného vojáka (chráněnou osobu) není možné transportovat či evakuovat.

Virtuální hospitalizace využívá technologie pro monitorování, diagnostiku a léčbu pacientů na dálku. Klíčovým prvkem tohoto modelu je telemedicína, která zahrnuje videokonzultace, vzdálené monitorování vitálních funkcí a elektronické zdravotní záznamy. Pacienti jsou vybaveni zařízeními, která umožňují sledování jejich zdravotního stavu v reálném čase, a lékaři mohou poskytovat péči a intervence na dálku. Tento přístup nejen zvyšuje pohodlí pacientů, ale také snižuje zátěž na zdravotnické zařízení a zdravotnický personál.[94, 95]

---

[24] V rámci vojenské zdravotnické péče jsou definovány různé úrovně zdravotnického zabezpečení, známé jako Role 1 až Role 4. Tyto úrovně označují různé fáze a typy péče, které jsou poskytovány v polních podmínkách nebo v rámci vojenských operací. Každá z těchto rolí nabízí jiný stupeň odbornosti a vybavení.

[25] Umělá inteligence (dále jen „umělá inteligence“ či „AI“) je obor informatiky zaměřený na vytváření systémů a strojů, které mohou vykonávat úkoly vyžadující lidskou inteligenci, jako je rozpoznávání řeči, rozhodování, učení se, řešení problémů a zpracování přirozeného jazyka. AI se snaží simulovat kognitivní funkce, jako je myšlení a učení, pomocí algoritmů a dat, což umožňuje počítačům vykonávat činnosti autonomně nebo na základě předchozí zkušenosti.

Jedním z hlavních přínosů virtuální hospitalizace je snížení nákladů na zdravotní péči. Virtuální péče eliminuje potřebu fyzického přijetí do zdravotnického zařízení, což snižuje náklady spojené s hospitalizací, jako jsou náklady na lůžka, stravu a další služby[96]. Dalším přínosem je zlepšení dostupnosti zdravotní péče. Pacienti v odlehlých nebo nedostatečně obsluhovaných oblastech mají přístup k odborné lékařské péči bez nutnosti cestování. To je obzvláště důležité pro starší pacienty a osoby s chronickými nemocemi[97] a zejména tedy pro chráněné osoby na bojišti či v oblastech, kde jim není možné zajistit zdravotní služby.

Virtuální hospitalizace také zvyšuje efektivitu a kvalitu péče. Díky neustálému monitorování vitálních funkcí mohou lékaři rychle reagovat na změny zdravotního stavu pacientů a předejít tak závažným komplikacím. Studie ukazují, že pacienti, kteří podstoupili virtuální hospitalizaci, měli nižší míru rehospitalizace a lepší zdravotní výsledky ve srovnání s tradiční hospitalizací.[98, 99]

Navzdory mnoha výhodám čelí virtuální hospitalizace několika výzvám. Jednou z hlavních překážek je technologická dostupnost a konektivita. Virtuální péče vyžaduje spolehlivý přístup k internetu a moderní zařízení, což může být problémem v některých regionech.[100] Další výzvou je zabezpečení a ochrana osobních údajů. Zdravotní data jsou citlivá a jejich přenos musí být chráněn před neoprávněným přístupem a kybernetickými útoky.[101] Navíc existují obavy ohledně kvality péče a osobního kontaktu mezi lékaři a pacienty. Někteří odborníci argumentují, že virtuální péče nemůže plně nahradit fyzické vyšetření a osobní interakci, která je klíčová pro diagnostiku a léčbu některých onemocnění.[102] Dále je třeba řešit otázky legislativy a regulace, aby byla zajištěna kvalita a bezpečnost virtuální péče.[103]

Budoucnost virtuální hospitalizace je slibná, zejména díky pokračujícímu technologickému pokroku a rostoucímu přijetí digitální zdravotní péče. Vývoj v oblasti umělé inteligence, strojového učení a pokročilých biosenzorů umožní ještě přesnější a personalizovanější péči. Integrace těchto technologií do zdravotnických systémů povede k lepším zdravotním výsledkům a efektivitě péče, což je možné aplikovat rovněž ve prospěch virtuální hospitalizace chráněných osob.[104]

Další významný vývoj lze očekávat v oblasti interoperabilních zdravotních systémů, které umožní sdílení zdravotních dat mezi různými poskytovateli zdravotní péče. To zlepší kontinuitu péče a umožní komplexnější sledování pacientů. Navíc se očekává, že pokroky v oblasti

telemedicíny a virtuální reality přinesou nové možnosti pro rehabilitaci a terapeutické intervence.[105]

Virtuální hospitalizace představuje významnou inovaci v poskytování zdravotní péče, která využívá moderní technologie k zajištění efektivní, dostupné a kvalitní péče. Přestože čelí několika výzvám, její potenciál pro transformaci zdravotnictví je značný. Budoucí vývoj technologií a legislativních rámců bude klíčový pro plné využití potenciálu virtuální hospitalizace. Tento přístup nejen zvyšuje pohodlí pacientů, ale také snižuje náklady na zdravotní péči a zlepšuje zdravotní výsledky, což přináší výhody jak pro pacienty, tak pro zdravotnické systémy jako celek.

2.7.1 Virtuální hospitalizace chráněných osob – válečná medicína

Již Napoleon Bonaparte si uvědomoval, že když velitelé přesunou polní nemocnice do první linie vojsk, vyhlašují tím svůj úmysl přijmout ztráty a rovněž úmysl bojovat. Dnes, s moderními technologiemi, může být tato blízkost zajištěna virtuálně. Při zranění vojáka na bojišti se jeho zdravotní data okamžitě přenášejí do zdravotnického zařízení vyšší úrovně péče, která je připravena poskytnout lékařskou pomoc na dálku.[106]

Válečné prostředí Ukrajiny vedlo k významnému posunu v pojetí a realizaci válečné medicíny, což bylo způsobeno vysokým počtem raněných a specifickými podmínkami bojiště, včetně rozsáhlého nasazení dělostřelectva a obtížemi s evakuací raněných. Nedostatky v přípravě a výcviku vojáků v poskytování první pomoci, spolu s intenzivním použitím dělostřelectva znemožňující bezpečnou evakuaci, vedly ke značným ztrátám.[107] To vše zvýšilo tlak na zdravotnické jednotky, jejich vybavení a implementaci nových postupů, včetně úplné digitalizace armádních zdravotnických procesů a kvalitního výcviku bojových zdravotníků.[108]

Změny ve vedení války vyžadují adaptaci nových strategií válečné medicíny, umožňující efektivně čelit novým výzvám. Klíčová je schopnost reakce na širší spektrum hrozeb a schopnost zajistit rychlou a efektivní péči.[109] Rychlá zacílení pomocí dronů a pokročilé technologie znamenají, že válečná medicína musí být nejen mobilní a flexibilní, ale také vybavená pro čelení sofistikovaným útokům, které mohou nečekaně změnit dynamiku na bojišti.[110]

V červenci 2022 publikoval časopis *Royal United Services Institute Journal* článek s názvem *„Jste nejslabším článkem: limity britských obranných lékařských schopností“*.[111] Tento

článek konstatoval, že válka na Ukrajině jasně poukázala na nedostatky a stagnaci ve vývoji vojenských lékařských schopností pro boj, které narostly během 30leté mírové doby po studené válce. Poznatky z války vyjadřují urgentní potřebu restrukturalizace spojeneckých válečných zdravotnických služeb[112], s čímž souvisí i operace na odstrašení ruské agrese a předcházení válce.[113] Díky těmto poznatkům lze získat prostor pro řešení nedostatků v kolektivních lékařských schopnostech aliance NATO a přijmout odpovídající nápravná opatření, která by byla sdílena přímo s alianční komunitou vojenských zdravotníků.[114]

Potřeba revize principů válečné medicíny je posilována opakovaným porušováním mezinárodního humanitárního práva a právních norem regulujících ozbrojené konflikty, zejména ze strany Ruska. Tradičně se předpokládalo, že adherenční principy Ženevských konvencí a uznání symbolu Červeného kříže zajišťují ochranu pro polní nemocnice v mezinárodních konfliktech. Současné konflikty, včetně těch, ve kterých se angažuje Rusko, však ukázaly, že tyto předpoklady nemusí být vždy splněny. Amnesty International[26] v roce 2016 poukázala na systematické a záměrné útoky ruských a syrských vládních sil na zdravotnická zařízení v severním Aleppu jako strategii usnadňující postup pozemních sil.[115] V důsledku těchto dlouhodobých konfliktů byli zdravotníci nuceni ukrývat se v podzemí nebo v neoznačených budovách, aby mohli poskytovat péči zraněným.[116]

Na Ukrajině se nyní jasně ukazuje, že mezinárodní konsenzus a stávající právní normy nezajišťují pro zdravotnické jednotky dostatečnou fyzickou ani virtuální ochranu před agresorem, který neuznává zákony ozbrojeného konfliktu ani humanitární principy.[117] Velvyslanec Neil Bush, vedoucí delegace Spojeného království při Organizaci pro bezpečnost a spolupráci v Evropě, v lednu 2023 zdůraznil narůstající počet důkazů o válečných zločinech vůči zdravotnickým objektům páchaných ruskými silami na Ukrajině, včetně útoků na oblasti pod jejich kontrolou.[118] Tyto nepřetržité údery na ukrajinská města a civilní zdravotnickou infrastrukturu mají trvalý humanitární dopad nejen na obyvatelstvo, ale i na raněné vojáky a možnosti jejich ošetření. Již v prvních týdnech invaze byla řada zdravotnických zařízení cílem útoků, často s ničivými následky.[109] Tyto poznatky, spolu se zkušeností Ukrajiny před

[26] Amnesty International je globální nevládní organizace, která se zaměřuje na ochranu lidských práv. Byla založena v roce 1961 a její hlavní misí je boj proti bezpráví, podporování svobody a ochrana lidské důstojnosti po celém světě. Organizace se zabývá dokumentováním porušování lidských práv, obhajobou spravedlnosti a organizováním kampaní na podporu lidských práv. Amnesty International působí v oblastech, jako jsou mučení, trest smrti, nespravedlivé věznění, svoboda projevu a práva migrantů.

počátkem konfliktu, kdy ačkoliv válka byla v médiích a komunikaci s veřejností neustále zmiňována, ukrajinská zdravotnická zařízení nebyla na invazi na systémové úrovni připraveny[119], vedou k rozšíření aplikace principů válečné medicíny také na civilní zdravotnická zařízení, která se v případě vyvolání konfliktu nutně stanou součástí vojenské zdravotnické infrastruktury.

Možným dílčím opatřením v takovém kontextu je přehodnocení operativních postupů ze strany vojenské zdravotní služby včetně zavedení taktiky maskování, klamání a rozptylování. To zahrnuje využití podzemních struktur, jako jsou podzemní parkoviště nebo pohotovostní nemocniční oddělení, pro bezpečné poskytování péče raněným vojákům.[120] Navíc může být nutné implementovat zvýšená opatření protivzdušné a kybernetické obrany pro zdravotnická zařízení umístěná v kritických oblastech, aby se zajistila jejich ochrana před nepřátelskými aktivitami.[120] Jako příklad je možné uvést nutnost reagovat na nepřátelské bezpilotní prostředky, které sledují označená zdravotnická vozidla až k místu extrakce (Role 2), přičemž je mnohdy následně na tuto oblast zaměřeno dělostřelectvo, aby došlo ke zničení či poškození tohoto prostoru a osob zde se nacházejících.[121]

Nejedná se jen o fyzickou bezpečnost vojenských zdravotnických zařízení ve všech rolích, ale také zejména o bezpečnost virtuální. **Navíc zranitelnost vojenských zdravotnických zařízení představuje i jejich elektromagnetický interferenční podpis (EMI)**[122]**, který se vztahuje nejen na místa určená pro velení a řízení, ale i na zdravotnické budovy, čímž funguje jako navigační maják pro nepřátelskou palbu**. Dle plukovníka Samuela L. Frickse, který působil na Ukrajině jako člen pozorovacího týmu ministerstva obrany USA, může být **cokoliv, co je na zemi stabilní déle než sedm minut, zaměřeno nepřítelem.**[121] Pro odhalení tedy není potřeba vizuální sledování. Popsaná situace je jednou ze základních příčin jak vysokých ztrát, tak vzniku potřeby hromadných evakuací a lékařské péče raněným vojákům přímo v poli.

V reakci na uvedené faktory se válečná medicína musí neustále adaptovat a transformovat, aby vyhověla požadavkům moderních konfliktů. Simulace a analýzy některých armád naznačují, že v konfliktech vysoké intenzity, jako je ten na Ukrajině, se role válečné medicíny stává klíčovým faktorem, který může rozhodnout o výsledku střetnutí.[107] Narůstající používání dělostřelectva, protiletadlové obrany a schopností pro údery na dlouhé vzdálenosti limituje možnosti pro rychlou lékařskou evakuaci, což představuje výzvu, s kterou se předchozí konflikty nižší intenzity nesetkávaly.[123] V daném kontextu pak hraje klíčovou roli virtuální

hospitalizace raněných vojáků, která má potenciál významným způsobem pomoci ke snížení počtu jejich úmrtí a zabezpečení efektivní první pomoci.

2.7.2 Přenos zdravotních dat chráněných osob

Tato podkapitola se zaměřuje na analýzu současných možností přenosu zdravotních dat chráněných osob, jejich přínosů, výzev a budoucích perspektiv v kontextu zajištění kvalitní a bezpečné zdravotní péče.

S rozvojem moderních technologií a jejich implementací do zdravotnických systémů se otevírají nové možnosti přenosu zdravotních dat chráněných osob, jako jsou vojáci či ostatní příslušníci ozbrojených sil a bezpečnostních sborů. Efektivní a bezpečný přenos těchto dat je zásadní pro zajištění kontinuity péče, rychlou reakci na zdravotní potřeby a ochranu citlivých informací před neoprávněným přístupem. Využití zmíněných technologií IoT, telemedicíny, AI a pokročilé šifrovací metody umožňuje nejen sledování zdravotního stavu v reálném čase, ale také zabezpečený přenos dat mezi různými úrovněmi zdravotnických zařízení a vojenských jednotek.

Armádní prostředí a krizové situace, jako jsou války a konflikty, historicky působí jako katalyzátory pro vývoj moderních technologií. Tento trend je patrný i v případě současného konfliktu na Ukrajině, kde armáda, vzhledem k výše uvedeným skutečnostem, čelí naléhavé potřebě inovovat a adaptovat technologie ve válečné medicíně tak, aby efektivně reagovala na výzvy spojené s léčbou zranění v bojových podmínkách. Historie ukazuje, že armády již dlouho využívají telemedicínu k překonání geografických a logistických bariér, což jim umožňuje poskytovat kritickou lékařskou péči v nejextrémnějších podmínkách. Prvopočátky využití rádiové telemedicíny zdokumentované armádou mají své kořeny v Austrálii ve Zdravotním vojenském a veteránském centru v Brisbane, kde v roce 1917 lékař J. J. Holland z Perthu telegraficky instruoval poštmistra v Halls Creek, vzdáleném 2900 kilometrů, jak ošetřit vážně zraněného chovatele.[124] Významným krokem ve vývoji telemedicíny obecně byla iniciativa NASA z roku 1989, kdy byl vytvořen americko-sovětský telemost Space Bridge po zemětřesení v Arménii, které způsobilo rozsáhlé škody na zdravotnické infrastruktuře a ztráty na životech.[125] Tento telemost umožnil přenos obrazové dokumentace a poskytnutí konzultační pomoci pacientům, což následně pomohlo i v ruském městě Ufa po tragické železniční nehodě. Telemedicínské spojení zajišťovalo přenos obrazové dokumentace z postižených míst a následnou konzultační činnost amerických vojenských lékařů.[126]

S možností přenosu dat souvisí ve vojenském kontextu také oblast telepsychiatrie a telerehabilitace, zejména na základnách, lodích, polních nemocnicích, ale také přímo na bojišti.[127] Významným přínosem telemedicíny je její schopnost poskytovat rehabilitační podporu zraněným vojákům a civilistům z válečných zón, jak bylo demonstrováno ve Spojených státech amerických, kde se telerehabilitace rozvinula především ve vojenské medicíně.[125] Tento přístup v kontextu dnešní doby ilustruje klíčovou roli telemedicíny v rychlém a efektivním poskytování lékařské péče v extrémních situacích, přičemž její využití v armádě a v reakci na válečný konflikt na Ukrajině nabízí příslib lepších výsledků léčby a záchranu více životů. Virtuální hospitalizace vojáků a poskytování zdravotních služeb v online prostředí tím nabývá na významu nejen v době míru, ale zejména v době krize.

Na příkladu Ukrajiny lze demonstrovat možnosti implementace virtuální hospitalizace vojáků. Základem pro implementaci vojenské telemedicíny přímo na Ukrajině je vývoj koordinovaného národního zdravotnického evakuačního systému a registru traumat, které by zlepšily jak dobu evakuace, tak zejména klinickou komunikaci.[128] Vývoj a využití takových systémů umožní kritické zlepšení traumatologického systému Ukrajiny a bude sloužit jako informační páteř pro zlepšování procesů všech systémů v rámci celého systému. Registr traumat je základem citlivého a dynamického traumatologického systému, který na Ukrajině chybí, a který shromažďuje informace týkající se úrazové události, zranění, péče a výsledků v celém kontinuu péče o traumata. Získané údaje umožňují systematickou analýzu vedoucí k průběžnému zlepšování kvality, alokaci zdrojů a změně postupů válečné medicíny obecně.[129] Ukrajina v současné době vyvíjí modifikované elektronické systémy a nástroje týkající se kompletní elektronizace jejich zdravotnictví s vazbou právě na probíhající ozbrojený konflikt. Zkoumá, jaké přístupy, politiky, standardy péče a pokyny jsou nezbytné k posílení systému traumatologické péče kromě registru traumat. Od začátku války se ministerstvo zdravotnictví zabývalo nastavením zdravotní péče pomocí světových standardů medicíny katastrof, nicméně se rozhodlo samo vyvinout vlastní traumatologický systém, který by vyhovoval jejich potřebám a omezením.[130, 131]

Důležitou otázkou je rovněž možnost využití již dostupných komunikačních a šifrovacích prostředků nevojenského sektoru, jako jsou například civilní mobilní aplikace.[132] Potenciál využití těchto prostředků byl potvrzen jejich využitím na Ukrajině, kde byly využívány pro přednemocniční péči, vzdálené sledování pacientů a také pro zlepšení standardizovaných formulářů.[128] Zásadním předpokladem pro využití již existujících technologií a systému

civilního sektoru pro účely virtuální vojenské medicíny je jejich využití **pouze pokud jimi využívaný digitální signál nepředstavuje potenciální cíl pro útok**.[114, 133] Dalším nutným opatřením pro implementaci těchto systémů bude např. i potlačení předávání geolokačních a kontaktních údajů jiným, než autorizovaným subjektům. Tento krok byl již například na Ukrajině učiněn v rámci všech elektronických zdravotních záznamů.[134] Přijetí opatření k odstranění zeměpisných a kontaktních údajů lékařů, vojáků a všech ostatních uživatelů zmíněného systému je zásadní pro zajištění optimální kybernetické bezpečnosti. Významným poznatkem z bojů na Ukrajině je implementace již zmíněné telemedicíny, která je využívána mezi civilisty pro primární péči, nicméně její role pro traumatologickou péči byla výrazně omezena, a to z důvodů jazykových bariér, nedostatečné technologické infrastruktury a zejména přetrvávajících obav o zajištění kybernetické bezpečnosti.[135, 136]

Pro zajištění přenosu dat a informací o chráněných osobách (příslušnících ozbrojených sil) napříč různými platformami a jednotkami je nezbytné ze strany aliančních armád vytvořit a dodržovat standardy interoperability. Tyto standardy v budoucnu umožní, obdobně jako v civilním sektoru, integraci systémů od různých výrobců a zajistí, že data mohou být efektivně sdílena a používána všemi relevantními stranami, jak v rámci vojenského sektoru, tak v civilním zdravotnictví, pokud to bude potřeba.

2.7.3 Cloudové řešení přenosu a zabezpečení pacientských dat chráněných osob

V éře digitální transformace zdravotní péče hraje cloudové řešení klíčovou roli při přenosu a zabezpečení pacientských dat chráněných osob. Integrace cloudových technologií do procesu virtuální hospitalizace umožňuje efektivní ukládání, sdílení a zpracování velkého objemu dat, což je zásadní pro zajištění nepřetržité zdravotní péče a rychlé reakce na zdravotní potřeby v terénu. Virtuální hospitalizace, která zahrnuje monitorování pacientů na dálku, videokonzultace a vzdálené diagnostické služby, se stává stále více závislou na spolehlivých cloudových řešeních. Bezpečnost těchto dat je však stejně důležitá jako jejich dostupnost, což vyžaduje implementaci robustních šifrovacích metod, autentizačních protokolů a pravidel pro řízení přístupu. Tato podkapitola se zaměřuje na analýzu cloudových řešení pro přenos a zabezpečení pacientských dat chráněných osob v procesu virtuální hospitalizace, jejich přínosů, výzev a budoucích perspektiv v kontextu moderní medicíny.

Značným vývojem v rámci akceptace cloudového řešení pro uchování a přenos zdravotnických dat již prošly i některé členské státy EU.

Zde v kontextu problematiky disertační práce a stále se rozvíjejícího pole válečné medicíny hraje klíčovou roli rychlé a bezpečné shromažďování, zpracování a distribuce dat a informací. Studie *„Cloud Intelligence for Decision Support and Analysis"* (dále jen „CLAUDIA"), financovaná Evropskou obrannou agenturou (dále jen „EDA")[27], odhalila zásadní přínosy *cloud computingu*[28], který lze aplikovat i na popsaný model virtuální hospitalizace chráněných osob. Cloudové technologie, které zahrnují výpočetní kapacity, ukládání dat a softwarové nástroje hostované externě, nabízí strategickou i taktickou výhodu. Platforma s názvem SWAN, vyvinutá projektem CLAUDIA, demonstruje schopnost cloudů podporovat taktické i strategické vojenské rozhodování nejen pro oblast vojenské medicíny, ale zejména pro lepší situační povědomí a zkrácení reakčních časů v různých operačních prostředích, a to pomocí virtualizace, která umožňuje vytváření virtuálních verzí serverů, úložišť a sítí.[137] EDA tedy hraje rozhodující roli ve vývoji obranných schopností členských států EU a v oblasti válečné medicíny podporuje iniciativy, jako je cloudové výpočetnictví, které usnadňují přeshraniční spolupráci a využití sdílených zdrojů, což je neocenitelné v situacích, kdy nemusí být možné zabezpečit včasnou evakuaci raněných chráněných osob. Využití telemedicíny a virtuálních konsilií v tomto prostředí je zásadní, umožňuje vysokou úroveň kvality lékařské péče bez ohledu na fyzickou vzdálenost od specializovaných zdravotnických zařízení.[138]

Evropský zdravotnický datový prostor[29][139] nabízí dále příležitosti pro vytvoření speciálního virtuálního prostoru pro bezpečné ukládání citlivých dat a informací vojáků členských armád EU. Tento prostor, respektující principy definované GDPR a směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních pro vysokou společnou úroveň

---

[27] Evropská obranná agentura (EDA) je agentura Evropské unie, která byla zřízena v roce 2004 s cílem podporovat spolupráci mezi členskými státy EU v oblasti obrany a bezpečnosti. Jejím hlavním úkolem je zlepšovat vojenské schopnosti členských států, podporovat výzkum a vývoj v oblasti obranných technologií, harmonizovat obranné politiky a usnadňovat spolupráci při nákupu vojenského vybavení. EDA také napomáhá efektivnějšímu využívání obranných zdrojů a zajišťuje koordinaci mezi členskými státy při řešení společných bezpečnostních výzev.

[28] Cloud computing je technologie, která umožňuje přístup k výpočetním zdrojům (jako jsou servery, úložiště dat, databáze, sítě, software a analytické nástroje) přes internet. Tyto zdroje jsou poskytovány vzdálenými datovými centry spravovanými poskytovateli cloudových služeb, což uživatelům umožňuje využívat výpočetní výkon a ukládat data bez nutnosti vlastnit fyzický hardware. Hlavní výhodou cloud computingu je flexibilita, škálovatelnost a úspora nákladů, protože uživatelé platí pouze za to, co skutečně používají, a mají přístup k těmto zdrojům odkudkoliv, kde je internetové připojení.

[29] Evropský zdravotnický datový prostor (dále jen „EHDS") je iniciativa Evropské unie, která má za cíl vytvořit jednotný prostor pro sdílení a využívání zdravotnických dat napříč členskými státy EU. EHDS usiluje o podporu lepší spolupráce mezi zdravotnickými systémy, zajištění bezpečného přístupu ke zdravotním informacím pro pacienty a zdravotníky a podpořit výzkum a inovace v oblasti zdravotní péče.

kybernetické bezpečnosti v celé Unii, o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148[30], představuje ekosystém, který je specificky navržen pro zdravotní oblast, skládající se z pravidel, společných norem a infrastruktur. Jeho primárním cílem je posílení postavení jednotlivců tím, že jim umožní lepší kontrolu nad jejich zdravotními údaji, a zároveň zajišťuje vysokou úroveň ochrany dat a soukromí.[140] Tato struktura by mohla být speciálně upravena tak, aby vytvořila izolovaný a zabezpečený segment pro účely využití v rámci hospitalizace chráněných osob, kde přístup mají pouze autorizované osoby se speciálními šifrovacími klíči, což zajistí, že přístupy k pacientským datům chráněných osob v citlivých a nebezpečných prostředích zůstanou chráněny.

Význam EHDS nejen pro vojenské zdravotní informační systémy, ale i systémy obsahující moduly pro hospitalizaci chráněných osob obecně, se dále prohlubuje integrací technologií umožňujících bezpečnou výměnu, opakované použití a analýzu zdravotních dat nejen pro poskytování zdravotní péče, ale i pro výzkum a inovace.[140] Tento přístup podporuje tvorbu jednotného trhu s elektronickými zdravotními záznamy a příslušnými technologiemi, což umožňuje efektivní spolupráci a interoperabilitu mezi vojenskými a civilními zdravotními systémy různých členských států. Využití EHDS by také umožnilo rychlejší a informovanější rozhodování v oblasti zdravotní péče na základě konkrétních lékařských poznatků, což je klíčové pro zlepšení připravenosti a reakce na krize a situace, kdy bude nutné zabezpečit data a informace chráněných osob tzv. ad hoc. Navíc, vytvořením speciálního segmentu pro chráněné osoby v rámci EHDS by zajistilo, že i v nejvyšším stupni ohrožení budou zdravotní data těchto osob chráněna před kybernetickými hrozbami, což odpovídá požadavkům na kybernetickou bezpečnost dle NIS 2.

2.8 Ochrana osobních údajů

Ochrana osobních údajů ve zdravotnictví je obecně klíčovým aspektem a základním stavebním kamenem moderního zdravotního systému, který si klade za cíl zajištění důvěrnosti, integrity a bezpečnosti citlivých informací týkajících se pacientů. V souvislosti s rychlým technologickým pokrokem a digitalizací zdravotní péče se stává ochrana osobních údajů stěžejním tématem.

[30] Dále jen „NIS2“.

Právo na ochranu osobních údajů je všeobecně rozeznáváno jako součást základního lidského práva na ochranu soukromí[141] a je tedy jedním z osobních práv chráněných Listinou v prvním oddílu druhé hlavy.[142] Samotné právo na ochranu osobních údajů je pak vedle dalších práv na ochranu soukromí v českém právním řádu upraveno zejména v čl. 10 odst. 3 Listiny. Na mezinárodní úrovni neexistuje samostatná úprava ochrany osobních údajů jako základního lidského práva, úpravu však můžeme nalézt v čl. 8 Listiny základních práv EU. Přímá ochrana osobních údajů jako základního lidského práva je relativně novým přístupem, který je typický zejména pro evropský prostor.[143] To dokládá již výše uvedený výčet mezinárodních smluv, které se ochranou osobních údajů zabývají. Jak je vidět, tak na rozdíl od úpravy ochrany soukromí jako takové, je ochrana osobních údajů spíše evropským prvkem. Úpravu ochrany soukromí můžeme nalézt například ve Všeobecné deklaraci lidských práv OSN, Mezinárodním paktu o občanských a politických právech, Evropské úmluvě o ochraně lidských práv a základních svobod, Listině základních práv EU, Americké úmluvě o lidských právech či Arabské chartě lidských práv. Nelze však přehlédnout skutečnost, že ochrana osobních údajů se jako podstatná část vyvinula právě z úpravy soukromí obsažené v mezinárodních smlouvách. K vývoji této úpravy je nutné dále poznamenat, že primárním cílem tohoto institutu byla ochrana jednotlivce před shromažďováním a zpracováním osobních údajů státem bez vědomí dotčeného jednotlivce, tedy zpracování údajů na vertikální úrovni.[144] Postupem času však došlo k rozšíření této úpravy i na úroveň horizontální a dnes jsou již chráněna práva jednotlivce i vůči neoprávněnému zpracování ze strany jiných fyzických či právnických osob.[144]

Osobní údaje ve zdravotnictví zahrnují širokou škálu informací, jako jsou jméno, příjmení, datum narození, pohlaví, adresa, zdravotní diagnózy, léčebné plány, laboratorní výsledky, léčebné záznamy a další vysoce citlivé informace. Tyto údaje jsou klíčové pro poskytování účinné a bezpečné léčby, ale zároveň nesou riziko zneužití, krádeže nebo neoprávněného přístupu.

Základem ochrany osobních údajů ve zdravotnictví je dodržování zásady „*privacy by design*“ (ochrana soukromí již v návrhu). Stručně řečeno, jedná se o takový přístup k ochraně soukromí, který zahrnuje zakotvení zásad ochrany soukromí již do návrhů různých technologií či situací. Jinými slovy, jde o uplatňování požadavků souvisejících s ochranou osobních údajů co nejdříve od počátečních fází existence technologických novinek. Původně se tento přístup aplikoval

skutečně především na vývoj nových technologií, časem se však rozšířil také například na oblast obchodních postupů a dalších oblastí.[145]

Další klíčovou zásadou je „nejmenší nezbytný zásah“ (*least privilege*), což znamená, že pouze oprávnění osobě by měly mít přístup k nezbytným informacím, které jsou potřebné pro poskytování lékařské péče. Lékaři a zdravotní pracovníci by měli mít přístup pouze k údajům pacientů, se kterými přímo pracují.[146]

Mezinárodní úmluvy, právo EU, zákony a další právní předpisy stanovují povinnosti a zodpovědnost za ochranu osobních údajů ve zdravotnictví. Zdravotnické instituce musí zajistit, že mají dostatečné technické a organizační opatření na ochranu dat a že jsou dodržovány všechny povinnosti týkající se informovaného souhlasu pacientů.

Existuje již celá řada kontrolních mechanismů, které je v případě incidentu s únikem nebo narušením osobních údajů nutné okamžitě podniknout. Jedná se například o kroky pro řešení situace a informování dotčené osoby včetně dozorového úřadu pro ochranu osobních údajů.

Rovněž vývoj a uplatňování nových technologií, jako je umělá inteligence a analýza velkých dat, přináší nové výzvy pro ochranu osobních údajů ve zdravotnictví. Je třeba zajistit, aby byly tyto technologie náležitě transparentní, etické a v souladu s platnými právními předpisy a normami. Lze deklarovat, že ochrana osobních údajů ve zdravotnictví je nezbytnou součástí důvěryhodného a bezpečného zdravotního systému. Dodržování zásad „*privacy by design*“ a „nejmenší nezbytný zásah“, dodržování příslušných právních předpisů a vyvíjení odpovídajících technických opatření jsou klíčové pro zajištění ochrany citlivých informací pacientů a udržení jejich důvěry ve zdravotní péči.

2.8.1 Ochrana osobních údajů v prostředí poskytovatele zdravotních služeb

Česká republika již dlouhou řadu let určuje právní rámec nakládání s osobními údaji pacientů a jejich zákonných zástupců, ať už jde o „standardní“ osobní údaje, jako je jméno, příjmení, adresa, e-mail nebo číslo telefonu, nebo o citlivé osobní údaje, to znamená ve zdravotnictví zejména informace o nemoci a průběhu i výsledcích léčby.[147]

V květnu 2018 vstoupilo v účinnost nařízení GDPR, které ukládá konkrétní povinnosti správcům osobních údajů a přineslo některá nová práva subjektům osobních údajů. Kontrola dodržování GDPR je v ČR v rukou Úřadu pro ochranu osobních údajů. V návaznosti na GDPR byl přijat o zpracování osobních údajů. V oblasti zdravotnictví přinesl, obdobně, jak je uvedeno

výše u GDPR, nové povinnosti správcům osobních údajů, jimiž jsou všichni poskytovatelé zdravotních služeb, tj. jak velká zdravotnická zařízení, tak ambulantní poskytovatelé zdravotních služeb. Došlo rovněž k zásadnímu rozšíření práv pacientů.

Nařízení GDPR ve zdravotnictví doplňuje jiné právní předpisy (např. zákon o zdravotních službách a vyhlášku o zdravotnické dokumentaci) nebo i jiné důležité dokumenty jako jsou akreditační standardy, kterými zdravotnické zařízení prokazuje kvalitu a bezpečí prováděné péče[31]. Nařízení GDPR nestanovuje povinnost všeobecného utajování a vymazávání osobních údajů, taktéž nelze na základě tohoto nařízení a priori odmítnout poskytnutí některých osobních údajů lékaři, či odmítnout nošení identifikačních náramků apod.

Zdravotníci v kontextu zákona o zdravotních službách a vyhlášce o zdravotnické dokumentaci velmi pečlivě zvažují, které osobní údaje pacientů jsou pro prevenci i léčbu potřebné. Na druhou stranu je v zájmu každého pacienta přesně a úplně takové osobní údaje poskytnout. Poskytnout příslušné údaje pacientovi ukládají české právní předpisy, viz § 52 a násl. zákona o zdravotních službách[29], Zdravotníci jsou v souladu s příslušnými pracovně[148] či služebně právními předpisy[149], kterými jsou jednotliví poskytovatelé zdravotních služeb vázáni, pravidelně školeni. Dle příslušné pracovní pozice pak musí být tedy zaměstnanci poskytovatele zdravotních služeb proškoleni například jak s osobními údaji pracovat, a to nejen z hlediska mlčenlivosti, ale i z hlediska délky jejich evidování, z hlediska jejich ochrany v počítačích, sdílení, zasílání elektronickou formou, zabezpečením apod.

Nařízení GDPR přineslo některá nová práva pro pacienty a zákonné zástupce, ale jejich aplikace ve zdravotnictví má s ohledem na speciální právní úpravu v zákoně o zdravotních službách určité limity, mezi které lze zařadit:

- Pacient má právo vědět, jaké osobní údaje (ať už získané se souhlasem nebo bez souhlasu subjektu údajů) a jak je poskytovatel zdravotních služeb zpracovává. To je možné zjistit z webových stránek nebo přímým dotazem směřovaným na poskytovatele zdravotních služeb.

[31] Mezi relevantní standardy patří například akreditační standardy pro nemocnice, ambulantní zařízení nebo záchranné služby, které jsou spravovány organizacemi, jako je **Spojená akreditační komise, o.p.s. (SAK)** a **EuroCert**. Na světové úrovni existují významné akreditační organizace, jako například **Joint Commission International (JCI)**, která poskytuje akreditace zdravotnickým zařízením po celém světě, a **DNV GL Healthcare**, která nabízí certifikace založené na mezinárodních standardech ISO a zaměřuje se na zlepšení kvality a bezpečnosti pacientů.

- Pacient má právo na přístup k osobním údajům.
- Pokud se zjistí chyba nebo neúplnost v osobních údajích pacienta, má právo na to, aby poskytovatel provedl bez zbytečného odkladu opravu nebo doplnění neúplných osobních údajů. Opravy ve zdravotnické dokumentaci se řídí speciální úpravou v zákoně o zdravotních službách.
- Právo na výmaz nebo jinak řečeno „právo být zapomenut“. Toto právo je ve zdravotnictví z pochopitelných důvodů velmi omezeno, neboť oprávnění zpracovávat osobní údaje, včetně délky doby, po kterou mohou být zpracovány v souvislosti s poskytováním zdravotních služeb nebo pro statistické účely, vyplývá ze zákona o zdravotních službách a z vyhlášky o zdravotnické dokumentaci. Je ale v zájmu pacienta, aby byla jeho zdravotnická dokumentace kompletní a dalo se z ní vycházet pro další léčbu a řešit pomocí ní i třeba vypořádání domnělých nebo skutečných pochybení personálu.
- Další práva – právo na omezení zpracování, oznamovací povinnost ohledně výmazu nebo opravy, právo na přenositelnost, právo na vznesení námitky, právo, aby subjekt údajů nebyl předmětem automatizovaného rozhodování včetně profilování, právo na podání stížnosti u dozorového úřadu, právo na účinnou soudní ochranu vůči dozorovému úřadu nebo správci, právo být zastoupen neziskovým subjektem, organizací nebo a právo na náhradu újmy aj.[146]

U každého poskytovatele zdravotních služeb musí být určena osoba, která za zpracování osobních údajů odpovídá. Ve zdravotnických zařízeních je ze zákona ustavena i speciální funkce pověřence pro ochranu osobních údajů, který se GDPR profesionálně zabývá a který má jasně vymezené kompetence a pracovní náplň. Kontakt na něj je zpravidla uveden na webových stránkách.[150]

Významný legislativní rámec tvoří též čl. 10 odst. 3 Listiny, který poskytuje každému právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě. K tomuto právu pak Ústavní soud v bodě 29 plenárního nálezu, sp. zn. Pl. ÚS 24/10, dovodil, že kromě výše zmíněného **právo na soukromí garantuje jednotlivci možnost rozhodnout, zda a případně v jakém rozsahu a jakým způsobem své osobní informace zpřístupní jiným subjektům**. Zásadní je v uvedeném kontextu shodný nález Ústavního soudu sp. zn. I.ÚS 512/02 (N 143/28 SbNU 271)[151], ve kterém tuto skutečnost dovodil rovněž vůči orgánům státní správy, tedy i poskytovatelům zdravotních služeb. Evropský soud pro lidská

práva pak v rozhodnutí Rotaru v. Rumunsko z roku 2000[267] dovodil, že zásahem do lidských práv je neoprávněným shromažďováním také shromažďování veřejně dostupných údajů.

Dílčím, avšak zásadním závěrem této podkapitoly je fakt, že uvedené **osobnostní právo na ochranu osobních údajů, jako takové, však není nedotknutelné a absolutní a může se tedy dostat do konfliktu s jinými lidskými právy. Z toho tedy plyne, že může být také omezeno**. Při střetu s jinou oblastí práva, bude nutné i v tomto případě, stejně jako u jiných základních lidských práv a svobod, provést test proporcionality, na jehož základě musí dojít ke zvážení, zdali je takový zásah ústavně konformní či nikoliv – zda je daný postup *lege artis*.[141] Dle názoru autora práce je právě test proporcionality zásadním nástrojem pro správnou aplikaci konkrétních opatření v případě zajištění ochrany dat a informací o chráněných osobách.

2.8.2 Ochrana osobních údajů chráněných osob

Ochrana osobních údajů chráněných osob má zvláštní význam, protože tyto osoby často čelí zvýšenému riziku ohrožení a nebezpečí zneužití svých osobních informací. Mezi specifika ochrany osobních údajů chráněných osob patří požadavek na přísnější ochranu jejich soukromí. **Chráněné osobnosti explicitně nemají právo na zvýšenou ochranu soukromí, nicméně, z hlediska zajištění jejich bezpečnosti je tento požadavek zcela zásadní**. Veřejný přístup k jejich osobním informacím by měl být z bezpečnostního hlediska omezen až na minimum. Zpracování a šíření jejich osobních údajů by mělo být prováděno pouze v souladu s příslušnými zákony a s vědomím institucí, které zajišťují jejich bezpečnost.[152]

V kontextu prostředí poskytovatele zdravotních služeb vzniká požadavek rovněž na omezený přístup k jejich datům a informacím. Pouze omezený počet oprávněných osob by měl mít přístup k osobním údajům chráněných osob. Tato opatření by měla být důsledně dodržována a monitorována, aby se minimalizovalo riziko úniku nebo neoprávněného přístupu k citlivým informacím.

Dále pak pro zajištění bezpečnosti osobních údajů chráněných osob mohou být uplatňována přísná bezpečnostní opatření. To zahrnuje používání například šifrování, využívání skryté identity, vícefaktorové autentizace ošetřujících osob a dalších technologií, které brání neoprávněnému přístupu k datům a informacím chráněných osob. Chráněné osoby nebo jejich bezpečnostní týmy mohou rovněž požádat o omezení množství zveřejňovaných informací. To může zahrnovat omezení zveřejňování osobních fotografií, adresy nebo i jiných citlivých údajů.

V rámci ochrany osobních údajů chráněných osob je třeba nastavit specifická opatření v rámci komunikace s chráněnými osobami, která by měla být prováděna s maximální opatrností, aby se minimalizovalo riziko úniku informací o chráněné osobě. To zahrnuje zajištění, že e-maily, textové zprávy a další formy komunikace jsou bezpečné a chráněné.[153]

Zpracování osobních údajů chráněných osob musí být v souladu s platnými právními předpisy a regulacemi týkajícími se ochrany osobních údajů. Je důležité, aby zodpovědné organizace a instituce, které mají přístup k osobním údajům chráněných osob, měly jasně stanovené politiky a postupy pro jejich ochranu a dodržování příslušných právních předpisů. Ochrana osobních údajů by měla být vnímána jako základní právo a zároveň klíčový aspekt zajištění celkové bezpečnosti chráněných osob.

2.8.3 Veřejný zájem na informacích o zdravotním stavu chráněné osoby

Na druhou stranu veřejný zájem na zpracování osobních údajů chráněné osoby je v rovině právní teorie nepochybně zároveň i zájmem takové chráněné osoby, a to bez ohledu na znalost subjektivního vnímání nebo vůle chráněné osoby. Lze tak vyvodit z příkladu hospitalizace prezidenta republiky. Jeho zájem na konformitě zpracování jeho osobních údajů v souladu s ústavním zákonem č. 1/1993 Sb., Ústava české republiky[32] byl proklamován již v jeho ústavním slibu, jehož složení je předpokladem výkonu funkce prezidenta republiky. Slib zahrnuje mimo jiné závazek, že bude zachovávat Ústavu a zákony a že svůj úřad bude zastávat v zájmu všeho lidu. Vyvstala-li by proto potřeba učinit konkrétní kroky vedoucí k naplnění Ústavy, například čl. 66 a zbavení prezidenta republiky výkonu jeho funkce ze zdravotních důvodů, měl by být zájem na jejich provedení u jakékoliv osoby ve funkci prezidenta republiky předpokládán. Z jiného úhlu lze na aktivaci čl. 66 Ústavy nahlížet jako na ochranu ústavní role prezidenta i ochranu osoby, která tuto roli zastává. Tento postřeh vystihl předseda Senátu Miloš Vystrčil svým vyjádřením: „*Článek 66 je ochrana prezidenta jako instituce a ochrana prezidenta jako osoby. To první, aby dál byly konány činnosti, které konány býti musí a to druhé, aby ten, kdo je nemocný, dočasně nemocný, se mohl vyléčit, měl klid, měl zabezpečený citlivý a lidský přístup a poté, co se vyléčí, se znovu mohl vrátit do své pozice.“*[154]

V souvislosti s okolnostmi zpracování osobních údajů chráněné osoby, explicitně prezidenta republiky, lze také zmínit fakt, že ústavní mechanismus zajištění výkonu pravomocí prezidenta

---

[32] Dále jen „Ústava“.

republiky v době jeho neschopnosti jinými ústavními činiteli byl do ústavního zákona včleněn v roce 1975 právě z důvodu vážné nemoci tehdejšího prezidenta Ludvíka Svobody.[155] Záměrem této zmínky v žádném případě není srovnávat situace, nýbrž pouze konstatovat fakt, že zdravotní stav prezidenta republiky jakožto chráněné osoby je zcela jistě jedním z možných závažných důvodů, pro které nemůže prezident vykonávat svůj úřad, a tedy i jedním z důvodů relevantních pro zvážení aplikace pravidla dle citovaného čl. 66 Ústavy.

V uvedeném kontextu lze potvrdit, že osobní údaje v podobě informací o zdravotním stavu prezidenta republiky v době jeho hospitalizace je možné, při dodržení zásad přiměřenosti, předat i bez jeho souhlasu například Senátu Parlamentu České republiky, a to právě za účelem jeho dalšího postupu například ve vztahu k aktivaci čl. 66 Ústavy.

V další rovině veřejného zájmu jakožto právního titulu zpracování osobních údajů chráněné osoby i bez jejího souhlasu lze nad rámec aplikace ústavního pravidla předmětné zpracování obhájit zájmem veřejnosti na informace o prezidentovi republiky, a to v rámci svobody projevu. Ústavní teorie judikovaná nálezem Ústavního soudu IV ÚS 1378/2016[268] i praxe standardně akceptuje, že *„legitimním důvodem pro omezení určitého práva může být prosazení jiného kolidujícího práva anebo určitý veřejný zájem. Právě veřejným zájmem lze legitimovat omezení soukromí jednotlivých osob.“*

Nařízení GDPR v recitálu 153 uvádí, že aby byl zohledněn význam práva na svobodu projevu v každé demokratické společnosti, je třeba vykládat pojmy související s touto svobodou, šířeji.

Dle plenárního nálezu Ústavního soudu č. ÚS 3/14[269] je *„v demokratické společnosti přístup k relevantním informacím obecným předpokladem realizace práva každého na aktivní účast ve veřejném životě na základě rovné participace. Pilířem demokratické společnosti je otevřená diskuze o výkonu veřejné moci a jeho dopadech na jednotlivce.“*.

Soudní dvůr EU v rozsudku ze dne 9. 11. 2010 ve spojených věcech C-92-09 a C-93-09[270] judikoval, že *„právo na ochranu osobních dat není absolutním právem, ale musí být posuzováno ve vztahu k jeho funkci ve společnosti. Velký senát Evropského soudu pro lidská práva konstatoval, že veřejný zájem se vztahuje k věcem, které* ***ovlivňují veřejnost do takové míry, že se o ně může zajímat, které přitahují její pozornost, nebo které se jí týkají do značného stupně, zvláště pokud ovlivňují životní úroveň občanů nebo život společnosti.*** *Je to také případ, když se informace týkající důležité sociální otázky, nebo zahrnují problém, o němž by veřejnost měla být informována.“*

Nejvyšší správní soud České republiky v rozsudku ze dne 22. 10. 2014 č. j. 8 As 55/2012[271] uvedl, že *„na kontrole veřejné moci se může podílet každý, a to přesně v té míře, v jaké se rozhodne být aktivní. Nikdo není vyloučen, každá má možnost se ptát a dozvědět se. To již samo o sobě posiluje vztah veřejné moci a občana, brání rozdělení na „my“ a „oni“ a posiluje vědomí veřejnosti, že veřejná moc není účele o sobě či prostředkem mocných k udržení jejich výsad, odcizeným od občanské společnosti, nýbrž nástrojem občanů, tvořících politickou obec, k prosazování obecných, společně sdílených zájmů a cílů.“*

Zásadním mezníkem v této oblasti je Evropský soud pro lidská práva, který rozsudkem ze dne 18. 5. 2004, č. stížnosti 58148/00[272], ve věci někdejšího prezidenta Francoise Mitteranda vyvodil legitimní zájem veřejnosti znát stav prezidenta, když vyhodnotil, že *„zveřejnění publikace obsahující informace o zdravotním stavu prezidenta bylo v kontextu široké debaty ve Francii ohledně záležitosti veřejného zájmu, zejména práva veřejnosti být informován ohledně jakýchkoliv závažných onemocnění, jimiž trpí hlava státu a otázky, zda osoba, která věděla, že je vážně nemocná je schopna zastávat nejvyšší národní úřad.“*. Veřejnosti tím bylo přiznáno právo na informace o fyzických a mentálních schopnostech čelních představitelů státu, tedy chráněných osob jakožto pacientů.

Názor zastávaný Evropským soudem pro lidská práva na ochranu soukromí se podobá české judikatuře. Oba soudy se shodují v tom, že veřejně význačné osobnosti (jako politici, umělci, sportovci) mají menší nárok na soukromí ve srovnání s ostatními jednotlivci. Evropským soudem pro lidská práva učinil rozhodnutím ze dne 18. 5. 2004, č. stížnosti 58148/00, jasný závěr, že je legitimní diskutovat o vlivu zdravotního stavu politika na výkon jeho funkce, zejména když je veřejně známo, že je těžce nemocný.[156]

V uvedeném případě bývalého francouzského prezidenta F. Mitterranda získalo vydavatelství Éditions Plon práva na vydání knihy od doktora Clauda Gublera, který dlouhá léta sloužil jako jeho osobní lékař. Kniha se zabývala vztahy mezi lékařem a pacientem, u kterého byla v roce 1981 diagnostikována rakovina. V rámci této knihy lékař rozebíral obtíže, které vznikly při zachování důvěrnosti prezidentova zdravotního stavu na jeho přání. Kniha vyšla devět dnů po prezidentově úmrtí.

Téhož dne podala vdova po F. Mitterrandovi žalobu, v níž argumentovala porušením mlčenlivosti, narušením prezidentova soukromí a zraněním citů příbuzných – vdovy a dětí. Soud zdůvodnil své rozhodnutí tím, že porušení mlčenlivosti způsobilo vážné narušení intimní

sféry prezidentova rodinného života, a tím pádem i života jeho ženy a dětí. Zejména vzhledem k nedávnému úmrtí prezidenta a jeho pohřbu považoval soud zásah do soukromí za zvláště neomluvitelný.

Co se týče zdravotního stavu politika, částečně je věcí veřejnou, ale podmínkou je, aby informace o jeho zdravotním stavu nebyly v rozporu s právem na lidskou důstojnost a obecným vkusem. Rozhodnutí dokonce rozlišuje mezi časem od uplynutí smrti politika: čím více času uplynulo, tím více převažuje zájem veřejnosti o informace o jeho životě nad ochranou jeho soukromí.[157]

U osob veřejně známých je tedy vždy nutné zvážit, zda poskytování informací je ve veřejném zájmu či nikoli a zda zdravotní stav může nebo bude mít vliv na výkon jejich veřejné činnosti. Aby veřejný zájem existoval, musí odhalování ze soukromého života souviset s dozorem nad vykonáváním jejich veřejných funkcí. *„Publikace článků, jejichž jediným účelem je uspokojit zvědavost určité části čtenářů, nelze považovat za příspěvek k jakékoli diskusi, pokud jde o obecný zájem společnosti, i přes to, že stěžovatelka je veřejnosti známa.“*[158]

Otázka, zdali lékař, po poskytnutí informací médiím o zdravotním stavu pacienta, když je tento stav již veřejnosti znám, souhlasil implicitně s prolomením povinnosti mlčenlivosti a s medializací pacientova zdravotního stavu, byla rovněž předmětem odborných diskuzí. Krajský soud v Brně rozhodoval o konkrétním případu[159], když zamítl žalobu pacientky na ochranu osobnosti (na ochranu soukromí) proti ošetřující lékařce, která zveřejnila informace týkající se zdravotního stavu pacientky v médiích. Soud zohlednil, že tyto informace byly v minulosti již zveřejněny samotnou pacientkou: *„Žalobkyně poskytla sdělovacím prostředkům obšírná a k postupu žalované kritická mediální vyjádření o celé věci, přičemž sama zveřejnila i údaje ze zdravotnické dokumentace. … Lze tedy důvodně učinit závěr, že žalobkyně vyloučila tímto postupem určité (jinak chráněné) skutečnosti ze svého soukromí, když v souladu se zásadou audiatur et altera pars (nechť je slyšena i druhá strana) musela důvodně předpokládat, že sdělovací prostředky ve věci kontaktují ohledně vyjádření k případu i žalovanou.“*[159]

Když pacient sám zveřejní informaci, nemůže očekávat, že třetí strany, které byly vázány mlčenlivostí, budou stále udržovat stejnou míru utajení jako v případě, kdy tyto informace nebyly veřejně známy. Jakmile se informace stane veřejně známou, stává se to, co nazýváme „věcí veřejnou“, a nelze od ní očekávat stejnou ochranu jako u informací, které zůstávají tajné. Jinými slovy, veřejně známé informace nemohou být nadále chráněny povinností mlčenlivosti.

Nicméně, časem může veřejná známost určitých skutečností pominout (zapomněním), čímž se opět stává důvěrnou.[160]

Kauza Selistö versus Finsko[156] představuje rovněž další případ, kdy došlo k prolomení mlčenlivosti v souvislosti se sdělovacími prostředky. V roce 1996 finská novinářka z regionálního deníku zveřejnila článek, který pojednával o údajně neprofesionálním jednání nejmenovaného chirurga, který měl být viněn ze smrti pacienta v místním zdravotnickém zařízení. Tento krok se však ukázal jako kontroverzní a novinářka byla v roce 1999 finskými soudy uznána vinnou trestným činem pomluvy. Novinářka však podala námitku k Evropskému soudu pro lidská práva s odkazem na porušení práva na svobodu projevu. A byla ve své námitce úspěšná. Evropský soud pro lidská práva potvrdil důležitost legitimního zájmu veřejnosti a klíčovou úlohu tisku v demokratické společnosti, zvláště pokud jde o diskuze o záležitostech veřejného zájmu. V tomto případě byl právě legitimní zájem veřejnosti oznámit, že došlo k chybě ve zdravotnickém zařízení, přednostnější než obava, že čtenáři by mohli lékaře (ač nejmenovaného) identifikovat. Důležité je zajistit transparentnost a informovanost ve společnosti, kdy tisk sehrává klíčovou roli v tomto procesu.[156]

Dílčí shrnutí

Nastíněné příklady lze v dílčím závěru této kapitoly shrnout do konstatování, že **veřejnost má právo na to znát informace o zdravotním stavu chráněné osoby, která vykonává exponovanou ústavní nebo politickou funkci, obzvláště pokud je veřejnosti známo, že s chráněnou osobou něco je.**

Tento pohled je však úzce zaměřen na chráněné osoby ve veřejném sektoru (politiky), které byly do své funkce zvoleny.

Rovněž je nezbytné konstatovat, že i zde není toto právo bezbřehé a podléhá v každém individuálním případě požadavku provedení testu proporcionality, kdy v případě poskytnutí informací je nutné v maximální možné míře chránit osobnostní práva chráněné osoby a poskytnout pouze takové informace, které jsou nezbytné k dosažení požadovaného účelu.

2.8.4 Právní ochrana osobních údajů příslušníků ozbrojených sil

Jak bylo zmíněno výše, jednou z vybraných skupin chráněných osob, na kterou je zacílena i výzkumná část práce, jsou obecně příslušníci ozbrojených sil a bezpečnostních sborů, které je v řadě případů nezbytné chránit více, nežli je obecně uznávaný standard. Mimo fyzické

a virtuální bezpečnosti jejich uchovaných zdravotních dat a probíhajících procesů hraje významnou roli také otázka právní úpravy jejich zpracování, zejména ochrany osobních údajů vojáků, kde řadíme i citlivé osobní údaje, kterými jsou jak informace o zdravotním stavu vojáků, tak jejich biometrické údaje. Ve světle současných a budoucích vojenských či bezpečnostních operací, vedených jak EU, tak NATO, se osobní údaje vojáků a příslušníků bezpečnostních sborů a jejich biometrické informace staly klíčovou složkou informační převahy a operační efektivity.[161]

Přestože existují přísná pravidla pro ochranu dat v civilním sektoru EU, podobně striktní rámec chybí pro vojenské mise EU. To představuje právní vakuum, zejména s ohledem na základní práva a ochranu osobních údajů, které jsou v EU chráněny jak primárním, tak sekundárním právem.[162]

V rámci komplexního procesu hospitalizace chráněných osob již v současné době nelze vnímat prostředí poskytovatele zdravotních služeb výhradně na jeho fyzický areál. V dnešním virtualizovaném světě je dosah takového poskytovatele prakticky po celém světě, obzvláště v rámci otázky přenosu informací o zdravotním stavu pacientů, kteří jsou transportováni do zdravotnického zařízení ze vzdálených míst, například z bojiště. V daném kontextu jsou pak jedním z využitelných prvků vojenského zdravotního informačního systému biometrické technologie, které se postupně stávají nezbytným nástrojem v oblasti vojenského zpravodajství a bezpečnosti. Vzhledem k nutnosti zabezpečení komplexní hospitalizace chráněných osob ze strany zdravotnického zařízení (Role 4) je nezbytné, aby toto zařízení bylo připraveno reagovat na aktuální bezpečnostní trendy v oblasti zahraničních operací a válečných konfliktů. Právě zmíněné biometrické údaje mohou hrát klíčovou roli, neboť mají, mimo jiné, schopnost odnímat nepřátelům výhodu anonymity, což může být naopak velkou slabinou v případě úniku dat a informací, což si zdravotnické zařízení nemůže dovolit.

Popsaná technologie byla již implementována v rámci operací vedených NATO a méně rozšířeně také v misích EU.[163] Vzhledem k významným přínosům této technologie v armádním prostředí lze očekávat snahu o její širší využití v rámci těchto misí a jednotlivých vojenských poskytovatelů zdravotních služeb. Významným aspektem je i skutečnost, že na rozdíl od NATO, EU jako mezinárodní organizace vyvinula rozsáhlý rámec pro ochranu dat, včetně biometrických údajů, což vyvolává očekávání ohledně právních záruk při používání biometrických systémů v rámci vojenských misí EU, zejména co se týče sdílení biometrických dat.[164] Uvedené má význam zejména pro členské státy EU, které jsou současně členy NATO

a mohou být vázány právem EU na ochranu dat při účasti na operacích NATO.[165] Tím vzniká velmi zajímavá právní otázka týkající se potenciálního vytvoření jednotné armády NATO a sdílení osobních údajů vojáků mezi jednotlivými armádami. V takovém případě bude jistě nezbytné, aby vojenský poskytovatel zdravotních služeb byl na zmíněné sdílení osobních údajů vojáků připraven po všech stránkách, zejména v oblasti kybernetické bezpečnosti a právní ochrany dat, neboť proces jeho hospitalizace je započat již jeho raněním na bojišti.

Pokud jde o ochranu osobních údajů v rámci vojenských misí EU, článek 39 Smlouvy o EU[33] je základem pro specifická pravidla týkající se ochrany osobních údajů v rámci Společné zahraniční a bezpečnostní politiky[34]. Přestože Rada EU zatím nepřijala rozhodnutí stanovující specifický režim ochrany dat pro SZBP, lze jistou míru ochrany dosáhnout aplikací existujících právních předpisů EU o ochraně dat, konkrétně se jedná o nařízení GDPR a dále Směrnici (EU) 2016/680 Evropského parlamentu a Rady ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány pro účely prevence, vyšetřování, odhalování nebo stíhání trestných činů nebo výkonu trestů a o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/JHA, která je *lex specialis* ve vztahu k GDPR, pokud jde o ochranu fyzických osob ve spojení se zpracováním osobních údajů pro účely vymáhání práva. Uvedený základní právní rámec EU se vztahuje i na zpracování a sdílení biometrických údajů v rámci misí vedených v rámci SZBP. Používání biometrické technologie v armádních operacích a misích EU nabývá na významu s ohledem na její potenciál odhalit identitu nepřátel a odstranit jejich výhodu anonymity.

Příkladem je relativně nedávná operace EUNAVFOR MED IRINI[35], zaměřená na vynucování zbrojního embarga OSN na Libyi, která může shromažďovat a ukládat osobní údaje, včetně biometrických, za účelem identifikace osob zapojených do přepravy zakázaných položek.[166]

Specifický právní rámec EU v oblasti ochrany dat, zahrnující informace o zdravotním stavu a biometrické údaje, vyvolává tlak na přijetí vysokých právních záruk při jejich zpracování

---

[33] Dále jen „SEU“.

[34] Dále jen „SZBP“.

[35] EUNAVFOR MED IRINI je vojenská operace EU zaměřená na prosazování zbrojního embarga OSN proti Libyi. Operace byla zahájena v březnu 2020 a nese název IRINI, což v řečtině znamená „mír“. Jejím hlavním úkolem je monitorování a zabránění nelegálnímu dovozu zbraní do Libye, čímž přispívá ke stabilizaci a mírovému řešení konfliktu v regionu. Operace zahrnuje také monitorování nelegálního obchodu s ropou, výcvik libyjské pobřežní stráže a námořnictva a pomoc v boji proti pašování a obchodování s lidmi. Operace EUNAVFOR MED IRINI využívá letecké, satelitní a námořní prostředky ke sledování lodní dopravy a dalších aktivit ve Středozemním moři.

a sdílení v rámci vojenských misí EU. To má dopad i na členské státy EU, které jsou současně členy NATO, jelikož mohou být vázány právem EU na ochranu dat při účasti na operacích NATO.[167] Významnou úlohu má aplikace právních předpisů EU o ochraně zdravotních dat na sdílení biometrických údajů v rámci vojenských misí EU. Důraz je kladen na vliv rámcového práva EU na zpracování a sdílení zdravotních dat a biometrických údajů, což zahrnuje případy, kdy členské státy implementují právní předpisy EU ve svých ozbrojených silách.[168] Tento přístup bude nutné při tvorbě vojenských zdravotních informačních systémů sjednotit s požadavky NATO a vymezit jasná pravidla pro sdílení osobních údajů mezi jednotlivými armádami.

Přijetí používání biometrie a nastavení pravidel pro ochranu osobních údajů v rámci vnitrostátní úpravy členských států formuje schválení jejich vojenského využití v zahraničí. Navíc způsob, jakým členský stát umožňuje své armádě zpracovávat osobní údaje, formuje procesy, jakými je dosaženo technické interoperability mezi ostatními armádami. Například právní výhrady pro uchovávání dat, pokud jsou aplikovatelné, musí být součástí technické interoperability, která doprovází vyměňovaná zdravotní a biometrická data po celou dobu jejich životního cyklu od jejich kolébky až po hrob.[169] Jelikož USA mohou být považovány za průkopníka vojenského využití biometrie a specifického zpracování citlivých osobních údajů, jejich právní záruky a obecně vyšší míra společenského souhlasu s přijetím nových technologií a jejich využíváním se výrazně projevuje v současných vojensko-technických standardech interoperability zdravotnických informačních systémů jednotlivých armád NATO.[168]

Další diskutovanou otázkou je i dopad biometrických systémů na interoperabilitu mezi různými misemi, či potřeba vytvoření komplexních pravidel ochrany dat v souladu s čl. 39 Smlouvy o EU, aby bylo možné efektivně sdílet osobní údaje získané v rámci misí SZBP s dalšími elementárními bezpečnostními režimy, jako je právě NATO nebo OSN.[170]

Článek 39 Smlouvy o EU, ve spojení s článkem 16 Smlouvy o EU, je klíčový pro zpracování osobních údajů v kontextu společné bezpečnostní a obranné politiky. Ačkoliv primární právo EU obsahuje silné fundamentální závazky k ochraně dat, efektivní ochrana v praxi závisí na detailech a implementaci sekundárního práva, které konkrétně řeší unikátní okolnosti vojenských misí a operací. Sekundární legislativa, jako je GDPR, přestože není primárně určena pro vojenské mise, může sloužit jako primární vodítko a analogie pro tvorbu chybějícího rámce.[171] Tento přístup je tedy nezbytné ze strany členských armád EU, které jsou i součástí NATO, využít jako základní právní rámec pro tvorbu vojenských zdravotnických informačních

systémů určených pro přenos a zpracování zdravotních dat až k poskytovateli zdravotních služeb, u kterého je anebo má být raněný voják hospitalizován.

Podstatným prvkem legálního zpracování osobních údajů chráněných osob je potřeba jasně definovaných a transparentních procesů pro sdílení a zpracování osobních údajů, s výslovným souhlasem dotčených osob nebo na základě jiného legitimního právního základu plynoucího z právních norem. Tato opatření musí být podložena pevnými zárukami, které chrání proti zneužití a poskytují možnost přístupu k osobním údajům a datům vojáků. Je zásadní, aby jakýkoliv přenos osobních údajů byl podložen adekvátními bezpečnostními standardy, a to zejména v případě transferů dat mezi různými mezinárodními organizacemi nebo státy. Otázka tvorby a přijetí těchto standardů bude jistě značně komplikovaná, nicméně zcela nutná.

Ve světle nedostatku specifického právního rámce pro kybernetickou ochranu sdílených dat v rámci zahraničních vojenských misí a jejich přenosu do informačních systémů vojenských poskytovatelů zdravotních služeb, u kterých má být raněný voják hospitalizován, je nezbytná tvorba a dodržování detailních dohod, které stanoví protokoly pro zpracování, sdílení a ochranu dat. Takové dohody by mohly sloužit jako dočasná náhrada za chybějící legislativu, ačkoliv jsou pouze provizorním řešením, neboť nevyřešené právní otázky mohou výrazně omezit efektivitu a interoperabilitu vojenských operací. V této oblasti hraje významnou roli i pokrok v technologiích a získané zkušenosti, kde virtuální medicína a využití cloudových technologií posouvají hranice možného, přesto vždy s důrazem na zabezpečení a individuální ochranu dat jednotlivých vojáků. Je otázkou, zda za nastavení bezpečnostních pravidel má být odpovědné zdravotnické zařízení, či je to otázka pro příslušné ministerstvo nebo přímo instituci na úrovni ústředního správného úřadu nebo vlády.

2.9 Shrnutí teoretické části práce

Na základě výše uvedeného a s ohledem na hlavní cíle disertační práce lze teoretické poznatky shrnout a rozšířit následujícím způsobem.

Chráněná osoba je definována jako jedinec nebo skupina osob, které je na základě platné právní úpravy, nebo rozhodnutí oprávněného subjektu, poskytována zvýšená míra ochrany. Tato ochrana se vztahuje nejen na fyzickou bezpečnost, ale analogicky také na bezpečnost kybernetickou. Do této kategorie chráněných osob patří nejen ústavní činitelé a veřejně známé osobnosti, ale také například příslušníci ozbrojených sil, bezpečnostních sborů a další jedinci, jejichž postavení nebo činnost vyžadují v určitém čase specifická bezpečnostní opatření.

Chráněným osobám je poskytována stejná úroveň kvality a rozsah zdravotních služeb jako běžným pacientům. Tudíž nemají na základě svého statusu právo na jakékoliv přednostní zacházení v rámci poskytování zdravotní péče. Základním principem zdravotního práva v České republice je rovnost všech pacientů bez ohledu na jejich společenské postavení.

Specifika spojená s chráněnými osobami však vyžadují zvláštní přístup k ochraně jejich osobních údajů a zajištění vyšší úrovně bezpečnosti během hospitalizace, přenosu dat a jejich zpracování. Vzhledem k tomu, že data chráněných osob mohou mít citlivější povahu a jejich neoprávněné zveřejnění by mohlo vést k ohrožení nejen jejich soukromí, ale i bezpečnosti, je nezbytné chránit jejich informace více než u běžných pacientů.

Klíčovým faktorem pro ochranu údajů chráněných osob je přenos a ukládání těchto dat. Je nezbytné, aby byla zavedena pokročilá technická opatření, která zajistí bezpečný přenos dat mezi zdravotnickými zařízeními a jejich zabezpečené uložení, například v privátních či semiprivátních cloudových řešeních. Zvláštní pozornost by měla být věnována šifrování dat a autentizaci přístupu, což jsou zásadní prvky v ochraně proti kybernetickým útokům, které by mohly ohrozit údaje chráněných osob.

Další důležitou otázkou je veřejný zájem na informování veřejnosti o zdravotním stavu chráněné osoby, zvláště pokud se jedná o ústavního činitele, politika nebo veřejně známou osobnost. Pokud je taková osoba hospitalizována, je přítomnost zájmu veřejnosti přirozená, zvláště v případech, kdy se ví, že dotyčná osoba má zdravotní problémy nebo je pod ochranou bezpečnostních složek. Velký senát Evropského soudu pro lidská práva konstatoval, že veřejný zájem se vztahuje k informacím, které ovlivňují veřejnost do té míry, že přitahují její pozornost

nebo se jí přímo týkají, obzvláště pokud se jedná o záležitosti, které mohou ovlivnit životní úroveň občanů nebo život společnosti jako celku.

Tento aspekt je však v přímém střetu s právem na ochranu osobních údajů a soukromí chráněné osoby. Proto je klíčové nalézt rovnováhu mezi právem veřejnosti na informace a právem chráněné osoby na soukromí. **Zveřejnění informací týkajících se zdravotního stavu by mělo být limitováno na základě toho, co je v daném případě nezbytné pro veřejné informování zejména s ohledem na výkon funkce chráněné osoby, aniž by došlo k porušení důstojnosti a práv pacientů na ochranu jejich soukromí.** V tomto kontextu je důležité využití analogie v těch právních aspektech, které nejsou explicitně upraveny.

Dílčím závěrem lze konstatovat, že zvýšená míra ochrany citlivých údajů chráněných osob, ať již jde o fyzické nebo digitální zabezpečení, je v dnešním světě nepostradatelná. Zdravotnická zařízení musí nevyhnutelně přijmout opatření, která zajistí nejen ochranu těchto informací během jejich přenosu a zpracování, ale také respektují právo veřejnosti na informace v případech, kdy to vyžaduje veřejný zájem. Takový komplexní přístup k ochraně dat a práv chráněných osob musí být v souladu s mezinárodními standardy a moderními technologickými postupy, aby byla zajištěna maximální úroveň bezpečnosti i v těchto citlivých případech.

3 Výzkumná část práce

3.1 Cíle a zaměření výzkumu

Cíle výzkumné části práce korespondují a navazují na soustavu cílů disertační práce vytyčených v kapitole 1.2 a byly stanoveny za účelem jejich naplnění. Patří mezi ně:

Hlavní výzkumný cíl

Hlavním výzkumným cílem této disertační práce je na základě získaných empirických dat a poznatků identifikovat klíčová riziková místa v oblasti bezpečnosti a ochrany osobních a zdravotních dat chráněných osob během jejich hospitalizace, přenosu a zpracování ve zdravotnických zařízeních v České republice. V návaznosti na to bude výzkumná část práce směřovat k formulaci konkrétních a prakticky využitelných doporučení, která přispějí k posílení ochrany citlivých údajů a zvýšení úrovně zabezpečení informací v těchto zařízeních.

Z uvedeného vyplývá několik dílčích výzkumných cílů, které korespondují s hlavním výzkumným cílem a které byly vytyčeny autorem práce:

Dílčí výzkumný cíl č. 1

Identifikovat nejčastější slabá místa v oblasti bezpečnosti a zabezpečení dat a informací při hospitalizaci chráněných osob. Výstupem bude soubor doporučení pro zlepšení bezpečnosti zpracování zdravotních dat chráněných osob ve zdravotnických zařízeních.

Dílčí výzkumný cíl č. 2

Identifikovat a analyzovat specifická rizika pro principy poskytování zdravotní péče a fyzické bezpečnosti pacientů se statutem chráněné osoby ve srovnání s běžnými pacienty. Výstupem bude navržení doporučení pro praxi včetně identifikace specifických zranitelností a doporučení pro jejich minimalizaci oproti běžným pacientům.

Dílčí výzkumný cíl č. 3

Zhodnotit aktuálně implementovaná technická, právní a organizační opatření pro ochranu citlivých informací pacientů se statutem chráněné osoby ve vybraných zdravotnických zařízeních. Výstupem bude přehled současného stavu zabezpečení a návrhy na jeho zlepšení.

Dílčí výzkumný cíl č. 4

Stanovit model ochrany, přenosu a zpracování zdravotních dat chráněných osob pro jejich virtuální hospitalizaci nebo vyšetření v podmínkách poskytovatele zdravotních služeb fakultního typu, zahrnující technická, organizační a legislativní opatření na základě kombinace kvantitativních a kvalitativních výzkumných metod. Zvolenou skupinou chráněných osob budou příslušníci ozbrojených sil a přenos jejich dat z bojiště do zdravotnického zařízení.

Jednotlivé dílčí výzkumné cíle budou realizovány pomocí kvalitativní metody polostrukturovaných rozhovorů s odborníky z praxe a kvantitativního empirického šetření pomocí dotazníkového šetření mezi zdravotnickým personálem, chráněnými osobami a bezpečnostními experty.

3.2 Metodologie výzkumu

3.2.1 Výzkumné přístupy

Činnosti vedoucí k vytvoření kvalitního a efektivního modelu zabezpečení osobních a zdravotních dat chráněných osob ve zdravotnických zařízeních úzce souvisí s přesným porozuměním a sjednocením základní terminologie v této oblasti. V oblasti kybernetické bezpečnosti a ochrany dat je tento proces značně náročný, neboť zahrnuje multidisciplinární přístup, který obsahuje jak technické aspekty, tak organizační a právní rámce. Proto je nutné pokusit se o určité sjednocení pojmů, které souvisí s problematikou této práce, neboť terminologická nejednotnost a různorodost mohou komplikovat snahy o vytvoření odpovídajícího modelu zabezpečení dat.

Při zpracování výzkumné části disertační práce byly proto použity následující metodologické přístupy:

- normativní přístup,
- deskriptivní přístup,
- interdisciplinární přístup,
- vývojový přístup,
- systémový přístup.

Využitím jednotlivých přístupů je možné vytvořit ucelený a systematický model zabezpečení zdravotních dat chráněných osob ve zdravotnických zařízeních.

1) **Normativní přístup** je založen na podrobné analýze, kdy jeho výsledkem jsou návrhy teoretických postupů řešení zkoumaného problému. V kontextu zabezpečení dat to znamená stanovení standardů a doporučených postupů pro ochranu citlivých zdravotních informací.
2) **Deskriptivní přístup** vychází z popisu určité skutečnosti v kvalitativní i kvantitativní podobě, a to v rámci vyjádření míry shodnosti mezi zkoumanými jevy. Je založen na empirickém rozboru již existujících systémů a ukazuje, jaká je skutečnost. V oblasti zabezpečení dat zahrnuje deskriptivní přístup analýzu současných bezpečnostních opatření a identifikaci slabých míst a rizikových faktorů.
3) **Interdisciplinární přístup** vysvětluje, že studovaný jev je možné zkoumat z různých hledisek, díky čemuž je možné se oprostit od starých zažitých postupů a využít nové pohledy na danou problematiku. Tento přístup umožňuje kombinaci technických, právních a organizačních perspektiv pro komplexní pochopení zabezpečení dat chráněných osob.
4) **Vývojový přístup** se snaží poukázat na skutečnost, že všechno se vyvíjí v určité konkrétní a historické situaci. Díky tomu je následně možné pochopit celou řadu vlivů a východisek, které se zdají být neaktuální a zastaralé. V kontextu zabezpečení dat to znamená zohlednění historického vývoje technologií a bezpečnostních opatření a jejich přizpůsobení aktuálním potřebám.
5) **Systémový přístup** je založen na myšlence diferenciace jednotlivých systémů či problémů, což znamená, že každý celek má své dílčí komponenty, mezi nimiž je možné nalézt určité vazby. Tento přístup umožňuje analyzovat různé části systému zabezpečení dat a jejich vzájemné vztahy, což je klíčové pro identifikaci potenciálních slabých míst a návrh efektivních bezpečnostních opatření.[172]

Využitím těchto metodologických přístupů lze vytvořit komplexní a robustní model zabezpečení zdravotních dat chráněných osob, který bude přizpůsoben specifickým potřebám zdravotnických zařízení a chráněných osob. Tento model bude zahrnovat jak technická, tak organizační a právní opatření, čímž zajistí maximální úroveň ochrany citlivých zdravotních informací.

3.3 Výzkumné metody

Výzkum bude realizován kombinací kvantitativních a kvalitativních metod, přičemž hlavními nástroji budou dotazníková šetření, komparace se zahraničím a polostrukturované rozhovory. Kvantitativní metody umožní získání statisticky relevantních dat a z nich plynoucích informací, zatímco kvalitativní metody poskytnou hlubší vhled do konkrétních problémů a jejich řešení.

V rámci výzkumného procesu bude nejprve realizováno dotazníkové šetření mezi zdravotnickým personálem, bezpečnostními experty a samotnými chráněnými osobami za účelem získání potřebných dat a informací. Následně budou získaná data a informace vyhodnocena a analyzována v kontextu současného stavu bezpečnosti a zabezpečení dat. Na základě výsledků této analýzy budou navržena konkrétní opatření a postupy pro zvýšení bezpečnosti a ochrany dat chráněných osob, včetně doporučení pro praxi v oblasti poskytování zdravotní péče a zajištění fyzické bezpečnosti chráněných osob.

Během výzkumné praxe se často potýkáme s různými problémy a omezeními, které vyplývají z použití specifických vědeckých metod a postupů. Rozlišení vědeckých metod na kvalitativní a kvantitativní bývá mnohdy nejasné, protože je obtížné přesně stanovit hranici mezi těmito přístupy. Například metody jako pozorování a rozhovory se používají jak v kvalitativním, tak kvantitativním výzkumu. Přestože rozdíl mezi kvalitativním a kvantitativním výzkumem je klíčový pro jejich správné použití, oba přístupy jsou rovnocenné a každý z nich přináší odlišné, ale cenné výsledky. Kvalitativní metody jsou vhodné pro získání hlubokých a detailních poznatků, zatímco kvantitativní metody poskytují měřitelná data. Oba typy výzkumu se vzájemně doplňují a přispívají k celkovému poznání.

Kombinace kvalitativních a kvantitativních metod umožňuje získat komplexní pohled na problematiku bezpečnosti dat chráněných osob. Kvalitativní data získaná prostřednictvím polostrukturovaných rozhovorů s odborníky a kvantitativní data z dotazníků poskytují hluboké a široké pochopení výzkumných otázek. Tyto metody společně umožňují nejen identifikaci hlavních problémových oblastí, ale také návrh konkrétních opatření a postupů pro zvýšení bezpečnosti zdravotních dat ve zdravotnických zařízeních.

Díky kombinaci těchto metod bude možné vytvořit efektivní opatření a postupy pro ochranu osobních a zdravotních dat chráněných osob ve zdravotnických zařízeních v České republice, což přispěje ke zvýšení kvality a bezpečnosti poskytované péče.

Kvalitativní a kvantitativní výzkum a s ním spjaté metody tvoří dva základní metodologické přístupy uplatňované v sociálních vědách. Svojí povahou, zaměřením i výsledky jsou tyto přístupy do jisté míry komplementární, většina výzkumů je z hlediska této distinkce smíšená. Oba přístupy se (nestejnou měrou) uplatňují na všech výzkumných rovinách a ve všech tradičně vymezovaných vědeckých disciplínách.[173]

Kvalitativní výzkum představuje *„proces hledání porozumění založený na různých metodologických tradicích zkoumání daného sociálního nebo lidského problému.“*[174] Výzkum, který se zaměřuje na to, jak jednotlivci a malé skupiny nahlížejí, chápou a interpretují svět, lze rovněž považovat za kvalitativní. Kvalitativní výzkum neužívá statistických metod a technik, čímž se staví do opozice vůči kvantitativnímu výzkumu. V praxi psychologického a sociologického výzkumu se oba přístupy často vzájemně doplňují.[175]

Obecně lze konstatovat, že za kvalitativní výzkum můžeme považovat takový výzkum, který v rámci svých postupů nevyužívá technik a metod statistiky. Samotné metody kvalitativního výzkumu se využívají k získávání kvalitativních dat, to znamená, že se snaží popsat smysl, nikoliv význam neboli četnost určitého konkrétního lidského projevu. Pokud by dané tvrzení mělo býti vztaženo na tuto práci, jednalo by se například o způsoby zabezpečení zdravotní dokumentace chráněných osob.

Kvalitativní výzkum může být výzkum prováděný na malé skupině respondentů s cílem zjistit nejen, jak se chovají, ale především proč se tak chovají, jaké důvody stojí za jejich chováním. Kvalitativní přístup se snaží nalézt pochopení zkoumaného jevu. V kvalitativním přístupu nejde o numerické řešení, ale spíše o interpretaci reality, kterou lze zjistit otázkami „kdo“, „proč“, „jak“.[176]

Součástí těchto výzkumných postupů mohou být specifické analýzy a interpretace dat, obecně zaměřené na pochopení problému. Metody kvalitativního výzkumu v dnešní době stále více rezonují v laické, ale především odborné veřejnosti. Jsou považovány za doplněk tradičních kvantitativních postupů, nebo jejich protiklad. Uvedené pojetí záleží na úhlu pohledu, který je zvolen. Jedná se ovšem o velmi užitečné přístupy v případech, kdy jde o zkoumání života lidí, historie i chodu organizací a jiných významných společenských procesů. Uvedené metody s sebou přináší rovněž celou řadu nových přístupů, které jsou neustále rozvíjeny v návaznosti na aktuální trendy v oblasti vývoje bezpečnostních opatření a obecně kvality poskytované zdravotní péče.[177]

Kvalitativní výzkum obsahuje například následující aspekty:

- má blíže k psychologii,
- jeho cílem je formulování nových hypotéz,
- poskytuje rozsáhlé informace o malém počtu jedinců,
- snižuje počet zkoumaných osob,
- nízká míra reliability (spolehlivosti),
- je vysoce validní (má vysokou schopnost potvrzovat či uznávat konkrétní postupy, tvrzení atd.).

Do sféry kvantitativního výzkumu lze naopak zařadit:

- popis procesů, vztahů, okolností, situací, systémů nebo lidí,
- interpretaci, explanaci a exploraci,
- verifikaci předpokladů, teorií nebo zobecnění,
- evaluaci a komparaci procesů – praktik v organizaci, inovaci programů.

Kvalitativní výzkum je jedním z přístupů, který se zaměřuje na porozumění činnostem a významům v jejich sociálním kontextu, aniž by redukoval počet proměnných nebo vztahy mezi nimi. Tento typ výzkumu preferuje otevřené a málo strukturované výzkumné plány, kde analýza vychází z velkého množství informací o malém počtu jedinců. Výsledky a teorie vznikají přímo ze získaných dat, což znamená, že jsou úzce propojeny se zkoumaným jevem v širším kontextu dané oblasti bádání.[177]

V kvalitativním výzkumu je klíčová součinnost mezi výzkumnou otázkou, daty a použitými metodami. Tato korelace je důležitým prvkem, který určuje kvalitu a validitu výzkumu. Například semi-strukturované rozhovory a focus groupy jsou běžně používané metody pro získání hlubokého porozumění subjektivním zkušenostem a motivacím respondentů.[178]

Kvantitativní výzkum je metoda standardizovaného vědeckého výzkumu, která popisuje jevy pomocí stanovených proměnných, jež měří určité vlastnosti. Kvantitativní výzkum se zaměřuje na numerická data, která jsou analyzována pomocí statistických metod s cílem identifikovat vzory, vztahy a kauzální souvislosti mezi proměnnými.[179]

Mezi hlavní metody kvantitativního výzkumu patří:

- **Experimenty**: Kontrolované studie, kde jsou proměnné manipulovány za účelem testování hypotéz a zjištění příčinných vztahů.
- **Průzkumy**: Dotazníky a ankety, které sbírají data od velkých vzorků populace, aby se identifikovaly trendy a vzory.
- **Observační studie**: Sledování a zaznamenávání chování v přirozeném prostředí bez manipulace proměnných.
- **Sekundární výzkum**: Analýza dat, která byla shromážděna pro jiné účely, například národní statistiky nebo historické záznamy.[12]

Kvantitativní výzkum je běžně používán v přírodních vědách, společenských vědách, zdravotnictví, vzdělávání a mnoha dalších oblastech. Výhody tohoto přístupu zahrnují objektivitu, reprodukovatelnost výsledků, možnost zobecnění nálezů na širší populaci a přesnost v měření a analýze dat.[179]

Charakteristickými rysy kvantitativního výzkumu podle Pavlici jsou:

1) **nezávislost** (výzkumník je nezávislý na zkoumaných jevech),
2) **hodnotová svoboda a autonomie vědy** [výběr a volba toho, co a jakým způsobem bude studováno, by mělo být determinováno objektivními kritérii (např. výsledky předchozích výzkumů, poukazující na určité problémy)],
3) **kauzalita** (cílem sociální vědy by měla být identifikace kauzálních vztahů a zákonitostí, které objasňují pravidelnost lidských projevů),
4) **hypoteticko-deduktivní přístup** (věda se rozvíjí prostřednictvím procesu formulace a testování hypotéz, týkajících se obecných pravidel a zákonitostí),
5) **operacionalizace** [vědecké pojmy by měly být operacionalizovány (tj. převedeny do řeči konkrétních projevů a faktů), aby tak bylo umožněno kvantitativní měření skutečností, ke kterým se vztahují a které charakterizují],
6) **redukcionismus** [problémům lze celkově lépe porozumět tehdy, jsou-li redukovány na co nejjednodušší elementy (s tímto předpokladem však všichni pozitivisté nesouhlasí)],
7) **generalizace** (možnost zobecnění zjištěných zákonitostí lidského a sociálního chování je nutno zajistit především dostatečně velkými vzorky zkoumaných osob),

8) **průřezová analýza** (obecná pravidla a zákonitosti lze nejlépe identifikovat prostřednictvím srovnávání variací napříč různými vzorky).[180]

Pokud by měl být kvantitativní výzkum rozdělen dle Windelbandovy klasifikace věd, jednalo by se o tzv. nomotetický přístup. Tento přístup se zaměřuje na zkoumání jevů řídících se objektivními zákonitostmi, které se v přírodě i v naší společnosti opakují. Nomotetický přístup se snaží vysvětlit sociální realitu a lidské chování na základě obecně platných zákonitostí. Tento přístup umožňuje identifikaci poznatků, které lze aplikovat na široké spektrum jevů, čímž poskytuje vysokou míru generalizace.[181]

Metody kvantitativního výzkumu v sociálních vědách jsou obšírné a mají základ v metodách přírodních věd. Tyto metody předpokládají, že lidské chování lze do jisté míry měřit a předvídat. Kvantitativní výzkum využívá dotazníky, pozorování, náhodné výběry a experimenty. Získaná data jsou analyzována za účelem vyhledávání, popisu a ověřování jejich validity. Na rozdíl od kvalitativního výzkumu se kvantitativní výzkum zaměřuje na rozsáhlejší společenské otázky a zkoumá větší okruh informací. Charakteristické rysy kvantitativního výzkumu zahrnují snadnou generalizaci výsledků na populaci, vysokou spolehlivost, deduktivní logiku výzkumu a ověřování hypotéz.[182]

Kvantitativní výzkum je však vhodný pouze v určitých situacích, například když je potřebné generalizovat nálezy vycházející z populace, pokud lze s jistotou odhadnout významné proměnné, nebo pokud je možné pro každou proměnnou navrhnout validní operační definice. Mezi omezení kvantitativního výzkumu patří nízká validita, omezený rozsah informací o mnoha jedincích, a redukce počtu zkoumaných znaků a vztahů mezi nimi.[183]

Zvolený postup výzkumu

Výzkum této disertační práce vzhledem k výše popsanému, a především v souvislosti s vytyčenými cíli a výzkumnými problémy musí mít proto povahu jak kvalitativního, tak i kvantitativního výzkumu.

Výsledky analýzy současného stavu bezpečnosti pacientských dat chráněných osob ve zdravotnických zařízeních v České republice, identifikace nejčastějších slabých míst a specifických rizik, zhodnocení existujících technických a organizačních opatření a návrh nových, efektivních řešení pro zlepšení bezpečnostních postupů a ochrany dat, budou po obhájení této práce prezentovány a předány nejen příslušným služebním funkcionářům a vedoucím pracovníkům zdravotnických zařízení, ale rovněž chráněným osobám

a představitelům ministerstev, které mají v gesci poskytovatele zdravotních služeb. Cílem je zkvalitnění úrovně bezpečnosti a ochrany osobních a zdravotních dat chráněných osob, a to na základě vyvinutých modelů a postupů. Tyto výstupy by měly přispět ke zvýšení bezpečnosti a kvality péče a poskytnout doporučení pro zdravotnická zařízení, která mohou být základem pro tvorbu centrální metodiky a jednotných postupů v oblasti nejen virtuální bezpečnosti.

3.3.1 Metody kvalitativního sběru dat

Než bylo přistoupeno k samotné aplikaci kvalitativních výzkumných metod, došlo k rozsáhlé teoretické analýze aktuálních poznatků v oblasti kybernetické bezpečnosti a ochrany zdravotních dat chráněných osob a rovněž poskytování zdravotních služeb této skupině osob. Tato část výzkumu byla nezbytná, protože vytvoření kvalitní odborné platformy bylo klíčové pro úspěšné provedení výzkumné části práce. Problematika kybernetické bezpečnosti je obecně velmi rozmanitá, a proto i diagnostické metody na její hodnocení musí být rovněž pestré.

Metody kvalitativního výzkumu se využívají k získání tzv. kvalitativních dat. Tyto přístupy jsou nápomocné pro stanovení smyslu a významu konkrétních projevů v oblasti bezpečnosti dat či přístupu zdravotnických zařízení k ochraně citlivých informací. Nejedná se o metody, které by stanovovaly určitou míru četnosti, ale umožňují analyzovat různými způsoby určitá data a následně je interpretovat.

Výběr metody pro sběr dat se provádí v závislosti na požadovaném typu informací, na zdroji, ze kterého informace získáváme, a na okolnostech, za jakých jsou data zjišťována. Za metodu sběru dat pro potřeby kvalitativního výzkumu byla zvolena metoda studia dokumentů a interpretativní fenomenologická analýza.

Studium dokumentů

Studium dokumentů je soubor metodických postupů používaných pro získání informací z dokumentárních zdrojů při studiu společenských jevů a procesů za účelem řešení konkrétních výzkumných problémů. Tato metoda je velmi významná pro sběr dat při provádění výzkumu, ve kterém dokumenty mohou být použity jako primární i sekundární zdroj informací. Typickým příkladem analýzy textových zdrojů je studium vědeckých publikací a zpráv o problematice kybernetické bezpečnosti ve zdravotnictví. Tento typ analýzy se obvykle provádí ve fázi návrhu výzkumného problému. Dokumenty jsou považovány za spolehlivé svědectví jevů, vyskytujících se v realitě, což velmi souvisí s úředními dokumenty, ale může se vztahovat i na neoficiální dokumenty. Nicméně při provádění výzkumu by měly být všechny dokumenty

vnímány kriticky, protože jejich výsledky se mohou výrazně lišit v závislosti na způsobu, jakým byly sestaveny.[184]

Interpretativní fenomenologická analýza (IPA)

Interpretativní fenomenologická analýza (Interpretative Phenomenological Analysis, dále také jen „IPA“) se zaměřuje na porozumění žité zkušenosti jednotlivců, což je klíčové při zkoumání bezpečnosti dat chráněných osob ve zdravotnických zařízeních. Tato metoda nám umožňuje detailně prozkoumat, jak jednotlivci přisuzují význam svým zkušenostem a jak tyto zkušenosti interpretují v kontextu konkrétních událostí nebo procesů.

IPA byla vyvinuta Jonathanem A. Smithem v 90. letech minulého století a původně byla spojena s psychologií zdraví. Dnes se však široce používá v různých oblastech, včetně klinické psychologie a psychoterapie. IPA poskytuje více prostoru pro kreativitu a svobodu ve výzkumném procesu než jiné kvalitativní přístupy a je považována za velmi vhodnou perspektivu pro zkoumání významu zkušeností jedinců v konkrétních podmínkách.[185]

Teoretická východiska IPA zakotvují svůj teoretický přístup ve třech hlavních oblastech: fenomenologii, hermeneutice a idiografickém přístupu. Tyto teoretické základy umožňují výzkumníkovi nejen popsat zkušenost, ale také ji interpretovat v kontextu žité reality jednotlivce. Fenomenologická reflexivita je v IPA vnímána jako nástroj pro zvědomění interpretační role výzkumníka, což je nezbytné pro porozumění zkušenosti jiných lidí.

Výzkumné otázky v IPA jsou formulovány tak, aby zkoumaly, jak jedinci vnímají a prožívají určitou situaci a jaký význam této zkušenosti přisuzují. V rámci výzkumu zaměřeného na bezpečnost dat chráněných osob se otázky mohou zaměřovat například na to, jak pacienti a zdravotnický personál vnímají a interpretují bezpečnostní opatření a rizika spojená s ochranou citlivých dat.[174]

Pro IPA je typické pracovat s menším počtem respondentů, aby bylo možné detailně analyzovat jejich individuální zkušenosti. Klíčovým požadavkem je homogenita vzorku, což znamená, že respondenti by měli reprezentovat daný fenomén co nejlépe. V našem výzkumu se zaměřujeme na zdravotnický personál a chráněné osoby, které zažívají specifické situace spojené s bezpečností jejich dat. Výběr respondentů byl zacílen na přední světové lékaře a lékařky, které mají zkušenosti s hospitalizací chráněných osob. Mimo to se jednalo rovněž o významné odborníky z oblasti IT.

Nejčastěji používanou metodou sběru dat v IPA je polostrukturovaný rozhovor, který umožňuje respondentům volně mluvit o tématu a reflektovat svůj postoj k němu. Autor práce se rozhodl ve výzkumu využít rozhovory s výše uvedeným zdravotnickým personálem a bezpečnostními experty.

Analýza v IPA začíná detailním prozkoumáním jednoho případu a postupně přechází k dalším případům. Cílem je formulovat témata, která zachycují esenci zkoumaného fenoménu. Tento proces zahrnuje opakované čtení textu, psaní počátečních poznámek, rozvíjení témat a hledání souvislostí mezi nimi. Vzhledem k zacílení tématu došlo k vytvoření základního rámce počátečních otázek pro každého osloveného respondenta.

Interpretace v IPA je úzce zakotvena v textu a přiznává, že je to vždy výzkumník se svým životním kontextem, kdo je jejím autorem. Výzkumník tvoří interpretace na základě dialogu s textem a svými zkušenostmi, což zajišťuje, že analýza je transparentní a důvěryhodná.[186]

Prezentace výsledků v IPA kombinuje perspektivu témat a jednotlivých případů. Interpretace by měly poukazovat na jedinečný způsob, jakým je dané téma významné pro jednotlivce. Výsledky proto budou strukturovány podle hlavních témat, doplněny komentáři a přímými citacemi respondentů, což činí výzkum transparentním a umožňuje ověřit si naše tvrzení.[187]

3.3.2 Metody kvalitativní analýzy dat

Poté, co byla shromážděna kvalitativní data, je nutné z nich získat patřičné informace, skutečnosti a vzájemné vazby. Na základě interpretačních postupů lze dospět ke konkrétním závěrům nebo teoriím. Samotnou analýzu dat v kontextu této práce vnímáme jako kontinuální metodu, která začala sběrem dat a pokračuje plynule až do okamžiku dosažení výzkumného cíle v podobě vytvoření optimálního modelu bezpečnosti zdravotních dat chráněných osob.

Autor v rámci kvalitativní analýzy dat zvolil jako patřičné nástroje kombinaci již zmíněné metody IPA, kvalitativní obsahové analýzy a zejména metody reduktivní deskripce. Tyto metody umožňují systematické nenumerické organizování dat s cílem odhalit témata, pravidelnosti, datové konfigurace, formy, kvality a vztahy.

Z hlediska analýzy dat se IPA zaměřuje na hluboké porozumění osobním zkušenostem účastníků výzkumu. V kontextu této práce IPA pomáhá identifikovat a interpretovat individuální vnímání a zkušenosti zdravotnických pracovníků a chráněných osob v oblasti bezpečnosti zdravotních dat.

Kvalitativní obsahová analýza zahrnuje systematické kódování a kategorizaci textových dat, s cílem identifikovat vzorce a tematické struktury v datech. V rámci této práce byla využita k analýze dokumentů, rozhovorů a dotazníkových šetření, aby bylo možné identifikovat a popsat hlavní témata a vzorce v oblasti bezpečnosti zdravotních dat.[188]

Metoda reduktivní deskripce byla použita k získání relevantních informací tím, že jednotlivé specifické projevy byly rozčleněny do společných větších významových jednotek podle společných faktorů (kategorií). Smyslem této metody je redukce pozorování bohatosti chování tak, že jednotlivé specifické projevy lze zařadit do společných větších významových jednotek – do kategorií. Pozorovatel vyznačuje jevy a události do předem připravených formulářů a schémat s připravenými kategoriemi (typy) chování, což je možné výborně aplikovat právě na problematiku disertační práce ve vztahu k danému tématu.[174]

Základní princip uvedené metody spočívá ve srovnávání a agregaci dat, kdy se empiricky získaná data porovnávají s určenou kategorií (vzorem), jež patří k navrženému typu případu. Kategorie (faktory) tvoří předem připravený rámec, do něhož lze zaznamenávat frekvenci výskytu určité skupiny pozorovaných a analyzovaných projevů odpovídajících vytvořené kategorii. Pokud výsledková konfigurace dat souhlasí, výsledek potvrzuje nějaké tvrzení.[174]

V rámci výzkumné části této práce dojde tedy k získání dat o bezpečnostních opatřeních a praxích ve zdravotnických zařízeních při hospitalizaci chráněných osob. Získaná data budou společně s kvantitativními daty podkladem pro dosažení cílů práce (viz dále).

Použitím kombinace interpretativní fenomenologické analýzy a kvalitativní obsahové analýzy bude možné získat hluboký a strukturovaný pohled na bezpečnost zdravotních dat a principy poskytování zdravotní péče chráněným osobám, identifikovat klíčová rizika a navrhnout efektivní opatření k jejich minimalizaci.

3.3.3 Metody kvantitativního sběru dat

Na základě metod kvantitativního výzkumu je možné získat potřebná data, analyzovat je a následně za pomoci různých metod vyhodnotit. Velmi důležité jsou metody určené pro sběr dat, neboť způsob, kterým je možné kvantitativní data získat, velmi ovlivňuje jejich kvalitu. Samotné získávání dat má totiž vliv nejen na jejich kvalitu, ale i strukturu. Jedná se o prostředek, díky kterému je možné nalézt vhodné interpretace daných problémových oblastí.

Jak bylo stanoveno výše, vyřešení jednotlivých výzkumných problémů, a tedy i dosažení cílů práce, bude možné zejména na základě kombinace kvantitativních a kvalitativních výzkumných metod. V rámci vytyčených problémových otázek došlo k vymezení tří hypotéz, jejichž potvrzením či vyvrácením bude možné dosáhnout cílů této práce.

K dosažení cílů této práce bylo zapotřebí zvolit metodu, která by svou podstatou umožnila obsáhnout všechny tři zmíněné hypotézy. Jako nejvhodnější výzkumná metoda pro sběr kvantitativních dat byla zvolena metoda dotazníkového šetření.

Dotazníky byly vytvořeny na základě kvalitativních výzkumných metod, a to analýzy pracovních činností zdravotnických zaměstnanců a potřeb chráněných osob ve zdravotnických zařízeních. Rovněž byla provedena analýza dostupných odborných pramenů obsahujících informace o poskytování zdravotních služeb chráněným osobám. Na základě uvedeného kroku došlo k sestavení finálních dotazníků autorem, kdy jednotlivé otázky dotazníků byly uspořádány tak, aby pokryly klíčové oblasti zájmu. Finální znění a podoba dotazníků byla konzultována rovněž s několika odborníky z praxe.

Dotazníky byly rozděleny a zacíleny na tři části:

1) poskytování zdravotní péče chráněným osobám,
2) fyzická bezpečnost a
3) virtuální bezpečnost.

Dotazníky byly určeny dvěma skupinám respondentů:

1) **Dotazník pro pracovníky ve zdravotnictví**

   První část dotazníku se zaměřuje na poskytování zdravotní péče chráněným osobám. Otázky v této části zjišťují, zda mají zdravotnická zařízení nastavena speciální pravidla pro poskytování zdravotní péče chráněným osobám, jakým způsobem jsou zaměstnanci informováni o těchto pravidlech, a jaké zkušenosti mají respondenti s péčí o chráněné osoby.

   Druhá část dotazníku se věnuje fyzické bezpečnosti chráněných osob. Otázky se zaměřují na to, kdo je odpovědný za nastavení bezpečnostních opatření, jaká opatření jsou přijímána, jak přítomnost ochranky chráněné osoby zasahuje do procesů zařízení, a jak jsou zaměstnanci informováni o pravidlech pro zajištění bezpečnosti.

   Třetí část dotazníku se zaměřuje na virtuální/kybernetickou bezpečnost chráněných

osob. Otázky zjišťují, zda mají zdravotnická zařízení nastavena speciální pravidla pro zajištění kybernetické bezpečnosti chráněných osob, jaká opatření jsou přijímána k ochraně dat, a jak jsou zaměstnanci školeni ohledně nakládání a ochrany dat chráněných osob.

Dotazník obsahuje rovněž otázky, na které lze odpovědět volnou formou. Úplná podoba dotazníku viz příloha č. 2.

2) **Dotazník pro chráněné osoby**

Dotazník pro chráněné osoby byl navržen tak, aby získal přímé zkušenosti a názory chráněných osob na kvalitu a bezpečnost poskytovaných zdravotních služeb. Byl rozdělen do několika částí zaměřených na zkušenosti s hospitalizací, informovanost o speciálních pravidlech pro chráněné osoby, poskytované benefity, fyzickou bezpečnost a kybernetickou bezpečnost.

Otázky byly formulovány tak, aby umožnily zhodnotit zkušenosti chráněných osob s péčí, přidělováním ošetřujících lékařů, bezpečnostními opatřeními a ochranou jejich osobních a zdravotních dat. Respondenti měli možnost hodnotit úroveň poskytovaných služeb, vyjádřit svůj názor na legitimitu zvláštního zacházení a navrhnout zlepšení v poskytovaných službách.

Dotazník obsahuje rovněž otázky, na které lze odpovědět volnou formou. Úplná podoba dotazníku viz příloha č. 3.

3.3.4 Metody kvantitativní analýzy dat

Data získaná kvantitativními metodami, zejména prostřednictvím dotazníkových šetření, je možné zpracovávat různými analytickými technikami, které umožní odhalit důležité informace a vztahy. V rámci práce se autor zaměřil na použití kvalitativní obsahové analýzy jako hlavní metody pro zpracování dat. Tato metoda umožňuje hlubší pochopení zkoumaných jevů a identifikaci klíčových témat, která jsou zásadní pro návrh efektivních bezpečnostních opatření pro ochranu dat chráněných osob ve zdravotnických zařízeních.

Postup kvalitativní obsahové analýzy

Po shromáždění dat z dotazníků byla data systematicky připravena pro další analýzu. Tento proces zahrnoval standardizaci odpovědí z uzavřených otázek a strukturování dat z otevřených otázek pro zajištění konzistentního zpracování. Namísto tradičního kódování byla použita

metoda **deskriptivní statistické analýzy**, kdy byly odpovědi respondentů prezentovány prostřednictvím grafů a vizualizací, které umožnily přehledné znázornění trendů a opakujících se vzorců.

Následná kvalitativní obsahová analýza byla provedena prostřednictvím interpretace těchto grafických zobrazení, přičemž se výzkum zaměřil na identifikaci klíčových témat a oblastí souvisejících s bezpečností dat chráněných osob. Tento přístup umožnil logické odhalení hlavních rizik a slabých míst v oblasti fyzické a kybernetické ochrany dat. Místo selektivního kódování byly klíčové oblasti zájmu definovány na základě opakujících se vzorců, které se ukázaly ve vizualizovaných datech.

Výsledky analýzy byly tedy prezentovány pomocí grafů a vizuálních zobrazení, které ukazují procentuální zastoupení jednotlivých kódovaných oblastí. Grafy poskytují přehled o tom, jak často se jednotlivé klíčové kategorie vyskytovaly v odpovědích respondentů, což usnadňuje identifikaci nejvýznamnějších problémů a oblastí vyžadujících pozornost. Tímto způsobem bylo možné kvalitativně vyjádřit kvantitativní data a lépe tak vizualizovat a interpretovat hlavní závěry studie.

Interpretace těchto dat umožnila hlubší pochopení vztahů mezi identifikovanými tématy a bezpečností dat chráněných osob. Na základě procentuálního zastoupení jednotlivých kategorií byly identifikovány hlavní problémy a oblasti vyžadující zlepšení. Z těchto zjištění byly formulovány konkrétní závěry a doporučení pro praxi, zaměřené na zvýšení úrovně bezpečnosti a ochrany dat ve zdravotnických zařízeních. (viz kapitola 5).

3.4 Výzkumné postupy

Jak bylo již nastíněno výše, celý výzkum je koncipován tak, že dochází ke kombinaci kvantitativních a kvalitativních výzkumných metod. Z toho důvodu byly rovněž i výzkumné postupy prostoupeny oběma zmíněnými druhy výzkumných metod. Výzkumné postupy bylo proto možné členit následovně:

1) přípravná fáze,
2) fáze získávání dat,
3) fáze analýzy a klasifikace informací.

3.4.1 Přípravná fáze

Přípravná fáze předcházela vlastnímu sběru dat a zahrnovala vytvoření základní platformy pro výzkum. Cílem bylo identifikovat klíčové pracovní pozice ve zdravotnických zařízeních, získat informace o cílech a strategických záměrech organizací ve vztahu k ochraně dat chráněných osob. Rovněž bylo nutné prostudování organizační struktury zdravotnických zařízení, zejména jakým způsobem jsou řízeny a jaké bezpečnostní protokoly mají zavedeny. Tato fáze také zahrnovala získání přístupu k relevantním dokumentům a přípravě výzkumných nástrojů, jako jsou dotazníky a průvodci pro polostrukturované rozhovory.

3.4.2 Fáze získávání dat

Fázi získávání dat je možné z hlediska konkrétního postupu autora práce rozdělit rovněž do několika dílčích fází:

1) Analýza a studium platných právních předpisů a interních aktů řízení.
2) Kvalitativní výzkum prostřednictvím polostrukturovaných rozhovorů.
3) Kvantitativní výzkum formou dotazníkového šetření

Ad 1) Analýza a studium platných právních předpisů a interních aktů řízení

Nejprve bylo nutné se zabývat aktuálními znalostmi a předpisy týkajícími se ochrany dat ve zdravotnických zařízeních. Pracovní proces jako takový je tvořen soustavou pracovních úkolů, pracovních činností či samostatných pracovních operací, které jsou základním elementem všech činností. Autor práce se zabýval jejich identifikací z hlediska současných požadovaných nároků na uvedené pracovníky a bezpečnostní opatření.

Tato fáze zahrnuje právní pohled a požadavky zákonů. Nejprve bylo analyzováno nařízení GDPR a jeho aplikace v kontextu ochrany osobních a zdravotních dat chráněných osob. Nařízení GDPR stanovuje přísné požadavky na ochranu osobních údajů, včetně principů zpracování dat, práv subjektů údajů, povinnosti správců a zpracovatelů dat, a sankcí za nedodržení předpisů. Zejména pak byla analyzována ustanovení týkající se možnosti zpracování osobních údajů bez souhlasu subjektu osobních údajů.

Dále byl proveden přezkum relevantních národních právních předpisů, které upravují ochranu osobních a zdravotních dat ve zdravotnických zařízeních, a posouzení jejich souladu s GDPR a dalšími mezinárodními standardy. Následovalo studium interních předpisů zdravotnických

zařízení, které se vztahují k ochraně dat a kybernetické bezpečnosti, s cílem identifikovat a analyzovat zavedené postupy a jejich efektivitu.

Kromě právních aspektů byly také zohledněny zahraniční zkušenosti a odborné studie. Přezkum zahrnoval zkušenosti se sdílením dat a kybernetickou bezpečností v rámci NATO a Evropské unie. Byly analyzovány případové studie a doporučení týkající se ochrany citlivých dat v mezinárodním kontextu, se zaměřením na nejlepší praxe a výzvy, kterým čelí členské státy při ochraně zdravotních dat.

V neposlední řadě bylo provedeno studium odborných studií a literatury zabývající se ochranou osobních a zdravotních dat v různých zemích. Byly identifikovány klíčové přístupy a strategie, které byly úspěšně implementovány v zahraničí a které by mohly být aplikovány i v českém zdravotnickém kontextu. Tímto způsobem byl vytvořen komplexní a odborný základ pro další fáze výzkumu, zaměřený na zajištění optimální úrovně bezpečnosti a ochrany dat chráněných osob ve zdravotnických zařízeních.

Ad 2) Kvalitativní výzkum prostřednictvím polostrukturovaných rozhovorů

Bylo nutné provést polostrukturované rozhovory s odborníky na fyzickou a kybernetickou bezpečnost ve zdravotnictví a předními světovými zdravotníky, aby bylo možné získat hluboké a kvalitní informace o současných praktikách, problémech a potenciálních řešeních. Rozhovory poskytly cenné poznatky o reálných zkušenostech a výzvách, kterým čelí zdravotnická zařízení při ochraně dat chráněných osob. V tomto kontextu lze odkázat na metodu IPA (viz část 3.3.1 a 3.3.2 této práce).

- **Příprava a realizace rozhovorů**

Rozhovory byly navrženy jako polostrukturované, aby bylo možné získat detailní a hluboké informace, přičemž se zároveň umožnila určitá flexibilita v průběhu rozhovoru. Tento přístup umožnil reagovat na specifické poznatky a zkušenosti respondentů. Každý rozhovor byl rozdělen do tří hlavních oblastí: **poskytování zdravotní péče, fyzická bezpečnost a virtuální bezpečnost chráněných osob**. Pro každou oblast byl předem definován okruh otázek, které byly respondentům pokládány.

- **Kontaktní a souhlasný proces**

Veškeré rozhovory byly provedeny osobně. Respondenti byli kontaktováni přímo se žádostí o účast na výzkumu. Byl zajištěn anonymní charakter rozhovorů, což bylo explicitně

komunikováno a s čímž respondenti vyjádřili souhlas. Anonymita byla klíčová pro zajištění otevřenosti a upřímnosti odpovědí. Před každým z rozhovorů proběhlo jejich právní poučení o dobrovolnosti účasti na výzkumu a byli podrobně seznámeni s obsahem a metodikou výzkumu. V případě potřeby všichni respondenti souhlasili s jejich zpětnou identifikací.

- **Výběr respondentů**

Výběr respondentů byl pečlivě plánován a konzultován se školitelem. Proběhlo prvotní vytipování na základě následujících kritérií:

- Odborná kvalifikace: Respondenti museli mít relevantní odborné vzdělání a kvalifikaci v oblasti zdravotnictví, kybernetické bezpečnosti nebo fyzické bezpečnosti.
- Praktické zkušenosti: Respondenti museli mít rozsáhlé praktické zkušenosti s péčí o chráněné osoby, což zahrnovalo jak klinickou praxi, tak vysoké manažerské pozice.
- Vědecké a odborné publikační aktivity: Upřednostňováni byli respondenti s aktivními publikačními aktivitami ve vědeckých a odborných časopisech.
- Rozsah odpovědnosti: Výběr zahrnoval respondenty na různých, však vrcholových, úrovních odpovědnosti, včetně ředitelů a náměstků, klinických lékařů, IT specialistů a manažerů kybernetické bezpečnosti.
- Geografická a institucionální diverzita: Respondenti byli vybíráni z různých zdravotnických zařízení, včetně velkých fakultních zdravotnických zařízení a specializovaných klinik, aby byla zajištěna reprezentativnost vzorku. Respondenti museli v souhrnu déle než rok působit v zahraničí nebo mít zkušenosti ze zahraničí. Někteří respondenti byli zaměstnanci zahraničních zdravotnických zařízení (Německo, Izrael, Slovensko).

Celkem bylo provedeno 10 rozhovorů. Respondenti byli vybíráni na základě stanovených kritérií.

- **Kumulativní funkce respondentů**

Vzhledem k požadavku na zachování anonymity a zabránění zpětné identifikace respondentů jsou kumulativní funkce respondentů popsány následovně: ředitel středně velkého fakultního zdravotnického zařízení (více než 2000 zaměstnanců), náměstek velkého fakultního

zdravotnického zařízení, přednosta nebo primář kliniky, docent nebo profesor, lékař, manažer kybernetické bezpečnosti, voják, vojenský lékař, specialista IT, specialista kybernetické bezpečnosti, bezpečnostní ředitel. Tito respondenti poskytli cenné a detailní informace, které byly klíčové pro analýzu a návrh bezpečnostních opatření pro ochranu dat chráněných osob ve zdravotnických zařízeních.

Tabulka č. 1: Rozdělení respondentů dle jejich zkušeností; Zdroj: autor (2024)

Označení respondenta	Délka zkušenosti ve zdravotnictví (roky)	Počet chráněných osob, které ošetřili[36]
R1	20-25	Desítky
R2	35-40	Desítky až stovky
R3	25-30	Desítky až stovky
R4	25-30	Desítky až stovky
R5	20-25	Desítky až stovky
R6	30-35	Stovky
R7	20-25	Desítky
R8	15-20	Desítky
R9	45-50	Stovky
R10	20-25	Desítky až stovky

Ad 3) Kvantitativní výzkum formou dotazníkového šetření

Pro účely získání kvantitativních dat byly vytvořeny dva druhy dotazníků. Jeden pro zaměstnance zdravotnických zařízení a druhý pro samotné chráněné osoby (jejich obsah a zaměření viz předchozí podkapitola), aby poskytly kvantitativní data o vnímání bezpečnosti dat, zkušenostech s bezpečnostními incidenty a úrovni povědomí o bezpečnostních opatřeních. Dotazníky byly vytvořeny tak, aby pokryly široké spektrum otázek týkajících se ochrany nejen zdravotních dat, ale také i ostatních bezpečnostních otázek a principů poskytování zdravotní

[36] Počtem chráněných osob, které ošetřili, je myšleno, kolik chráněných osob ošetřili, léčili nebo museli v rámci svých pracovních činností nějakým způsobem řešit. Například v případě pracovníka IT se mohlo jednat o řešení požadavku zabezpečení dat v případě hospitalizace chráněné osoby apod.

péče obecně a byly dostupné prostřednictvím elektronické platformy Google. Dotazníky byly navrženy s ohledem na zachování anonymity respondentů a zajištění maximální upřímnosti odpovědí.

Dotazník pro chráněné osoby byl distribuován prostřednictvím e-mailových žádostí na velkou skupinu respondentů v rámci České republiky. Vždy došlo k oficiálnímu oslovení statutárního orgánu, ředitele, či vedoucího příslušného orgánu nebo přímo chráněné osoby s žádostí o možnost distribuce dotazníku mezi ostatní chráněné osoby či s žádostí přímo o jeho vyplnění. Jak samotné žádosti, tak dotazník, obsahovaly poučení o způsobu vyplnění, anonymitě a způsobu využití dat k výzkumným účelům s možností kontaktovat autora práce.

Dotazník byl distribuován na: všechny poslance Poslanecké sněmovny Parlamentu České republiky a zároveň všechny senátory Senátu Parlamentu České republiky; všechny velvyslance České republiky a jejich rodiny; všechny české prvoligové fotbalové kluby, hokejové kluby a basketbalové kluby; na české representanty v atletice a olympijské representanty; na všechny sportovce zařazené v rámci Armádního sportovního centra Dukla; na vybrané veřejně známé osobnosti (youtubery, zpěváky, moderátory, ostatní sportovce, umělce, herce atd.); na všechny hejtmany a jejich náměstky a na všechny starosty v rámci České republiky.

Kvalifikovaný odhad počtu oslovených respondentů byl 12.000 osob. **Dotazník pro chráněné osoby vyplnilo celkem 616 respondentů z České republiky**.

Dotazník pro zaměstnance zdravotnických zařízení byl distribuován oficiálně prostřednictvím e-mailových žádostí adresovaných statutárním orgánům všech českých poskytovatelů zdravotních služeb fakultního typu, krajských zdravotnických zařízení a vybraných okresních zdravotnických zařízení. Vždy došlo k oslovení statutárního orgánu s žádostí o možnost distribuce dotazníku mezi zaměstnance osloveného zdravotního zařízení za účelem jeho vyplnění. Jak samotné žádosti, tak dotazník, obsahovali poučení o způsobu vyplnění, anonymitě a způsobu využití dat k výzkumným účelům s možností kontaktovat autora práce.

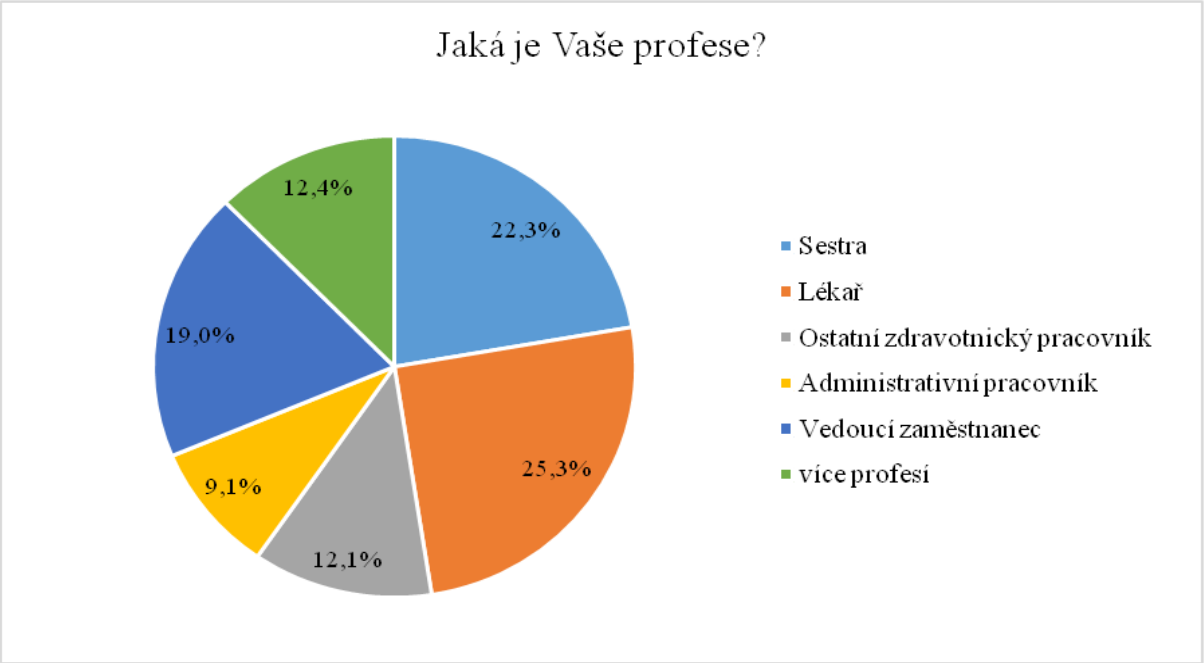
Kromě České republiky byl stejný dotazník distribuován v angličtině i na mezinárodní úrovni, a to na všech kontinentech kromě Antarktidy. Cílem bylo získat široké spektrum pohledů a zkušeností z různých geografických oblastí. Evropa byla rozdělena na regiony Severní, Jižní,

Střední, Východní a Západní, aby bylo možné lépe analyzovat rozdíly v přístupu k bezpečnosti dat a ochraně osobních údajů.

Kvalifikovaný odhad počtu oslovených respondentů v rámci České republiky i zahraničí byl 110.000. **Dotazník pro zdravotníky vyplnilo celkem 321 respondentů z České republiky a 95 respondentů ze zahraničí**.

Rozložení zahraničních respondentů bylo následující: 9 ze Severní Evropy, 8 z Východní Evropy, 7 z Jižní Evropy, 48 ze Západní Evropy, 5 ze Střední Evropy, 4 z Asie (Izrael) a 15 z Austrálie.

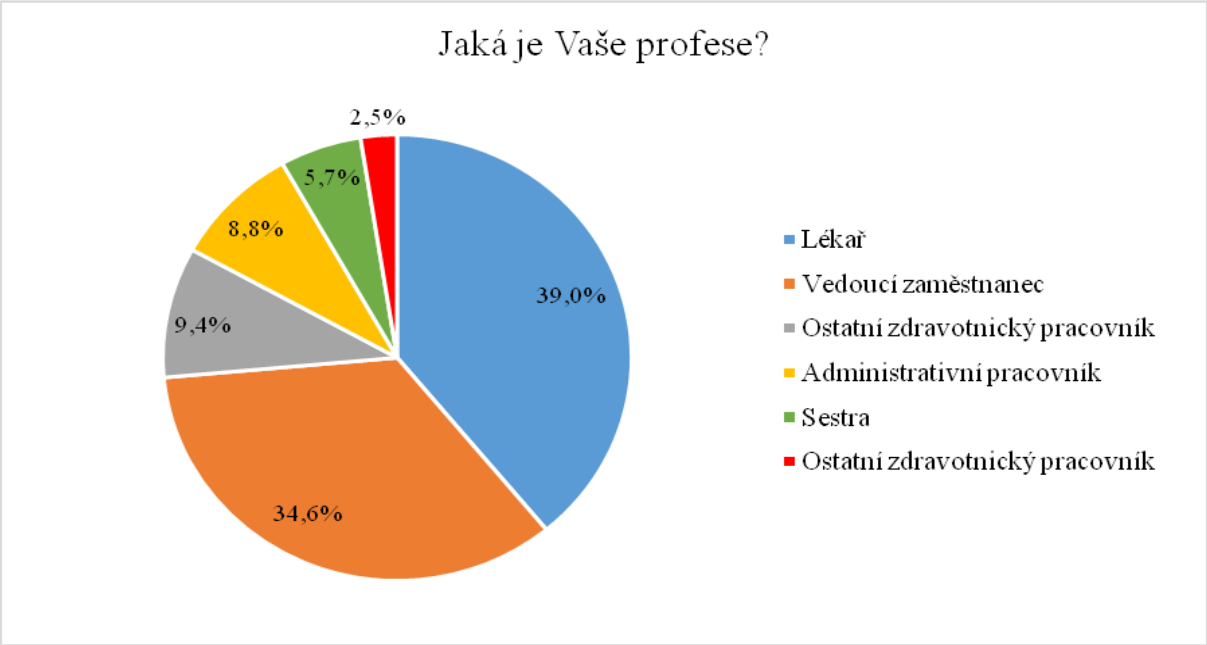
Graf 1: Rozdělení českých respondentů podle profese; Zdroj: autor (2024)



Na základě grafu č. 1 je zřejmé, že největší zastoupení mezi respondenty mají lékaři a sestry, což odpovídá klíčovým rolím, které tito profesionálové hrají ve zdravotnickém sektoru. Toto rozložení je významné pro výzkum, protože umožňuje získat vhled do specifických zkušeností a postojů těchto profesí, které mají přímý vliv na poskytování zdravotní péče. Dále, přítomnost vedoucích zaměstnanců naznačuje zapojení rozhodovací sféry, což poskytuje důležité informace o strategických a organizačních aspektech zdravotnických zařízení. Zahrnutí administrativních pracovníků a dalších zdravotnických pracovníků přispívá k širšímu pochopení podpůrných a specializovaných funkcí, které jsou také kritické pro chod zdravotnických zařízení.

Rozmanité zastoupení profesí, včetně respondentů vykonávajících více profesí, poskytuje komplexní pohled na zdravotnický sektor a umožňuje posoudit rozdílné perspektivy a přístupy, kdy největší zastoupení měla pozice lékaře a zároveň vedoucího zaměstnance. Tato pestrost dat je důležitá pro validitu výzkumu, protože reflektuje reálnou dynamiku a multifunkční povahu zdravotnického prostředí, čímž umožňuje zohlednit různé aspekty poskytování péče a řízení zdravotnických institucí.

Graf 1a: Rozdělení zahraničních respondentů podle profese; Zdroj: autor (2024)



Na základě zahraničních dat je zřejmé, že mezi respondenty převládají lékaři a vedoucí zaměstnanci. Toto rozložení naznačuje, že zahraniční průzkum byl zaměřen převážně na osoby s rozhodovacími pravomocemi a klíčovými rolemi ve zdravotnických zařízeních. Ostatní zdravotnický personál tvoří menší podíl respondentů, což odráží relativně nižší zapojení těchto rolí ve výzkumu. Zastoupení administrativních pracovníků ukazuje na jejich roli v podpůrných a organizačních funkcích. Sestry a ostatní zdravotnický pracovník mají nejmenší zastoupení, což může ovlivnit schopnost průzkumu zachytit jejich perspektivy na péči a interakci s pacienty.

Ve srovnání s českými daty je patrné, že v zahraničních zařízeních je výraznější podíl lékařů a vedoucích zaměstnanců (39 % lékařů a 34,6 % vedoucích zaměstnanců oproti 25,3 % lékařů a 19 % vedoucích zaměstnanců v českých datech). To naznačuje, že ze zahraničních dat bude možné interpretovat více zkušeností od vedoucích zaměstnanců v rozhodovacích pozicích.

Naopak, český vzorek zahrnuje větší zastoupení sester (22,3 % oproti 5,7 % v zahraničních datech) a ostatních zdravotnických pracovníků (12,1 % oproti 9,4 %).

3.4.3 Fáze analýzy a klasifikace informací

Rovněž zde došlo k rozdělení pracovního postupu do několika dílčích fází:

1) Vyhodnocení dat získaných z dotazníků a polostrukturovaných rozhovorů pomocí kvantitativních a kvalitativních výzkumných metod.
2) Interpretace získaných dat.
3) Kombinace kvalitativních a kvantitativních dat.
4) Analýza získaných dat.
5) Tvorba a definování doporučení a opatření pro praxi.
6) Vytvoření modelu pro zajištění bezpečného přenosu a zpracování zdravotních dat.

Ad 1) Vyhodnocení dat získaných z dotazníků a polostrukturovaných rozhovorů pomocí kvantitativních a kvalitativních výzkumných metod

Data získaná z dotazníků byla vyhodnocena pomocí statistických metod, které umožnily identifikaci hlavních trendů, problémů a úrovně bezpečnosti dat ve zdravotnických zařízeních, včetně principů poskytování zdravotní péče a zajištění fyzické bezpečnosti. Jak bylo zmíněno výše, primární metodou byla kvalitativní obsahová analýza.

Data získaná z polostrukturovaných rozhovorů budou vyhodnocena metodou IPA.

Ad 2) Interpretace získaných dat

Vyhodnocená data z dotazníků a rozhovorů byla rovněž interpretována, a to nejen v rámci jednotlivých odpovědí, ale také vzhledem k širšímu kontextu ochrany dat ve zdravotnických zařízeních. Tento proces zahrnuje analýzu hlavních témat a vzorců, které se objevily v rozhovorech a dotaznících. Bylo provedeno identifikování a popis klíčových témat a souvislostí mezi nimi.

Ad 3) Kombinace kvalitativních a kvantitativních dat

Data z kvalitativních a kvantitativních metod byla kombinována, aby poskytla komplexní obraz o zvolené problematice disertační práce. Tato triangulace dat umožnila ověřit a zpřesnit závěry a zajistit, že výsledky budou robustní a spolehlivé. Na jejich základě následně došlo k tvorbě základního rámce pro analýzu rizik.

Ad 4) Analýza získaných dat

Na základě získaných dat bude provedena jejich analýza. Cílem této fáze bylo identifikovat a vyhodnotit rizika spojená s ochranou dat chráněných osob, jejich fyzickou bezpečností a principy poskytování zdravotní péče ve zdravotnických zařízeních a navrhnout opatření pro jejich minimalizaci.

Ad 5) Fáze tvorby a definování doporučení a opatření pro praxi

V této fázi se veškeré poznatky získané během výzkumu promítnou do konkrétních doporučení a opatření, která budou prakticky využitelná ve zdravotnických zařízeních. Na základě provedených analýz a identifikovaných rizik budou definována klíčová opatření zaměřená primárně na zlepšení bezpečnosti, přenosu a zpracování zdravotních dat chráněných osob. Rovněž ale dojde k definování opatření a doporučení do oblastí poskytování zdravotní péče a fyzické bezpečnosti chráněných osob.

Cílem této fáze je vytvořit soubor konkrétních a realizovatelných kroků, které budou reflektovat jak technické, tak organizační aspekty poskytování zdravotní péče, zajištění fyzické i virtuální bezpečnosti. Doporučení budou navržena tak, aby byla v souladu s platnými legislativními rámci a mezinárodními standardy a aby bylo možné jejich efektivní implementaci do praxe zdravotnických zařízení. Tato fáze představuje klíčový přechod od teoretických závěrů k praktickému využití výsledků výzkumu.

Ad 6) Fáze vytvoření modelu pro zajištění bezpečného přenosu a zpracování zdravotních dat

Veškeré aktivity autora práce se promítnou právě do této fáze, která v sobě zahrnuje finální podobu modelu zabezpečení přenosu a zpracování dat chráněných osob ve zdravotnických zařízeních. Vytvoření tohoto modelu bude možné až po provedení všech analýz a syntézy získaných dat. Vlastní proces počítá s:

a) Návrhem modelu na základě analýzy dat.
b) Validací modelu prostřednictvím odborných konzultací.
c) Implementací a doporučeními.

Ad a) Návrh modelu na základě analýzy dat

Na základě interpretace výsledků a analýz budou navrženy konkrétní modely a postupy pro zajištění bezpečnosti dat chráněných osob. Tento model bude zahrnovat technická, organizační a právní opatření, která budou vycházet ze získaných informací a budou založena na nejnovějších poznatcích a osvědčených postupech.

Ad b) Validace modelu prostřednictvím odborných konzultací

Navržený model bude podroben odborným konzultacím s klíčovými stakeholders, aby byla zajištěna jeho praktická aplikovatelnost a efektivita. Bude se jednat o zpětnou vazbu od odborníků z oblasti zdravotnictví, kybernetické bezpečnosti a právní oblasti.

Ad c) Implementace a doporučení

Na základě navrženého modelu bude vytvořen implementační plán, který bude zahrnovat konkrétní kroky a opatření potřebná k jeho úspěšné implementaci ve zdravotnických zařízeních. Součástí budou také doporučení pro pravidelnou aktualizaci a přizpůsobování modelu novým hrozbám a technologickému vývoji. Tato fáze daleko přesahuje zadání této disertační práce a bude realizována jako kontinuální aktivita autora práce.

Díky tomuto komplexnímu přístupu bude možné vytvořit robustní a efektivní model zabezpečení dat chráněných osob, který bude přispívat ke zvýšení bezpečnosti a ochrany citlivých informací ve zdravotnických zařízeních.

3.5 Interpretace kvalitativní analýzy

V následující kapitole a dílčích podkapitolách budou interpretována získaná kvalitativní data na základě strukturovaných rozhovorů metodou IPA. Kvalitativní výzkum byl zaměřen na tři oblasti, které korespondují s názvy podkapitol: péče o chráněné osoby; fyzická a bezpečnostní opatření chráněných osob; virtuální a kybernetická bezpečnost chráněných osob.

Přepisy odpovědí respondentů ke každé z otázek jsou uvedeny v příloze č. 1. Odpovědi jsou vyhodnoceny v jejich celkovém kontextu i s ohledem na dílčí interpretace.

3.5.1 Péče o chráněné osoby

Otázka 1: Má Vaše zdravotní zařízení nastavena speciální pravidla pro poskytování zdravotní péče, bezpečnosti nebo virtuální bezpečnosti chráněným osobám?

Na základě odpovědí respondentů na první otázku, která se týkala existence speciálních pravidel pro poskytování zdravotní péče, bezpečnosti nebo virtuální bezpečnosti chráněným osobám, můžeme identifikovat několik klíčových aspektů, které reflektují současnou praxi v různých zdravotnických zařízeních.

Z odpovědí vyplývá, že přístup ke speciálním pravidlům pro chráněné osoby není jednotný a liší se v závislosti na konkrétním zdravotnickém zařízení. Někteří respondenti uvedli, že taková pravidla ve svém současném pracovišti nemají vůbec, zatímco jiní zmiňovali, že na předchozích pracovištích byla tato pravidla implementována, byť často jen v omezené míře nebo neformálně. Z tohoto lze vyvodit, že v některých zařízeních může chybět systémový přístup k ochraně chráněných osob, což může vést k inkonzistentnímu poskytování péče a bezpečnosti. Také je zřejmé, že i tam, kde jsou pravidla nastavena, nejsou vždy efektivně komunikována zaměstnancům, což může snižovat jejich účinnost.

Z výzkumného hlediska tato situace naznačuje potřebu standardizace přístupu k péči o chráněné osoby napříč různými zdravotnickými zařízeními. Dále je evidentní, že by měl být zvýšen důraz na formální komunikaci těchto pravidel a zajištění jejich dodržování, což by mohlo přispět k vyšší úrovni bezpečnosti a ochrany citlivých informací. Toto zjištění také poukazuje na možný deficit v legislativním rámci, který by měl jasněji definovat povinnosti a standardy pro péči o chráněné osoby v různých typech zdravotnických zařízení.

Celkově lze shrnout, že přístup ke speciálním pravidlům pro chráněné osoby je v současnosti nejednotný a vyžaduje systematickou změnu, která by zajistila vyšší úroveň péče a bezpečnosti pro tuto specifickou skupinu pacientů.

Otázka 2: Jak jsou tato pravidla komunikována zaměstnancům?

Odpovědi respondentů na druhou otázku, která se zaměřuje na způsob, jakým jsou pravidla pro poskytování zdravotní péče, bezpečnosti nebo virtuální bezpečnosti chráněným osobám komunikována zaměstnancům, ukazují na významný nedostatek formálního a systematického přístupu v této oblasti.

Většina respondentů uvedla, že pravidla buď nejsou komunikována vůbec, nebo jsou komunikována pouze neformálně. Někteří respondenti se dokonce museli sami aktivně zajímat o to, jak jsou tato pravidla aplikována, což poukazuje na absenci centralizovaného a strukturovaného postupu. Z tohoto vyplývá, že **zaměstnanci často nemají k dispozici jasné a konkrétní pokyny, jak se v situacích týkajících se chráněných osob chovat a jak zajistit jejich bezpečnost a ochranu jejich osobních údajů**. Tento stav může vést k inkonzistentní aplikaci pravidel a potenciálním rizikům pro bezpečnost jak pacientů, tak samotných zaměstnanců. Pokud nejsou pravidla jasně definována a komunikována, může to mít za následek různé interpretace a nejednotné postupy, což je v oblasti zdravotní péče velmi rizikové.

Z výzkumného hlediska je tento nedostatek alarmující a poukazuje na potřebu zavedení formálních, písemně kodifikovaných postupů, které budou pravidelně komunikovány a aktualizovány. Je nezbytné, aby pravidla byla nejen definována, ale také efektivně implementována a průběžně kontrolována. To by mohlo zahrnovat školení zaměstnanců, pravidelné porady a vytvoření přístupných metodických materiálů.

Lze shrnout, že současný stav komunikace pravidel týkajících se chráněných osob **je nedostatečný a představuje potenciální riziko**. Zajištění konzistentní a efektivní komunikace těchto pravidel je klíčové pro zajištění vysoké úrovně bezpečnosti a ochrany v rámci zdravotnických zařízení.

Otázka 3: Podílel jste se na tvorbě pravidel pro poskytování zdravotní péče chráněným osobám?

Odpovědi respondentů na třetí otázku ukazují na různé úrovně zapojení a přístupů. Většina respondentů uvedla, že se přímo nepodílela na tvorbě centrálních pravidel, ale někteří uvedli, že se snažili iniciovat ad hoc postupy v rámci svých týmů nebo oddělení.

Z odpovědí vyplývá, že existuje určitý stupeň iniciativy mezi jednotlivými odborníky, avšak tato iniciativa je často omezena na konkrétní situace a není podpořena širším organizačním rámcem. To opět naznačuje absenci formální struktury a systémového přístupu k problematice chráněných osob v mnoha zdravotnických zařízeních. Někteří respondenti uvedli, že jejich snaha o vytvoření nebo sjednocení pravidel nebyla vždy úspěšná, **což poukazuje na nedostatek podpory ze strany vyššího managementu**. To může být důsledkem

nedostatečného zájmu o tuto problematiku nebo neexistence legislativního či institucionálního tlaku na zavádění takových pravidel.

Je zřejmé, že nedostatek formálních pravidel a systémového přístupu představuje značné riziko pro konzistentnost a kvalitu péče o chráněné osoby. Je důležité, aby byla zavedena centrálně definovaná pravidla, která by byla závazná pro všechna zdravotnická zařízení. Tato pravidla by měla být vytvořena ve spolupráci s odborníky z praxe, kteří mají přímou zkušenost s péčí o chráněné osoby, aby byla zajištěna jejich efektivita a praktičnost.

Souhrnně lze konstatovat, že zapojení jednotlivých odborníků do tvorby pravidel pro chráněné osoby je často omezené a nesystematické, což vyžaduje zavedení formálních procesů a podpory ze strany vyššího managementu. Tento krok by mohl významně přispět ke zvýšení kvality a bezpečnosti poskytované péče.

Otázka 4: Myslíte si, že chráněným osobám je v praxi poskytována vyšší kvalita nebo rozsah zdravotní péče ve srovnání s běžnými pacienty?

Odpovědi respondentů na čtvrtou otázku odhalují určitou nejednotnost v přístupu a vnímání této otázky. Většina respondentů se shodla na tom, že z medicínského hlediska by nemělo docházet k žádné diskriminaci mezi Chráněnými osobami a běžnými pacienty, pokud jde o kvalitu a rozsah poskytované lékařské péče. Lékařské postupy by měly být aplikovány stejně bez ohledu na postavení pacienta. Někteří však připustili, že chráněné osoby mohou mít rychlejší přístup k péči nebo lepší podmínky, například v podobě lepších pokojů či přednostního ošetření. To je často motivováno snahou ochranky nebo samotného zdravotnického zařízení co nejrychleji zajistit péči a uvolnit kapacity, což může vést k určitému privilegovanému zacházení.

Tento rozdíl mezi ideálem a realitou může být způsoben tlakem na rychlé a efektivní ošetření chráněných osob, aby se minimalizovala jejich přítomnost ve zdravotnickém zařízení a snížilo se riziko pro jejich bezpečnost. Tímto způsobem může docházet k určitému upřednostňování, které však není odůvodněno medicínskými potřebami, ale spíše organizačními nebo bezpečnostními důvody, což považuji za legitimní.

Popsaná situace vyvolává otázky o rovnosti přístupu ke zdravotní péči. Přestože by měla být zajištěna stejná kvalita péče pro všechny pacienty, v praxi může docházet k odlišnostem, které jsou spíše výsledkem vnějších tlaků než medicínských potřeb. Toto zjištění **naznačuje potřebu**

důsledněji aplikovat principy rovnosti v poskytování zdravotní péče, aby nedocházelo k nerovnému zacházení, které by mohlo ohrozit důvěru ve zdravotnický systém.

Lze vyvodit, že zatímco medicínské standardy by měly být pro všechny pacienty stejné, v praxi se objevují případy, kdy chráněné osoby dostávají určité výhody, které nejsou přímo spojené s kvalitou lékařské péče, ale spíše s organizačními potřebami nebo bezpečnostními opatřeními. Tento trend by měl být sledován a analyzován, aby bylo možné zajistit spravedlivý přístup ke zdravotní péči pro všechny pacienty.

Otázka 5: Jaká konkrétní opatření a služby jsou poskytovány chráněným osobám nad rámec standardní péče?

Odpovědi respondentů odhalují několik společných prvků, které se opakují napříč různými zdravotnickými zařízeními. Všichni respondenti zmínili, že chráněné osoby často dostávají přednostní nebo rychlejší přístup k vyšetřením a léčbě. Tento přístup je motivován snahou minimalizovat dobu, po kterou jsou tyto osoby vystaveny možnému riziku, a zajistit jejich rychlý návrat k plnění jejich společenských či politických funkcí. Někteří respondenti také uvedli, že chráněným osobám jsou často poskytovány lepší podmínky na pokojích, například samostatné pokoje, což zvyšuje jejich komfort a bezpečnost.

Dalším zmiňovaným aspektem bylo, že ve výjimečných případech dochází k logistickým opatřením, kdy je zajištěn speciální transport nebo asistence během pobytu ve zdravotnickém zařízení, aby se minimalizoval kontakt s jinými pacienty a personálem. Tato opatření a služby nad rámec standardní péče nejsou vždy přímo vázána na zdravotní potřeby, ale spíše na ochranu soukromí a bezpečnosti chráněných osob. To může vést k rozdílům v přístupu k péči mezi chráněnými osobami a běžnými pacienty, což opět vyvolává otázky o rovnosti v přístupu ke zdravotní péči.

Z výzkumného hlediska je zřejmé, že existuje určitá neformální praxe poskytování nadstandardních služeb chráněným osobám, která je motivována spíše organizačními a bezpečnostními důvody než medicínskými potřebami. Tento přístup by měl být pečlivě analyzován, aby se zjistilo, zda je skutečně nezbytný, a aby se zajistilo, že nedochází k nepřiměřenému upřednostňování této skupiny pacientů na úkor ostatních.

Chráněné osoby tedy často dostávají nadstandardní služby a péči, které nejsou vždy založeny na jejich zdravotních potřebách, ale spíše na snaze zajistit jejich bezpečnost a ochranu soukromí. Tento přístup by měl být zvažován v kontextu rovnosti přístupu ke zdravotní péči

a potenciálního dopadu na ostatní pacienty, zejména by pak měla existovat jasná pravidla, která by tento přístup a postupy legitimizovala, čímž by došlo k odstranění předsudků či názorů zpochybňujících poskytování zdravotní péče chráněným osobám. Díky pravidlům by došlo k vysvětlení případů přednostního ošetření, právě z důvodu zachování určité požadované míry bezpečnosti chráněných osob se zachováním standardních postupů co do rozsahu a kvality v oblasti poskytování zdravotní péče.

Otázka 6: Jaké jsou nejčastější problémy plynoucí z Vašich zkušeností, se kterými se setkáváte při péči o chráněné osoby?

Dle odpovědí respondentů na šestou otázku je jedním z nejčastěji zmiňovaných problémů obtížnost v ochraně utajovaných skutečností a citlivých informací o zdravotním stavu chráněných osob. Někteří respondenti upozorňují na nejasnosti a složitost při rozhodování, kdy a jak informovat nadřízené nebo příslušné instituce o zdravotním stavu těchto osob. Tento problém je dále komplikován politickými tlaky, které mohou ovlivnit objektivní hodnocení zdravotního stavu a schopnosti chráněných osob vykonávat své funkce.

Další výzvou je zajištění bezpečnosti a ochrany chráněných osob během jejich pobytu ve zdravotnickém zařízení. Respondenti uvádějí, že je často obtížné zajistit, aby nebyly chráněné osoby vystaveny dalšímu riziku, což vyžaduje speciální organizační opatření, která mohou komplikovat běžný provoz zdravotnického zařízení.

Také se objevuje problém se stanovením hranic mezi poskytováním péče a respektováním autonomie chráněných osob. Někteří respondenti zmiňují, že je těžké určit, za jakých podmínek by měla být chráněná osoba považována za neschopnou vykonávat svou funkci a jak tuto informaci vhodně komunikovat.

Zmíněné problémy poukazují na potřebu jasnějších a konzistentnějších pravidel a postupů, které by zdravotnickému personálu usnadnily práci s chráněnými osobami. Je zřejmé, že **současná praxe není vždy efektivní a může vést k nedorozuměním, nesprávným rozhodnutím nebo dokonce k ohrožení bezpečnosti a zdraví chráněných osob**.

Závěry směřují ke konstatování, že péče o chráněné osoby přináší řadu specifických problémů, které vyžadují pečlivé zvažování a často i ad hoc řešení. Pro zajištění kvalitní péče a ochrany těchto osob by bylo vhodné vytvořit jasné a závazné postupy, které by byly systematicky komunikovány a implementovány ve všech zdravotnických zařízeních.

3.5.2 Fyzická a bezpečnostní opatření chráněných osob

Otázka 1: Kdo je odpovědný za nastavení bezpečnostních opatření?

Odpovědi respondentů na první otázku ve druhé sekci, která zkoumá odpovědnost za nastavení bezpečnostních opatření při hospitalizaci chráněných osob, ukazují na jednotný konsensus ohledně toho, kdo nese tuto odpovědnost. Všichni respondenti jednoznačně identifikovali bezpečnostního ředitele jako klíčovou osobu zodpovědnou za nastavení a implementaci bezpečnostních opatření v rámci zdravotnického zařízení. Vedle něj byla opakovaně zmiňována také role přednosty kliniky nebo ošetřujícího lékaře, kteří mají zodpovědnost za konkrétní opatření na klinice, kde je chráněná osoba hospitalizována.

Tento přístup ukazuje na hierarchickou strukturu odpovědnosti, kde se bezpečnostní ředitel stará o generální bezpečnostní opatření a jejich koordinaci, zatímco přednostové klinik a ošetřující lékaři zajišťují jejich implementaci v praxi. Toto rozdělení odpovědnosti je logické, protože zajišťuje, že bezpečnostní opatření jsou přizpůsobena specifickým potřebám a podmínkám jednotlivých klinik.

Z pohledu autora práce je důležité, že existuje jasná struktura odpovědnosti, která umožňuje efektivní řízení bezpečnostních opatření. Tato struktura by měla být podporována jasně definovanými postupy a pravidly, které by zajistily, že všechny zúčastněné strany vědí, jaké jsou jejich povinnosti a jakým způsobem mají jednat v případě, že dojde k hospitalizaci chráněné osoby. Je také důležité zajistit, aby existovaly mechanismy pro pravidelné hodnocení a aktualizaci těchto opatření, aby byly vždy v souladu s aktuálními riziky a potřebami.

Dle názoru autora lze konstatovat, že odpovědnost za bezpečnostní opatření při hospitalizaci chráněných osob je vnímána jako dobře definovaná a rozdělena mezi několik klíčových aktérů, což umožňuje efektivní a cílenou ochranu těchto pacientů v rámci zdravotnických zařízení, a to napříč různými státy.

Otázka 2: Jaký vliv má přítomnost ochranky chráněné osoby na procesy ve Vašem zařízení?

Odpovědi respondentů ukazují na výrazně negativní dopad této přítomnosti na běžný chod zdravotnického zařízení. Všichni respondenti se shodují na tom, že přítomnost ochranky způsobuje komplikace a narušuje standardní procesy ve zdravotnickém zařízení. Respondenti

opakovaně zmiňují zvýšený stres mezi personálem, omezení přístupu jiných pacientů k vyšetřením a obecnou komplikaci v efektivitě práce.

Jedním z hlavních problémů je, že **ochranka často zvyšuje tlak na personál**, což může vést k chybám nebo zpožděním v poskytování péče. Omezení přístupu k určitým prostorám nebo snížený počet osob, které mohou být přítomny při vyšetřeních, dále snižují efektivitu provozu zdravotnického zařízení. Tato omezení mají přímý dopad nejen na péči o chráněnou osobu, ale také na ostatní pacienty, kteří mohou být nuceni čekat déle na vyšetření nebo léčbu.

Zmíněná situace poukazuje na potřebu lepšího řízení a koordinace mezi ochrankou a nemocničním personálem. Je třeba najít rovnováhu mezi zajištěním bezpečnosti chráněné osoby a udržením co nejplynulejšího provozu zdravotnického zařízení. To by mohlo zahrnovat jasně definované protokoly a lepší komunikaci mezi bezpečnostními složkami a zdravotnickým personálem, aby byla minimalizována narušení běžných procesů.

Přítomnost ochranky chráněné osoby tedy má významný negativní vliv na procesy ve zdravotnických zařízeních, což může zhoršit nejen pracovní podmínky personálu, ale také kvalitu a dostupnost péče pro ostatní pacienty. Tento problém by měl být řešen prostřednictvím lepšího plánování a spolupráce mezi všemi zúčastněnými stranami, subjekty a složkami.

Otázka 3: Jsou jiní pacienti omezeni činností ochranky chráněné osoby?

Respondenti na třetí otázku druhé sekce vykreslují poměrně jednoznačný obraz. Všichni respondenti souhlasí s tím, že přítomnost ochranky má negativní dopad na ostatní pacienty, což se projevuje v různých formách omezení.

Často zmiňují omezení přístupu k vyšetřením, kdy je například omezena přítomnost jiných pacientů v blízkosti chráněné osoby. Toto omezení může způsobit zdržení nebo snížení dostupnosti zdravotní péče pro ostatní pacienty, což může mít vliv na jejich komfort a kvalitu poskytované péče. **Přítomnost ochranky také způsobuje organizační komplikace**, které mohou vést ke zmatku a narušení standardního provozu zdravotnického zařízení.

Tato zjištění naznačují, že zatímco bezpečnost chráněných osob je prioritou, nelze přehlížet dopad, který má tato bezpečnostní opatření na ostatní pacienty. Pro zajištění spravedlivého a efektivního fungování zdravotnického zařízení je nutné najít způsoby, jak minimalizovat tyto dopady, například lepší koordinací a plánováním přítomnosti ochranky, aby se zamezilo nadměrným omezením pro ostatní pacienty.

Z výzkumného hlediska je důležité zaměřit se na vývoj strategií, které umožní efektivní ochranu chráněných osob, aniž by to vedlo k nadměrným omezením pro ostatní pacienty. Tento problém by měl být součástí širší diskuze o rovnosti přístupu ke zdravotní péči a o tom, jak zajistit, aby bezpečnostní opatření nevedla k neúměrnému znevýhodnění ostatních pacientů.

Dle názoru autora lze tvrdit, že přítomnost ochranky chráněných osob omezuje jiné pacienty a narušuje běžný chod zdravotnických zařízení. Tato omezení by měla být minimalizována prostřednictvím lepšího plánování a koordinace mezi ochrankou a zdravotnickým personálem, aby bylo zajištěno, že ostatní pacienti nebudou zbytečně ovlivňováni těmito opatřeními.

Otázka 4: Jaká opatření jsou přijímána pro zajištění fyzické bezpečnosti personálu v přítomnosti chráněných osob?

Odpovědi respondentů ukazují na zásadní nedostatek v této oblasti. Většina respondentů uvedla, že žádná specifická opatření pro zajištění fyzické bezpečnosti personálu nejsou přijímána. Tento fakt poukazuje na podceňování rizik, kterým může být zdravotnický personál vystaven v přítomnosti chráněných osob.

Zodpovědnost za bezpečnost personálu je v mnoha případech přehlížena, ačkoli přítomnost chráněné osoby, zejména pokud je doprovázena ochrankou, může představovat určité bezpečnostní riziko. Někteří respondenti se zmiňovali o situacích, kdy byl ve zdravotnickém zařízení hospitalizován vězeň, což zvýšilo riziko pro personál, aniž by byla přijata adekvátní bezpečnostní opatření.

Tento nedostatek opatření může vést k potenciálně nebezpečným situacím, které by mohly ohrozit nejen samotný personál, ale také ostatní pacienty. Je zřejmé, že existuje potřeba zavedení jasných a závazných bezpečnostních protokolů, které by zahrnovaly ochranu zdravotnického personálu v situacích, kdy jsou hospitalizovány chráněné osoby nebo jiné rizikové skupiny.

Získaná zjištění naznačují, že oblast bezpečnosti zdravotnického personálu je často opomíjena, což může vést k vážným rizikům. Doporučuje se, aby zdravotnická zařízení přijala konkrétní opatření, která by zajistila fyzickou bezpečnost personálu v případech hospitalizace chráněných osob, a aby tato opatření byla součástí širší strategie ochrany všech zúčastněných.

Můžeme shrnout, že v oblasti fyzické bezpečnosti personálu při hospitalizaci chráněných osob existují zásadní nedostatky. Tato problematika by měla být prioritně řešena prostřednictvím

zavedení adekvátních bezpečnostních opatření a protokolů, které by zajistily ochranu nejen chráněných osob, ale také zdravotnického personálu, to vše ideálně z centrální úrovně.

Otázka 5: Jak hodnotíte přítomnost ochranky chráněné osoby? Pustil byste ji na operační sál nebo výkon kolonoskopie?

Tato otázka byla záměrně koncipována šířeji a při rozhovorech respondentům vysvětlena. Její podstatou bylo zjistit, zda je vnímání ochranky chráněné osoby stejné pro všechny typy vyšetření nebo výkonů. Odpovědi respondentů odhalují jasnou shodu mezi respondenty v otázce, že přítomnost ochranky v těchto konkrétních situacích není žádoucí. Všichni respondenti se shodují, že přítomnost ochranky na operačním sále by mohla narušit sterilní prostředí, což by mohlo vést k riziku infekce a snížení kvality zdravotní péče.

Navíc respondenti zmiňují, že přítomnost ochranky by mohla narušit vztah mezi lékařem a pacientem, což by mohlo negativně ovlivnit samotný výkon lékaře. Bylo také zmíněno, že ochranka může ohrozit bezpečnost pacientských dat, což je další důvod, proč by neměla být přítomna v takto citlivých situacích. Všichni respondenti by souhlasili s přítomností ochranky maximálně v předsálí, ale nikoli přímo na operačním sále nebo při intimních vyšetřeních, jako je kolonoskopie.

Z výzkumného hlediska tyto odpovědi zdůrazňují potřebu udržet přísné standardy sterilního prostředí a respektovat intimitu a soukromí pacientů během lékařských zákroků. Je evidentní, že přítomnost ochranky v těchto situacích je považována za nevhodnou a potenciálně škodlivou, a proto by měla být pečlivě zvážena, pokud vůbec povolena.

Respondenti se nezávisle na sobě shodli v tom, že přítomnost ochranky na operačním sále nebo při intimních lékařských zákrocích, jako je kolonoskopie, není považována za vhodnou a měla by být minimalizována nebo zcela vyloučena, aby byla zachována kvalita péče, bezpečnost pacientských dat a sterilní podmínky ve zdravotnickém zařízení. Zároveň ale přítomnost hodnotili spíše kladně, ovšem pouze při úkonech, které neovlivní vztah lékaře a pacienta. Velmi zajímavým byl názor jednoho z respondentů, který vyjádřil, že **není potřeba chráněnou osobu střežit před lékařem**.

Otázka 6: Jaké jsou nejčastější problémy spojené s fyzickou bezpečností při hospitalizaci chráněných osob?

Odpovědi respondentů na tuto otázku odhalují, že tato oblast není dostatečně řešena a je podceňována. Většina respondentů, ačkoliv se až na jednoho z nich nejednalo o primárně odborníky na fyzickou bezpečnost, nedokáže posoudit tuto problematiku vzhledem ke své odbornosti, což samo o sobě naznačuje, že otázka fyzické bezpečnosti zdravotnického personálu při hospitalizaci chráněných osob není běžně diskutována ani zohledňována v rámci jejich práce.

Tento nedostatek vědomostí a zájmu o problematiku fyzické bezpečnosti může mít za následek podcenění rizik, kterým může být personál vystaven, a absence adekvátních bezpečnostních opatření. Ačkoli je přítomnost ochranky považována za dostatečné opatření pro ochranu chráněné osoby, neexistuje odpovídající ochrana pro zdravotnický personál, což může vést k potenciálně nebezpečným situacím.

Z výzkumného hlediska je zřejmé, že je třeba většího zaměření na zajištění fyzické bezpečnosti nejen chráněných osob, ale také zdravotnického personálu, který je může ošetřovat. Tento problém by měl být řešen na institucionální úrovni prostřednictvím zavedení jasných protokolů a školení, které by připravily personál na možné bezpečnostní incidenty a minimalizovaly rizika spojená s hospitalizací vysoce rizikových skupin.

Můžeme shrnout, že problematika fyzické bezpečnosti při hospitalizaci chráněných osob je nedostatečně řešena a vyžaduje zvýšenou pozornost. Je třeba zavést odpovídající bezpečnostní opatření, která zajistí nejen ochranu chráněných osob, ale i personálu, a tím předejdou potenciálním rizikům a nebezpečným situacím.

3.5.3 Virtuální a kybernetická bezpečnost chráněných osob

Otázka 1: Jaká jsou nejčastější slabá místa a specifická rizika v oblasti bezpečnosti pacientských dat chráněných osob při jejich fyzické anebo virtuální hospitalizaci?

Odpovědi respondentů na první otázku ve třetí sekci ukazují na několik klíčových oblastí, které jsou považovány za problematické. Respondenti se shodují, že **nejslabším článkem v ochraně těchto dat je jednoznačně lidský faktor, který představuje významné riziko jak pro fyzickou, tak virtuální bezpečnost**.

Jedním z hlavních problémů je podle respondentů nedostatečné školení a povědomí personálu o významu ochrany dat. Chybí pravidelná a efektivní školení, která by personál vzdělávala v oblasti kybernetické bezpečnosti a správného zacházení s citlivými informacemi. Toto selhání vede k tomu, že se personál může stát snadným cílem pro útoky, jako je phishing nebo sociální inženýrství, což může vést k úniku dat.

Dalším rizikem je technologická zastaralost systémů, které nejsou schopny čelit moderním kybernetickým hrozbám. Někteří respondenti zmiňují, že stávající systémy nejsou dostatečně robustní a nedokážou efektivně detekovat a odrážet pokusy o neoprávněný přístup nebo kybernetické útoky.

Kombinace lidského faktoru a technologické zastaralosti činí z ochrany dat chráněných osob značně zranitelnou oblast. Tato zranitelnost je umocněna tím, že **data chráněných osob jsou často považována za vysoce citlivá a mohou být cílem útoků, které mají za cíl získat důležité informace o těchto osobách**.

Z výzkumného hlediska tyto odpovědi ukazují na potřebu komplexního přístupu k ochraně dat, který zahrnuje jak technologická řešení, tak důsledné vzdělávání a školení personálu. Je nezbytné, aby zdravotnická zařízení nejen modernizovala své technologické systémy, ale také zavedla pravidelné a povinné školení pro všechny zaměstnance, kteří přicházejí do styku s citlivými daty.

Jako dílčí shrnutí lze tvrdit, že slabá místa v oblasti bezpečnosti pacientských dat chráněných osob jsou způsobena především selháním lidského faktoru a nedostatečnou technologickou vybaveností. Tato rizika je třeba řešit prostřednictvím kombinace pokročilých technologických řešení a zlepšeného školení personálu, aby byla zajištěna co nejvyšší úroveň ochrany citlivých dat.

Otázka 2: Jaká jsou specifická rizika virtuální bezpečnosti pacientů se statutem chráněné osoby ve srovnání s běžnými pacienty?

Odpovědi respondentů ukazují na jednoznačný názor, že u chráněných osob existuje mnohem vyšší míra rizika spojená s únikem dat. Respondenti shodně uvádějí, že v případě úniku informací o zdravotním stavu chráněné osoby může mít tento únik dalekosáhlé politické a bezpečnostní důsledky, zatímco u běžného pacienta je dopad omezený převážně na jeho osobní život.

Několik respondentů zdůrazňuje, že zdravotní data chráněných osob musí být chráněna mnohem přísněji než u běžných pacientů. Uniknutí těchto dat by mohlo vést k destabilizaci politických struktur, ohrožení národní bezpečnosti nebo k ohrožení samotné chráněné osoby. Například informace o zdravotním stavu vrcholného politika nebo vojenského velitele by mohly být zneužity nepřátelskými subjekty nebo konkurenčními státy.

Z výzkumného hlediska tyto odpovědi naznačují, že je nutné přistupovat k ochraně dat chráněných osob s mimořádnou opatrností a že standardní bezpečnostní opatření, která jsou běžně aplikována na data běžných pacientů, rozhodně nejsou dostatečná. Je zřejmé, že zdravotnická zařízení musí zavést dodatečná opatření, která zajistí, že data chráněných osob budou chráněna před neoprávněným přístupem a zneužitím.

Specifická rizika virtuální bezpečnosti pacientů se statutem chráněné osoby jsou tedy mnohonásobně vyšší než u běžných pacientů, což vyžaduje zavedení přísnějších bezpečnostních opatření a neustálé zlepšování technologií a procedur pro ochranu těchto citlivých dat.

Otázka 3: Jaká technická a organizační opatření (pravidla) jsou aktuálně implementována pro ochranu citlivých dat pacientů se statutem chráněné osoby ve vybraných zdravotnických zařízeních (ambulantně i při hospitalizaci)?

Odpovědi respondentů odhalují různé přístupy a názory na to, jak by měla být data těchto osob chráněna. Většina respondentů se shoduje na tom, že je třeba zavést přísná a specifická opatření, která by zajišťovala bezpečnost těchto dat nad rámec standardních procedur.

Někteří respondenti zmiňují použití fiktivních rodných čísel nebo jmen, aby se snížila možnost identifikace chráněné osoby v případě úniku dat. Dále je doporučováno uchovávat citlivá data v papírové formě mimo elektronické systémy, což je považováno za bezpečnější způsob ochrany. Tento přístup je v některých případech inspirován praxí v jiných zemích, kde se při hospitalizaci vysoce postavených osob počítače zcela vypínají a přechází se na papírovou dokumentaci.

Další respondent navrhuje použití šifrování a uložení dat na zabezpečených serverech, což by mělo být doplněno pravidelnými aktualizacemi bezpečnostních protokolů a školením personálu. Jiný respondent zdůrazňuje potřebu využití skrytých identifikátorů a značek, které by umožnily sledovat, kdo a kdy k datům přistupoval, což by mělo ztížit neoprávněný přístup.

Získané odpovědi ukazují na nutnost komplexního přístupu k ochraně dat chráněných osob, který zahrnuje jak technologická opatření, tak organizační postupy. Je důležité, aby zdravotnická zařízení kombinovala různé metody ochrany, aby byla zajištěna maximální bezpečnost citlivých informací. Rovněž je nesmírně důležitá diversifikace bezpečnostních opatření obecně. Celkově lze konstatovat, že technická a organizační opatření pro ochranu dat chráněných osob vyžadují zavedení pokročilých metod, které kombinují šifrování, omezení přístupu a fyzickou ochranu dat, to vše založeno na diversifikaci. Tato opatření by měla být pravidelně aktualizována a personál by měl být školen, aby zajistil, že bezpečnost dat bude na nejvyšší možné úrovni.

Otázka 4: Jaká opatření jsou přijímána pro zajištění ochrany dat chráněných osob před neoprávněným přístupem ze strany zaměstnanců?

Odpovědi respondentů přináší různé úrovně implementace bezpečnostních opatření v různých zdravotnických zařízeních.

Většina respondentů zdůrazňuje význam neustálého monitoringu přístupů k citlivým datům, včetně snímání logů a používání dynamických monitorovacích systémů, které mohou rychle reagovat na podezřelou aktivitu. Někteří respondenti zmiňují potřebu vytvoření speciálních, flexibilních softwarových center, která by mohla okamžitě zasáhnout v případě podezření na neoprávněný přístup. Dalším klíčovým prvkem je omezení přístupových práv pouze na zaměstnance, kteří mají nezbytnou autorizaci, přičemž je důležité pravidelně kontrolovat a aktualizovat, kdo má přístup k těmto citlivým informacím, včetně dublované kontroly ze strany supervizorů nebo nadřízených zaměstnanců.

Několik respondentů také zmínilo potřebu zvýšené kontroly a vynucování těchto bezpečnostních opatření, včetně přísných nařízení, která by měla být důsledně dodržována. Nicméně, někteří z respondentů uvedli, že v praxi tato opatření často nejsou dostatečně implementována nebo vynucována, což představuje významné riziko pro bezpečnost dat.

Odpovědi poukazují na **potřebu zvýšeného zaměření na zabezpečení dat ze strany zaměstnanců**. I když jsou zavedeny technologické nástroje a bezpečnostní protokoly, je nezbytné zajistit, aby byly v praxi skutečně uplatňovány a pravidelně kontrolovány. Lze konstatovat, že ochrana dat chráněných osob před neoprávněným přístupem ze strany zaměstnanců vyžaduje nejen technologická opatření, ale také pravidelnou kontrolu, aktualizaci

a důsledné vynucování bezpečnostních nařízení, aby byla zajištěna maximální úroveň ochrany těchto citlivých informací.

Otázka 5: Jaká opatření jsou přijímána pro zajištění ochrany dat chráněných osob před neoprávněným přístupem zvenku?

Odpovědi respondentů poukazují na různé přístupy a úrovně zabezpečení v jednotlivých zdravotnických zařízeních.

Někteří respondenti zdůrazňují používání standardních technologií, jako jsou firewally, antivirové programy a šifrování dat, které jsou považovány za základní nástroje pro ochranu před neoprávněným přístupem zvenku. Další klíčová opatření zahrnují pravidelnou aktualizaci těchto systémů a testování jejich zranitelností, což pomáhá odhalit a odstranit případné slabiny.

Jedním z respondentů bylo také zmíněno, že v ideálním případě by měla být pro ochranu dat chráněných osob vytvořena oddělená, utajená síť, která by byla používána pouze pro tyto účely. Tato síť by měla být izolována od běžných komunikačních kanálů, což by významně snížilo riziko neoprávněného přístupu zvenku. Nicméně, bylo také přiznáno, že zavedení takových opatření je často náročné a může být omezeno finančními a technickými možnostmi zařízení.

Někteří respondenti upozorňují na to, že i když jsou tyto technologie zavedeny, klíčovým faktorem pro jejich efektivitu je lidský dohled a rychlá reakce na případné bezpečnostní incidenty. **Bezpečnostní opatření mohou být sebelepší, ale pokud nejsou správně monitorována a spravována, ztrácejí na své účinnosti**.

V celkovém souhrnu odpovědi naznačují, že ochrana dat chráněných osob před neoprávněným přístupem zvenku je dobře rozvinutá v teoretické rovině, ale její praktická implementace často naráží na omezení. Lze potvrdit, že efektivní ochrana dat před neoprávněným přístupem zvenku vyžaduje nejen implementaci technických opatření, ale také stálý dohled, pravidelnou aktualizaci a testování těchto opatření, aby byla zajištěna jejich maximální účinnost v reálném prostředí.

Otázka 6: Jakým způsobem jsou zaměstnanci školeni ohledně kybernetické bezpečnosti chráněných osob?

Odpovědi respondentů poukazují na výrazné nedostatky v této oblasti. Většina respondentů se shoduje, že školení zaměstnanců ohledně specifické ochrany dat chráněných osob buď vůbec neprobíhá, nebo je na velmi nízké úrovni. Někteří respondenti přímo uvádějí, že zaměstnanci

nejsou školeni v rozpoznávání rizik spojených s ochranou dat chráněných osob a nevnímají tato rizika jako důležitá. Tento nedostatek povědomí a školení představuje značné riziko pro bezpečnost dat, protože zaměstnanci, kteří nejsou dostatečně informováni, mohou nevědomky ohrozit ochranu citlivých informací.

Respondenti rovněž naznačují, že i tam, kde se školení provádí, se zaměřuje spíše na obecné aspekty kybernetické bezpečnosti než na specifika týkající se chráněných osob. To vede k situacím, kdy jsou zaměstnanci připraveni řešit běžné kybernetické hrozby, ale nejsou vybaveni znalostmi potřebnými k ochraně dat chráněných osob, které mohou čelit specifickým a sofistikovanějším útokům.

Odpovědi zdůrazňují potřebu zlepšení a specializace školení v oblasti kybernetické bezpečnosti. Je nezbytné, aby zdravotnická zařízení nejen pravidelně školila své zaměstnance v oblasti ochrany dat, ale aby také zohledňovala specifické potřeby ochrany dat chráněných osob. Školení by měla být více zaměřena na identifikaci a zvládání rizik spojených s ochranou citlivých informací těchto vysoce ohrožených skupin. Lze konstatovat, že **současná úroveň školení zaměstnanců v oblasti kybernetické bezpečnosti chráněných osob je nedostatečná a vyžaduje výrazné zlepšení**. Zaměstnanci musí být lépe informováni o rizicích a specifických potřebách ochrany dat chráněných osob, aby byla zajištěna maximální úroveň bezpečnosti těchto citlivých informací.

Otázka 7: Jaké jsou nejčastější problémy, se kterými se setkáváte v oblasti kybernetické bezpečnosti chráněných osob?

Odpovědi respondentů odhalují několik zásadních problémů, které trápí zdravotnická zařízení. Většina respondentů se shoduje, že ideálním stavem by bylo, aby ochrana dat chráněných osob byla zajištěna standardizovaným způsobem, který by vycházel z platné legislativy a regulací. Bohužel, jak respondenti uvádějí, realita je často jiná. Současná bezpečnostní opatření jsou podle nich nedostatečná, což je způsobeno především nedostatkem stanovených standardů a směrnic, které by se specificky zaměřovaly na ochranu dat „VIP osob“.

Někteří respondenti také zdůrazňují, že v mnoha případech nejsou tato data chráněna samostatnou sítí, což zvyšuje riziko jejich kompromitace. Bylo navrženo, aby státní instituce stanovily přísné standardy pro ochranu těchto dat a aby byla vytvořena samostatná síť, která by byla zcela izolována od běžné infrastruktury a zabezpečená proti jakémukoli vnějšímu i vnitřnímu útoku.

Další významný problém, který byl zmiňován, spočívá v nedostatečné analýze rizik. Respondenti se domnívají, že stávající systémy často neberou v úvahu specifická rizika spojená s kybernetickou bezpečností chráněných osob. **Tato data by měla být chráněna jiným způsobem než běžná data**, což vyžaduje podrobnou analýzu rizik a následné přizpůsobení ochranných opatření specifickým hrozbám, kterým tato data mohou čelit.

Získané odpovědi ukazují na zásadní potřebu zlepšení v oblasti kybernetické bezpečnosti. Je nezbytné, aby zdravotnická zařízení nejen zvýšila úroveň ochrany dat, ale také aby byly stanoveny jasné standardy a postupy pro ochranu dat chráněných osob. Lze tvrdit, že hlavní problémy v oblasti kybernetické bezpečnosti chráněných osob jsou způsobeny **nedostatečnou standardizací, neexistencí samostatných sítí a slabou analýzou rizik**. Tato rizika je třeba řešit prostřednictvím zavedení jasných regulací, standardů a specifických technologií, které zajistí bezpečnost citlivých dat chráněných osob na nejvyšší možné úrovni.

Otázka 8: Řešíte ochranu dat chráněných osob nebo skupin osob (vojáků/policistů/příslušníků zpravodajských služeb atd.) ve velkých souborech dat (tzv. „big data“), která jsou předávána například za účelem výzkumu?

Odpovědi respondentů ukazují na různé úrovně povědomí a praxe v této oblasti. Někteří respondenti uvádějí, že ochrana těchto dat je zajištěna především legislativně, kdy zákon poskytuje chráněným osobám vyšší úroveň ochrany. Při práci s velkými soubory dat, které obsahují informace o vojácích, policistech nebo příslušnících zpravodajských služeb, by měl stát zajistit jejich maximální bezpečnost a správně je anonymizovat, aby nebylo možné tyto osoby zpětně identifikovat.

Jiní respondenti ovšem vyjadřují obavy, že ve skutečnosti není ochrana těchto dat vždy dostatečná. Například pokud jsou data předávána pro vědecký výzkum, anonymizace nemusí být vždy dostatečně silná, což představuje riziko, že citlivé informace mohou být zneužity. Dále někteří respondenti poukazují na to, že většina výzkumníků se při práci s daty soustředí především na obsah těchto dat a nezohledňuje vždy jejich bezpečnostní aspekty, což může být potenciálně nebezpečné.

Zajímavým aspektem, který někteří respondenti zmínili, je možnost kombinace různých zdrojů dat, například zdravotních údajů s údaji od mobilních operátorů, což může umožnit neautorizovaným osobám sledovat pohyb chráněných osob nebo zjistit jejich identitu.

Nashromážděné informace naznačují, že ochrana dat chráněných osob ve velkých souborech dat představuje složitý a často podceňovaný problém. I když jsou legislativní základy nastaveny, v praxi mohou existovat mezery, které mohou vést k úniku citlivých informací.

Dle názoru autora lze konstatovat, že i přes právní ochranu je nutné klást větší důraz na praktické aspekty ochrany dat v kontextu zpracování velkých souborů pacientských dat. To zahrnuje důslednou anonymizaci, posouzení rizik při kombinování dat z různých zdrojů a zajištění, aby státní a výzkumné instituce měly k dispozici dostatečné nástroje a znalosti pro ochranu citlivých informací chráněných osob.

Otázka 9: Řešíte nějak vyšší míru bezpečnosti dat chráněných osob v případě jejich předávání do jiných zdravotních zařízení (například laboratoří, jiných poskytovatelů zdravotních služeb atd.)?

Odpovědi respondentů jasně poukazují na závažné nedostatky v této oblasti.

Většina respondentů se shoduje, že přenos dat mezi různými zdravotnickými zařízeními není dostatečně zabezpečen, což zvyšuje riziko úniku citlivých informací. Různí respondenti upozorňují na skutečnost, že bezpečnostní opatření nejsou dostatečně dodržována a často zcela chybí, což vede k vysoké míře zranitelnosti těchto dat. Někteří z nich dokonce zmiňují konkrétní příklady, kdy došlo k úniku informací z lékařských zpráv pacientů, což jen potvrzuje závažnost tohoto problému.

Dále někteří respondenti vyjadřují obavy z toho, že **neexistují jednotné standardy pro zabezpečení přenosu těchto dat**, což vede k rozdílnému přístupu mezi jednotlivými zařízeními. Tento nesourodý přístup může mít za následek neadekvátní ochranu citlivých informací a zvýšené riziko jejich zneužití.

Z výzkumného hlediska je zřejmé, že současná praxe v oblasti přenosu dat mezi zdravotnickými zařízeními vykazuje značné mezery. Je nezbytné, aby státní orgány nebo jiná relevantní instituce vytvořily a implementovaly jasné a závazné standardy, které by zajistily jednotnou a vysokou úroveň ochrany těchto dat napříč všemi zdravotnickými zařízeními. Lze vyzdvihnout, že oblast přenosu dat chráněných osob mezi různými zdravotnickými zařízeními představuje významné riziko a vyžaduje urgentní pozornost. Aby byla zajištěna bezpečnost těchto citlivých informací, je nutné zavést přísnější a standardizované bezpečnostní protokoly ze strany státu, které budou striktně dodržovány v praxi.

Otázka 10: Jak by měl vypadat přenos dat chráněných osob, vojáků, z bojiště kdekoliv na světě do zdravotnického zařízení v ČR?

Odpovědi respondentů na desátou otázku ve třetí sekci, která se zaměřuje na přenos dat chráněných osob, zejména vojáků, z bojiště kdekoliv na světě do zdravotnického zařízení v ČR (EU), odhalují různé pohledy a návrhy na zabezpečení takového přenosu.

Většina respondentů se shoduje, že přenos těchto dat musí být rychlý a zároveň maximálně bezpečný. Někteří navrhují využití tzv. mikrodatových přenosů, což znamená odesílání malých, zašifrovaných bloků dat v krátkých záblescích, které jsou obtížně zachytitelné nepřítelem. Tento přístup by mohl zahrnovat použití speciálních šifrovaných vysílaček, které minimalizují možnost detekce a lokalizace přenosu. Respondenti také zdůrazňují, že jakmile se data přenáší vzduchem, jsou potenciálně zranitelná, a proto by se měl klást důraz na technologie, které snižují riziko odhalení.

Další respondenti upozorňují na důležitost volby mezi online a offline přenosem. Někteří se přiklánějí k tomu, aby se data přenášela offline, což by výrazně snížilo riziko zachycení a útoku na přenos. Jiní navrhují, že by bylo vhodné použít hybridní přístup, kde by se data rozkouskovala a přenesla různými směry, aby se minimalizovalo riziko ztráty nebo kompromitace dat.

Z popsaného hlediska tyto odpovědi naznačují, že **přenos dat z bojiště do zdravotnického zařízení vyžaduje velmi specifický přístup, který kombinuje rychlost s vysokou úrovní zabezpečení**. Je zřejmé, že standardní metody přenosu nejsou v tomto případě dostatečné a že by měla být vyvinuta specializovaná řešení, která by byla schopna zvládnout nároky takto citlivých operací.

Pro bezpečný a efektivní přenos dat chráněných osob z bojiště je tedy klíčové kombinovat různé technologie a přístupy. Zajištění bezpečnosti těchto dat bude záviset na použití pokročilých šifrovacích technologií, minimalizaci rizika detekce a volbě mezi online a offline přenosovými metodami v závislosti na konkrétní situaci a prostředí, ve kterém se přenos uskutečňuje.

Otázka 11: Jak vnímáte tzv. cloudová úložiště a jejich využití pro uchování zdravotních dat? Využíval byste je pro přenos a ukládání zdravotních dat vojáků (chráněných osob)?

Odpovědi respondentů reflektují rozdílné názory na toto téma. Někteří respondenti vyjadřují obavy z využívání cloudových úložišť pro uchovávání citlivých vojenských dat. Poukazují na

to, že použití běžných komerčních cloudových služeb může být rizikové, zejména v případě výpadků nebo kybernetických útoků, které by mohly ohrozit dostupnost a bezpečnost těchto dat. Například jeden z respondentů upozorňuje na nebezpečí výpadků cloudových služeb a uvádí příklad z Černé Hory, kde výpadek elektřiny způsobil přerušení přístupu k datům a narušil funkčnost klíčových služeb.

Jiní respondenti se přiklání k tomu, že pokud by cloudová úložiště měla být využívána, pak jedině v případě, že budou pod přísnou kontrolou a správou armády nebo státními institucemi. Armádní cloud by podle nich měl být spravován výhradně armádou a měl by být navržen tak, aby byl odolný vůči vnějším útokům a zajišťoval maximální bezpečnost citlivých informací.

Získané odpovědi naznačují, že i když cloudová úložiště mohou nabídnout rychlý a efektivní přístup k datům, jejich použití v kontextu vojenských nebo chráněných osob musí být velmi pečlivě zváženo. Je nezbytné provést podrobnou analýzu rizik a zajistit, aby cloudová řešení byla schopna poskytnout úroveň zabezpečení odpovídající citlivosti dat, která mají uchovávat.

Celkově lze konstatovat, že použití cloudových úložišť pro uchovávání zdravotních dat chráněných osob je kontroverzní téma. Zatímco někteří vidí výhody v rychlém přístupu k datům, většina respondentů se shoduje na tom, že pokud mají být cloudová úložiště využívána, musí být spravována s nejvyššími standardy bezpečnosti a kontrolována výhradně státními institucemi nebo armádou.

Otázka 12: Jaká doporučení byste dali pro zlepšení kybernetické bezpečnosti při hospitalizaci chráněných osob?

Odpovědi respondentů odkazují na řadu důležitých aspektů, které je třeba zvážit. Většina respondentů se shoduje na tom, že budoucnost ochrany dat ve zdravotnictví spočívá v zavádění nových technologií a standardů, které zajistí vyšší úroveň bezpečnosti. Například někteří z nich zdůrazňují potřebu pravidelné aktualizace bezpečnostních protokolů a školení personálu, což by mělo přispět k lepšímu povědomí o ochraně dat a zvýšit úroveň zabezpečení v praxi.

Další respondenti navrhují zavedení specifických standardů, jako je například Health Level Seven (dále jen „HL7“) pro výměnu zdravotních dat, které by měly být zavedeny rychle a efektivně. HL7 označuje soubor mezinárodních standardů pro přenos klinických a administrativních dat mezi softwarovými aplikacemi různých poskytovatelů zdravotní péče. Tato standardizace by podle nich mohla výrazně přispět k ochraně citlivých informací a zajištění jejich bezpečného přenosu mezi různými systémy a zařízeními.

Závěry respondentů naznačují, že existuje široký konsenzus o potřebě modernizace a zlepšení současných bezpečnostních opatření ve zdravotnictví, zejména při hospitalizaci chráněných osob. Respondenti navrhují kombinaci technických inovací, standardizace postupů a důsledného školení personálu, což by mělo vytvořit robustní systém ochrany dat. Můžeme tvrdit, že pro zajištění vyšší úrovně kybernetické bezpečnosti při hospitalizaci chráněných osob je nezbytné přijmout integrovaný přístup, který zahrnuje jak technologická řešení, tak i lidský faktor. Pravidelná aktualizace protokolů, standardizace výměny dat a důkladné školení personálu jsou klíčovými prvky, které mohou přispět k dosažení této cíle.

Otázka 13: Máte nějaké zkušenosti ze zahraničí v diskutované oblasti?

Odpovědi respondentů ukazují různé úrovně zkušeností a uvědomění. Někteří respondenti mají přímé zkušenosti ze zahraničí, například od vojenských poskytovatelů zdravotnických služeb nebo zdravotnických zařízení na vojenských základnách, kde byla zavedena přísná bezpečnostní opatření. Tito respondenti upozorňují na to, že v zahraničí, zejména v rámci NATO, jsou nastaveny vysoké standardy pro přenos dat a zabezpečení, které zajišťují ochranu citlivých informací napříč různými systémy a institucemi. Zdůrazňují, že standardizace a interoperabilita mezi systémy jsou klíčovými prvky, které přispívají k bezpečnosti dat ve vyspělých zemích. Jiní respondenti však přiznávají, že nemají přímé zkušenosti se zahraničními praktikami nebo inovacemi v oblasti kybernetické bezpečnosti, což může omezovat jejich schopnost porovnávat a implementovat osvědčené postupy z jiných zemí.

Z výzkumného hlediska tyto odpovědi naznačují, že i když někteří odborníci mají hodnotné zkušenosti ze zahraničí, je zde stále prostor pro rozšíření znalostí a dovedností v oblasti kybernetické bezpečnosti ve zdravotnictví. Význam těchto zkušeností je zřejmý, protože umožňují lépe porozumět mezinárodním standardům a přizpůsobit domácí praktiky tak, aby dosahovaly stejné úrovně ochrany.

Jistě lze tvrdit, že sdílení zkušeností a osvědčených postupů ze zahraničí by mohlo výrazně přispět ke zlepšení kybernetické bezpečnosti při hospitalizaci chráněných osob. Respondenti, kteří mají zkušenosti s prací v zahraničních zdravotnických zařízeních, poukazují na nutnost standardizace a interoperabilitu systémů, což jsou klíčové faktory pro dosažení vysoké úrovně ochrany dat.

Dle názoru autora byly zahraniční zkušenosti nesmírným přínosem nejen pro něj samotného, ale i pro další rozvoj a zkvalitnění činností samotných respondentů.

Otázka 14: Měla by, dle Vašeho názoru, mít veřejnost právo bez souhlasu ústavního činitele (chráněné osoby) znát informace o jeho zdravotním stavu?

Odpovědi respondentů na poslední otázku ukazují na opatrný přístup k tomuto citlivému tématu.

Většina respondentů se shoduje na tom, že **veřejnost by měla mít omezený přístup k informacím o zdravotním stavu ústavních činitelů**. Připouštějí, že některé **informace, které by mohly ovlivnit schopnost ústavního činitele vykonávat jeho funkci, by měly být sděleny, avšak pouze v rozsahu, který je nezbytný**. Detailní zdravotní informace by měly být přístupné pouze vybraným státním úředníkům nebo zákonodárcům, kteří mají pravomoc rozhodnout o dalším postupu, například o přechodném předání funkcí. Respondenti zdůrazňují, že ochrana soukromí ústavních činitelů je důležitá, a proto by veřejnost neměla mít přístup k citlivým údajům, které by mohly narušit jejich soukromí nebo bezpečnost.

Jejich odpovědi naznačují, že otázka veřejného práva na informace o zdravotním stavu ústavních činitelů je komplexní a vyžaduje pečlivé zvažování mezi právem na soukromí a veřejným zájmem. Respondenti navrhují, že veřejnost by měla být informována pouze v nezbytném rozsahu, aby byl zachován její legitimní zájem na tom, zda ústavní činitel může vykonávat své povinnosti, zatímco detailní a citlivé informace by měly zůstat chráněné. Dle názoru autora práce **to zcela koresponduje s požadavkem provedení balanční analýzy v souladu s GDPR**.

Existuje tedy potřeba vyváženého přístupu při sdělování informací o zdravotním stavu ústavních činitelů. Přístup k těmto informacím by měl být pečlivě regulován a omezen na to, co je nezbytné pro zajištění transparentnosti a odpovědnosti veřejných činitelů, aniž by bylo ohroženo jejich právo na soukromí a bezpečnost.

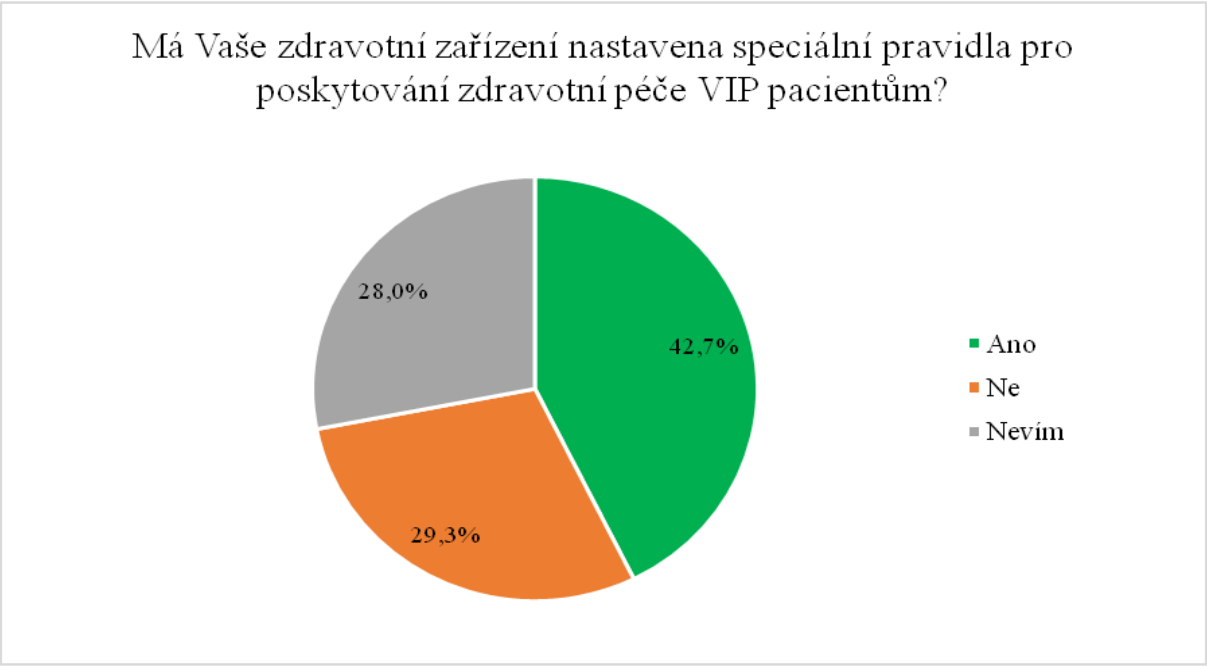
3.6 Interpretace kvantitativní analýzy

3.6.1 Dotazník pro pracovníky ve zdravotnictví

U většiny otázek (mimo těch dobrovolných), jsou vždy pro porovnání uvedeny jak výstupy od českých respondentů, tak těch zahraničních.

- **Sekce 1: Péče o Chráněné osoby**

Graf 1.1: Existence speciálních pravidel pro poskytování zdravotní péče chráněným osobám; Zdroj: autor (2024)



Z výsledků zobrazených v tabulce vyplývá, že většina respondentů potvrzuje, že jejich zdravotní zařízení má nastavena speciální pravidla pro poskytování zdravotní péče chráněným osobám. Tento relativně vysoký podíl naznačuje, že téměř polovina zdravotnických zařízení uznává potřebu zvláštních opatření při péči o chráněné osoby, což může být spojeno s vyššími nároky na bezpečnost, soukromí a rychlost poskytované péče. Na druhou stranu téměř třetina respondentů uvedla, že taková pravidla ve svých zařízeních nastavena nemají. Tento podíl ukazuje, že existuje značná část zařízení, která nepovažuje za nutné, nebo možná nemá kapacitu, zavést specifická opatření pro chráněné osoby.

Další téměř třetina respondentů odpověděla, že **nevědí, zda jsou v jejich zařízení taková pravidla nastavena**, což může naznačovat nedostatečnou komunikaci nebo transparentnost ohledně postupů v organizaci. Tento nedostatek informovanosti by mohl potenciálně vést

k nesouladu v praxi a k nesprávnému zacházení s chráněnými osobami, což by mohlo mít negativní dopad na jejich spokojenost a vnímanou kvalitu péče. Z hlediska výzkumu tato zjištění poukazují na variabilitu přístupů v rámci zdravotnických zařízení a zdůrazňují potřebu jasně definovaných a komunikovaných pravidel pro péči o chráněné osoby. Tato variabilita může být také důležitým bodem pro další výzkum, který by se zaměřil na identifikaci nejlepších postupů a jejich efektivity.

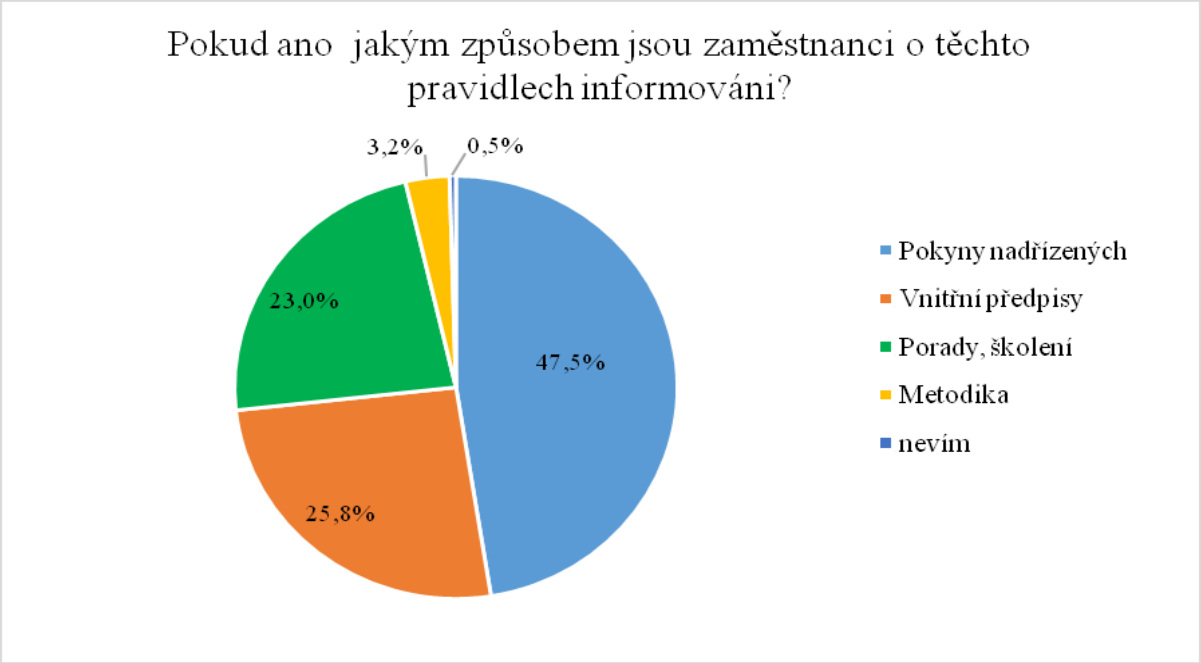
Graf 1.1a: Existence speciálních pravidel pro poskytování zdravotní péče chráněným osobám v zahraničí; Zdroj: autor (2024)

Výsledky této otázky ukazují značný rozdíl v přístupu k nastavení speciálních pravidel pro poskytování zdravotní péče chráněným osobám mezi českými a zahraničními zdravotnickými zařízeními. V zahraničních zařízeních, jak vyplývá z dat, drtivá většina respondentů potvrdila, že mají taková pravidla nastavena, což je výrazně vyšší podíl oproti 42,7 % v českých zařízeních. Tento rozdíl může poukazovat na odlišnosti v prioritách a přístupech k ochraně citlivých skupin pacientů, případně na různé legislativní nebo kulturní požadavky, které zahraniční zdravotnická zařízení motivují k přijetí striktnějších opatření.

Podíl respondentů, kteří uvedli, že jejich zařízení nemají žádná speciální pravidla, je v zahraničních zařízeních nižší (15,8 %) ve srovnání s českými (29,3 %). To naznačuje, že v zahraničí je obecně větší povědomí o nutnosti specifických opatření pro péči o chráněné osoby. Mnohem nižší je také podíl respondentů, kteří nevědí o existenci takových pravidel

(3,2 % oproti 28,0 % v českých zařízeních), což může ukazovat na lepší komunikaci a transparentnost postupů v zahraničních zdravotnických organizacích. Tato komparace naznačuje, že česká zdravotnická zařízení by mohla těžit z přijetí přísnějších a jasněji definovaných pravidel pro péči o chráněné osoby, inspirovaných zahraničními modely.

Graf 1.2: Způsob informování zaměstnanců o pravidlech poskytování zdravotní péče chráněným osobám; Zdroj: autor (2024)



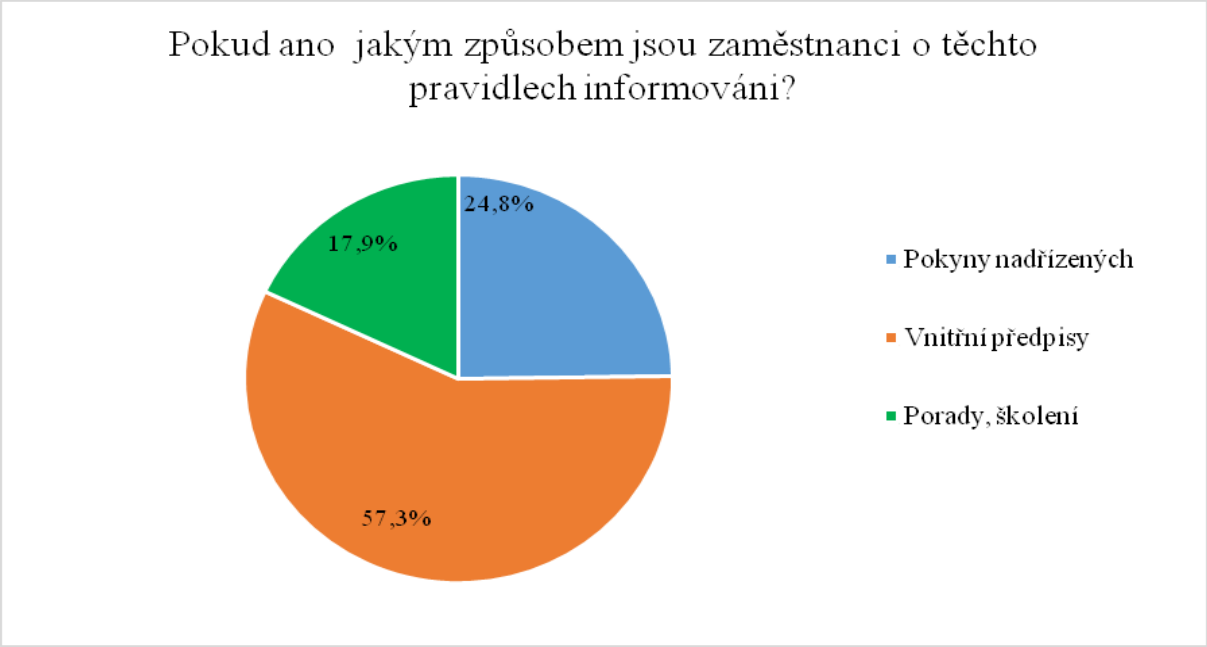
Výsledky týkající se způsobů, jakými jsou zaměstnanci informováni o pravidlech pro poskytování zdravotní péče chráněným osobám, odhalují zajímavé rozložení preferovaných metod komunikace. Nejčastějším způsobem jsou pokyny nadřízených, což bylo uvedeno ve většině případů. Tento vysoký podíl naznačuje, že přímá ústní komunikace a řízení ze strany vedení jsou v mnoha zdravotnických zařízeních klíčovým kanálem pro sdílení důležitých informací. Vnitřní předpisy jsou druhou nejčastěji používanou metodou, což ukazuje na snahu některých institucí formalizovat postupy a zajistit, aby byly dobře dokumentované a dostupné zaměstnancům.

Na třetím místě jsou porady a školení. Tento výsledek naznačuje, že i když je přímá komunikace častější, existuje také potřeba formálnějších a strukturovanějších vzdělávacích aktivit, které mohou zaměstnancům poskytnout hlubší pochopení pravidel a jejich důležitosti. Metodika a strukturovaný přístup jsou na posledním místě, což ukazuje na možnou mezeru v systematickém školení a implementaci postupů. Pouze 0,5 % respondentů uvedlo, že neví,

jak jsou o těchto pravidlech informováni, což naznačuje relativně vysokou úroveň povědomí mezi zaměstnanci.

Celkově tato data ukazují, že zatímco přímá a neformální komunikace je preferována, existuje prostor pro zlepšení formálních a systematických přístupů ke komunikaci pravidel o péči o chráněné osoby. To by mohlo zahrnovat více strukturovaných školení, jasně definované metodiky a pravidelnou revizi a aktualizaci vnitřních předpisů.

Graf 1.2a: Způsob informování zahraničních zaměstnanců o pravidlech poskytování zdravotní péče chráněným osobám; Zdroj: autor (2024)



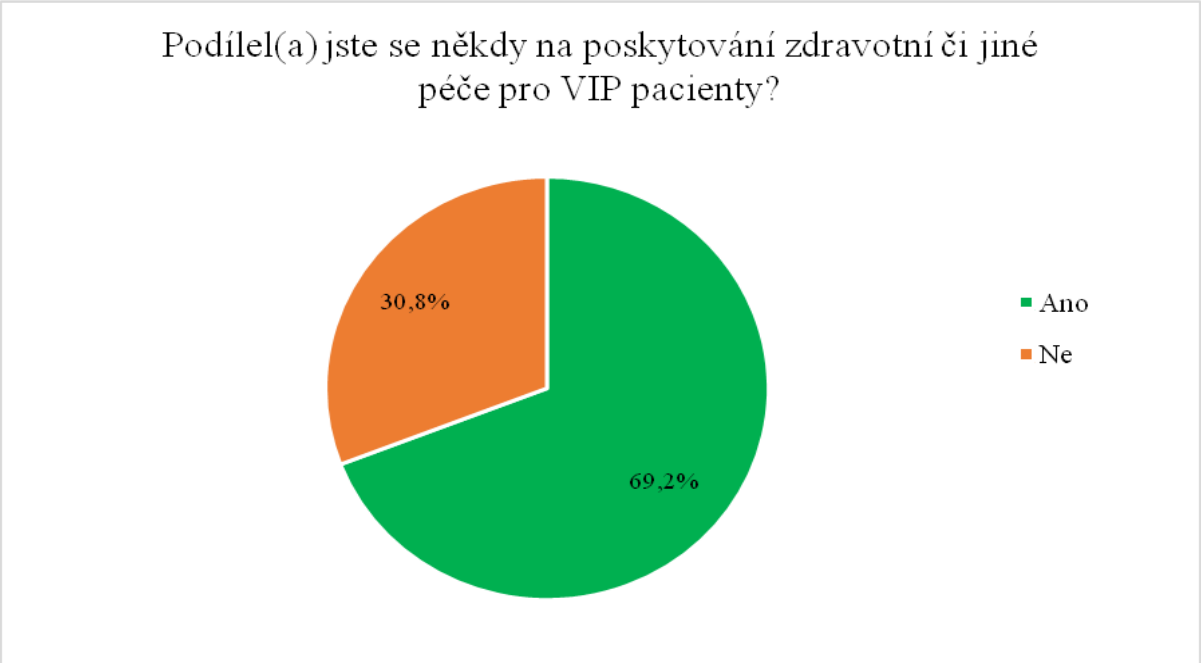
Zahraniční data ukazují, že nejčastěji používaným způsobem informování zaměstnanců o pravidlech pro poskytování zdravotní péče chráněným osobám jsou vnitřní předpisy. Tento výsledek je výrazně odlišný od českých dat, kde pokyny nadřízených byly nejčastější metodou informování (47,5 %). Rozdíl naznačuje, že zahraniční zdravotnická zařízení kladou větší důraz na formalizaci a dokumentaci postupů, což může být indikátorem rozdílného přístupu k řízení a transparentnosti v oblasti zdravotní péče.

Pokyny nadřízených, které jsou v zahraničních zařízeních uvedeny jako druhý nejčastější způsob informování, stále hrají významnou roli, ale nejsou tak dominující jako v České republice. Tento posun směrem k formalizovaným přístupům může naznačovat snahu o zajištění větší konzistence a jednotnosti v aplikaci pravidel. Porady a školení jsou třetí nejčastější metodou informování v zahraničních zařízeních, což je srovnatelné s českými daty,

ale stále ukazuje na nižší preference této metody ve srovnání s přímými pokyny a vnitřními předpisy.

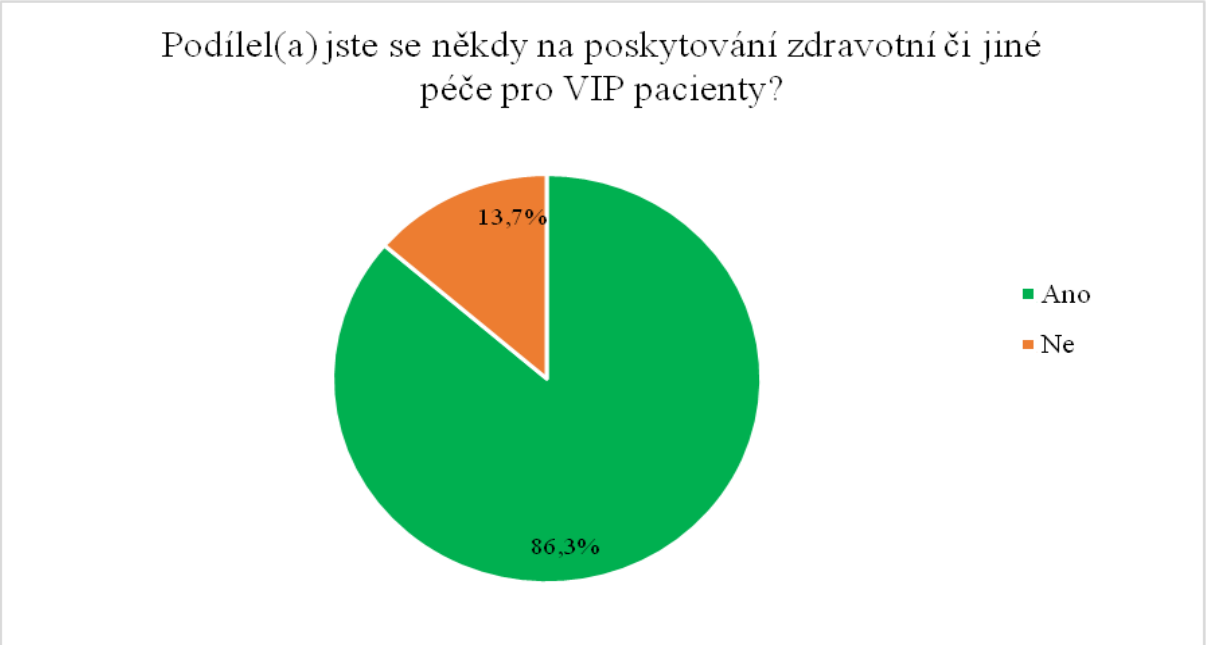
Celkově lze z těchto dat usuzovat, že zatímco zahraniční zdravotnická zařízení kladou větší důraz na formální a strukturované přístupy k informování zaměstnanců, česká zařízení preferují více přímou a osobní komunikaci.

Graf 1.3: Podíl participace na léčbě, péči nebo zabezpečení chráněných osob; Zdroj: autor (2024)



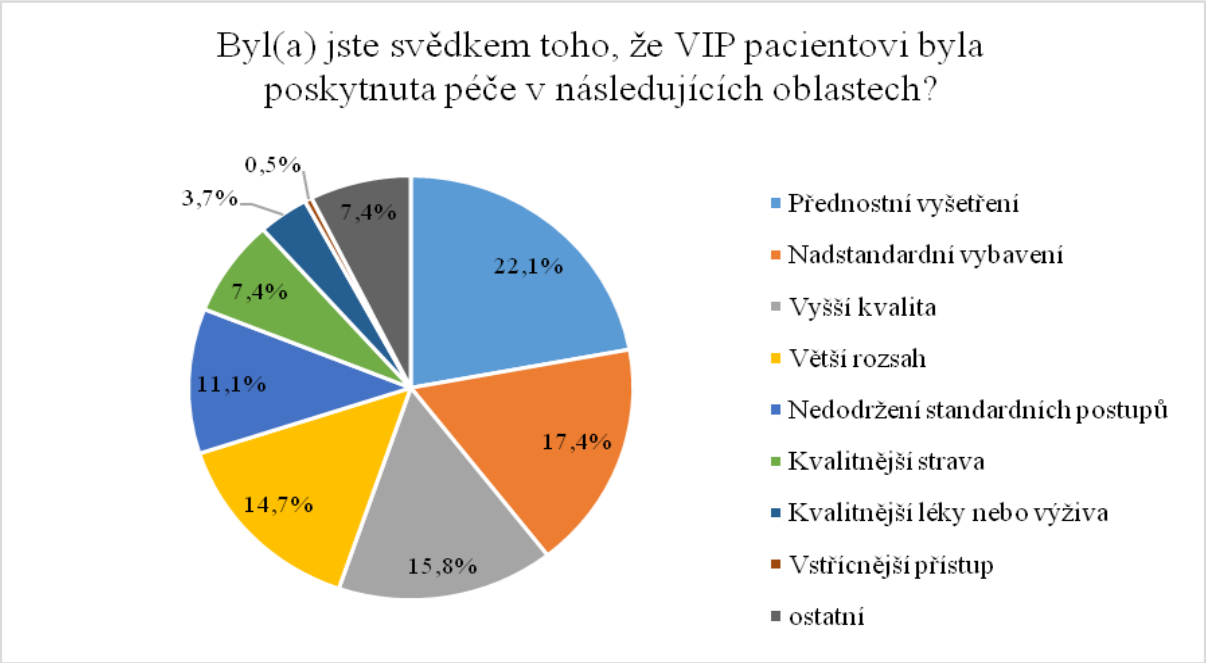
Výsledky této otázky ukazují, že většina respondentů se někdy podílela na poskytování zdravotní či jiné péče chráněným osobám. To naznačuje, že interakce s chráněnými osobami je v rámci zdravotnických zařízení relativně častým jevem a mnoho pracovníků má přímé zkušenosti s touto specifickou skupinou pacientů. Tento údaj může indikovat také míru potřebné připravenosti a školení, které zdravotnický personál musí mít, aby mohl efektivně reagovat na potřeby chráněných osob. Naopak téměř třetina respondentů uvedla, že se na poskytování péče chráněným osobám nikdy nepodílelo, což může naznačovat, že v některých zařízeních nebo odděleních nemusí být takové situace běžné nebo že jsou vyhrazeny specializovanému personálu. Tyto rozdíly v odpovědích mohou odrážet rozdílné protokoly a organizační struktury napříč různými zdravotnickými zařízeními.

Graf 1.3a: Podíl participace na léčbě, péči nebo zabezpečení chráněných osob - zahraničí; Zdroj: autor (2024)



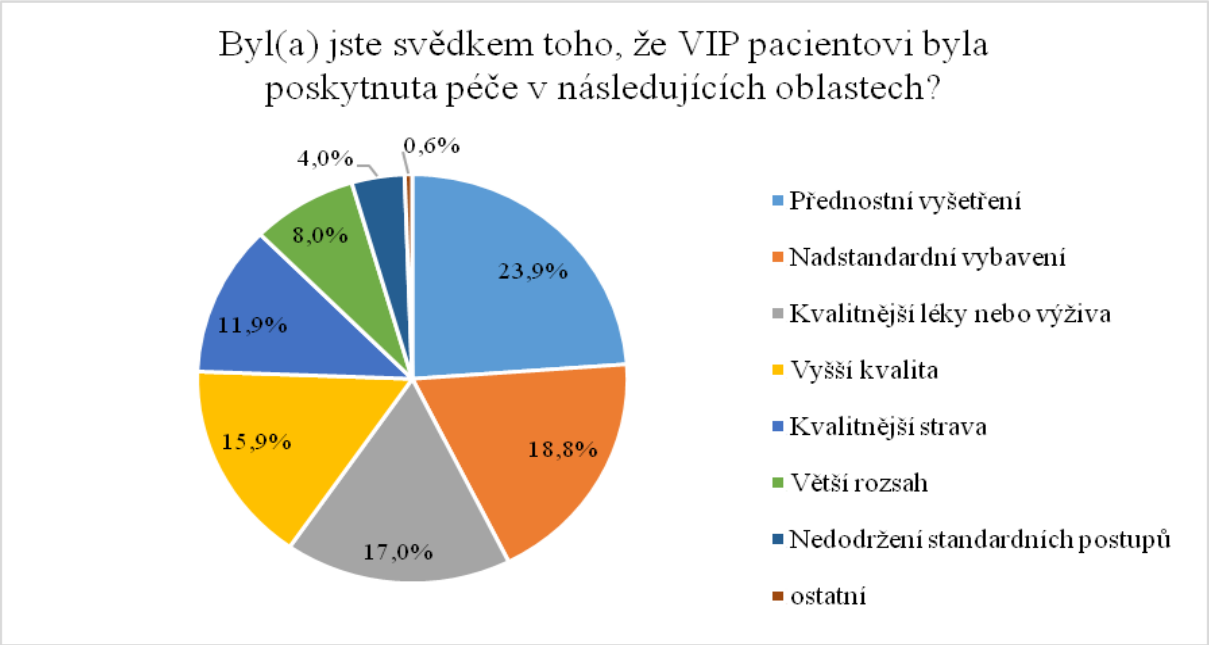
Výsledky této otázky odhalují, že podíl zahraničních respondentů, kteří se podíleli na poskytování péče chráněným osobám, je výrazně vyšší než v českém kontextu. Zatímco v zahraničních zařízeních většina respondentů uvedla, že měli zkušenost s péčí o chráněné osoby, v českých zařízeních to bylo pouze 69,2 %. Tento rozdíl naznačuje, že zahraniční zdravotnické instituce mohou častěji zahrnovat péči o chráněné osoby do běžné praxe, což může být způsobeno rozdílnými organizačními strukturami, politikami nebo kulturními přístupy k péči o tyto pacienty. Nižší procento respondentů bez zkušeností s chráněnými osobami v zahraničí (13,7 % oproti 30,8 % v ČR) může naznačovat vyšší míru integrace „VIP péče“ do standardních pracovních postupů zahraničních zdravotnických zařízení.

Graf 1.4: Zkušenosti zdravotníků s poskytováním nestandardní zdravotní péče; Zdroj: autor (2024)



Výsledky této otázky, na kterou odpovědělo 190 respondentů, poukazují na to, že přibližně pětina z nich byla svědky toho, že chráněné osoby měly přednostní přístup k vyšetření, což je nejčastěji zmiňovaný typ nadstandardní péče. Nadstandardní vybavení bylo zaznamenáno u téměř šestiny odpovědí, což naznačuje, že i v oblasti materiálního zabezpečení mohou mít chráněné osoby určité výhody. Důležité je také zmínit, že **více než desetina respondentů byla svědkem nedodržení standardních postupů**, což může mít etické a profesionální důsledky. Ostatní uvedené oblasti, jako kvalitnější strava, léky, výživa, nebo vstřícnější přístup, byly zmíněny méně často, což však neznamená, že by nebyly relevantní. Tato data naznačují, že existuje vnímání rozdílů v péči o chráněné osoby, které by mohly vyvolávat otázky týkající se rovnosti a etiky ve zdravotní péči.

Graf 1.4a: Zkušenosti zahraničních zdravotníků s poskytováním nestandardní zdravotní péče; Zdroj: autor (2024)

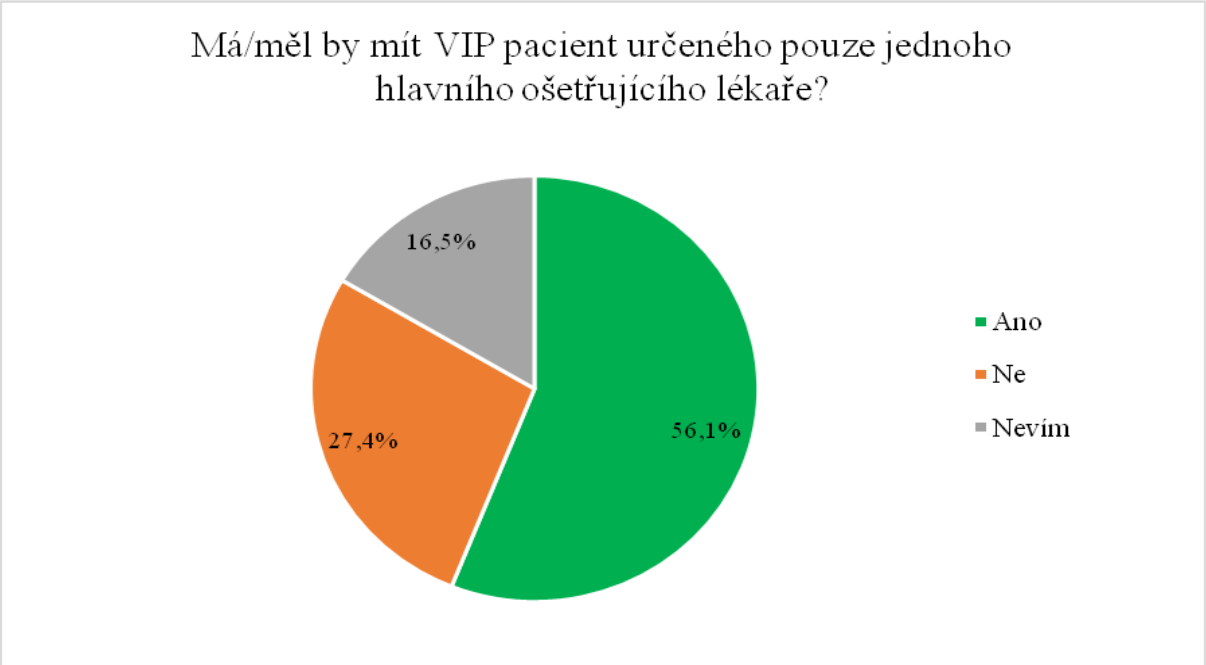


Zahraniční data naznačují, že chráněné osoby jsou ve větší míře upřednostňovány při vyšetřeních, což je zjevně častější praxe v zahraničních zařízeních než v České republice. Nadstandardní vybavení bývá rovněž poskytováno zahraničním pacientům častěji, což poukazuje na mírně vyšší důraz na komfort a technickou úroveň péče. Pokud jde o kvalitu samotné zdravotní péče, výsledky ukazují podobnosti mezi zahraničními a českými zařízeními, přičemž rozdíl je patrný zejména ve větším zaměření zahraničních zařízení na kvalitnější léčiva a výživu, což odráží snahu o vyšší zdravotní standardy pro chráněné osoby. **Zahraniční zařízení se rovněž jeví jako přísnější v dodržování standardních postupů**, což může být dáno lepšími kontrolními mechanismy a důslednějším dodržováním protokolů.

Srovnání s českými zařízeními naznačuje, že zahraniční zařízení poskytují chráněným osobám mírně vyšší úroveň péče ve formě přednostních vyšetření, nadstandardního vybavení a kvalitnější stravy. Toto zvýšené zaměření na kvalitní léky a výživu může být odrazem kulturních a systémových rozdílů ve zdravotní péči, kde zahraniční zařízení kladou větší důraz na medicínské a nutriční standardy. Naopak nižší výskyt nedodržování standardních postupů v zahraničních zařízeních naznačuje lepší dodržování protokolů, což může přispívat k vyšší kvalitě a konzistenci péče. Celkově tato data naznačují, že zahraniční zařízení mají tendenci poskytovat chráněným osobám o něco vyšší standard péče než česká zařízení, což může být

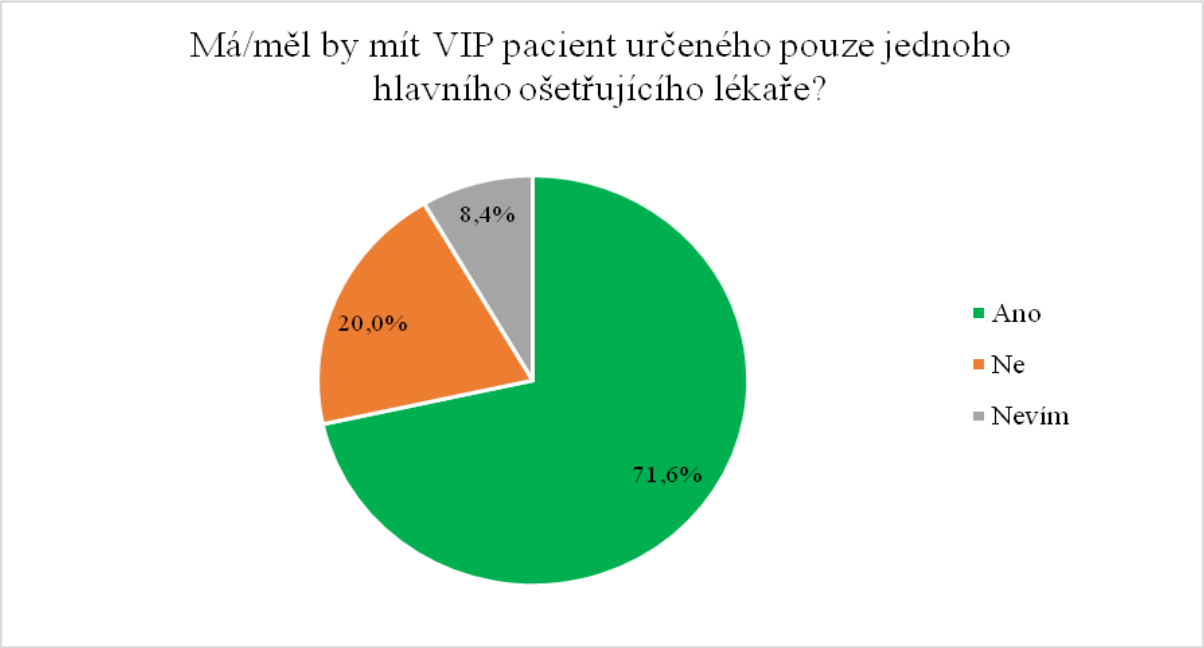
způsobeno rozdílnými přístupy ke zdravotní péči, rozdíly v legislativě nebo vnitřními směrnicemi zdravotnických zařízení.

Graf 1.5: Vyjádření respondentů k otázce jednoho hlavního ošetřujícího lékaře; Zdroj: autor (2024)



Výsledky ukazují, že většina respondentů preferuje, aby chráněná osoba měla jednoho hlavního ošetřujícího lékaře. Tento přístup se jeví jako efektivní zejména z hlediska kontinuity péče, jelikož lékař má lepší přehled o zdravotním stavu pacienta a může lépe koordinovat léčbu. Na druhou stranu, část respondentů se domnívá, že není nutné mít určeného jednoho lékaře, což naznačuje, že někteří upřednostňují flexibilitu a přístup k širšímu týmu odborníků, kteří mohou poskytnout specializovanou péči dle aktuálních potřeb pacienta. Nejednoznačný postoj části respondentů může naznačovat nedostatečnou zkušenost s touto praxí nebo chybějící jasná pravidla. Tento rozmanitý přístup podtrhuje potřebu dalšího výzkumu a možného definování standardů péče, které by zajistily jak kontinuitu, tak multidisciplinární přístup k léčbě.

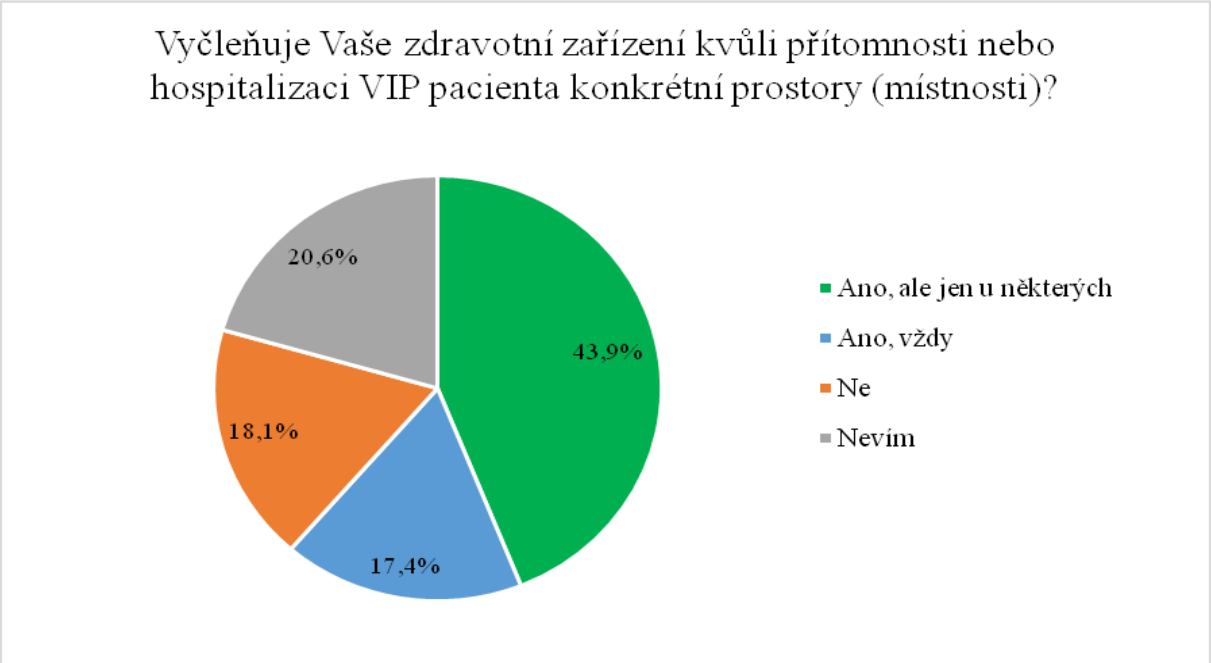
Graf 1.5a: Vyjádření zahraničních respondentů k otázce jednoho hlavního ošetřujícího lékaře; Zdroj: autor (2024)



Výsledky naznačují rozdílné přístupy v názorech na přidělení jednoho hlavního ošetřujícího lékaře chráněným osobám. Zatímco v českém vzorku většina respondentů preferuje přítomnost jednoho klíčového lékaře kvůli kontinuitě péče, významná část respondentů s tímto názorem nesouhlasí a někteří nemají jasný postoj. Tento rozpor může odrážet rozdílné zkušenosti s koordinací péče a jejími praktickými důsledky.

Naopak zahraniční vzorek ukazuje na ještě silnější tendenci k přidělení jednoho lékaře, což může naznačovat větší důraz na centralizaci péče v zahraničních zdravotních systémech. Tato preference je pravděpodobně výsledkem kulturních a systémových rozdílů, kde je jednoznačná odpovědnost hlavního lékaře považována za klíčový prvek péče o pacienty, zejména chráněné osoby. Rozdíly mezi těmito přístupy také naznačují, že zahraniční zdravotnická zařízení kladou vyšší důraz na koordinovanou a personalizovanou péči prostřednictvím jednoho klíčového zdravotnického pracovníka.

Graf 1.6: Otázka samostatných prostor pro poskytování zdravotní péče o chráněné osoby; Zdroj: autor (2024)



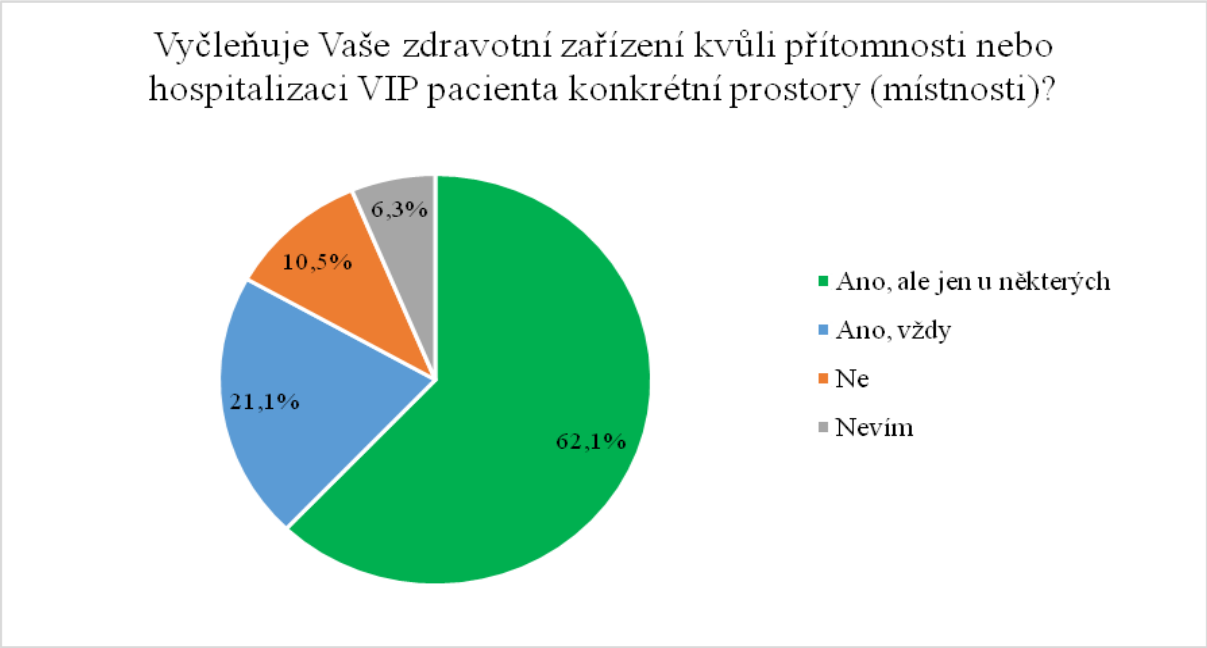
Interpretace výsledků této otázky ukazuje, že přístup zdravotnických zařízení k vyčleňování speciálních prostor pro chráněné osoby je nejednotný a často závisí na konkrétních potřebách nebo specifikách dané situace. Přibližně čtyři z deseti zařízení tuto praxi aplikují pouze selektivně, což může naznačovat, že některé chráněné osoby vyžadují vyšší míru soukromí nebo bezpečnosti, zatímco jiné ne. Tento přístup může být ovlivněn omezenými prostorovými kapacitami nebo organizačními pravidly, která nejsou striktně definována.

Další skupina zařízení se však vyznačuje konzistentním vyčleňováním speciálních místností, což naznačuje vyšší standardizaci postupů při péči o chráněné osoby a jasnou snahu o zajištění jejich bezpečí a soukromí. Tato zařízení zřejmě disponují lepšími kapacitními možnostmi a pravidly, která umožňují předvídatelnost péče.

Naopak některá zdravotnická zařízení prostory nevyčleňují, což může být způsobeno buď omezenými zdroji, nebo vnímáním, že tato opatření nejsou vždy nezbytná. Poměrně významná část personálu, která odpověděla, že o této problematice nemá informace, poukazuje na to, že interní postupy nejsou vždy jasně komunikovány nebo že je o ně zájem spíše omezený.

Tato rozmanitost přístupů naznačuje, že je zapotřebí zlepšit komunikaci a vytvořit jasně definovaná pravidla pro péči o chráněné osoby, aby byla zajištěna jednotnost a předvídatelnost této péče napříč různými zdravotnickými zařízeními.

Graf 1.6a: Otázka samostatných prostor pro poskytování zdravotní péče o chráněné osoby v zahraničí; Zdroj: autor (2024)



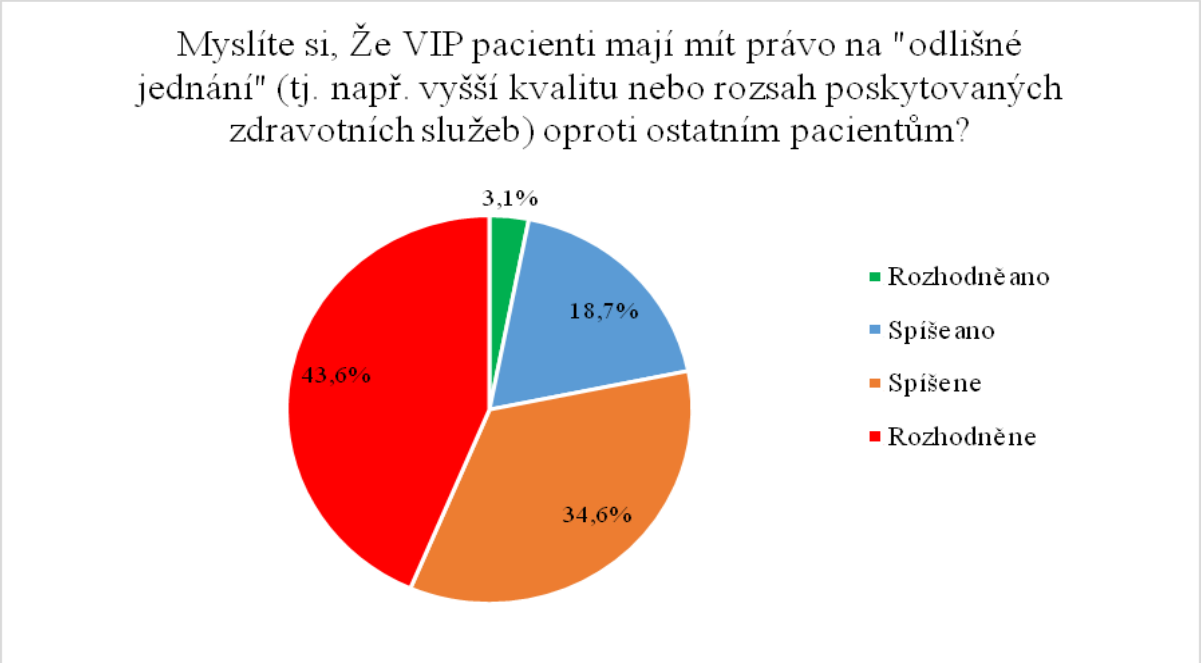
Interpretace zahraničních dat ukazuje, že ve srovnání s českými zařízeními je v zahraničí častější vyčleňování konkrétních prostor pro chráněné osoby. Zahraniční zařízení zřejmě mají více strukturované nebo flexibilní přístupy k poskytování oddělených prostor na základě individuálních potřeb pacientů. Tento přístup může být podpořen lepšími organizačními pravidly nebo dostupností zdrojů.

Významná část zahraničních respondentů rovněž uvedla, že vždy vyčleňují speciální místnosti pro chráněné osoby. Tento přístup odráží důraz na standardizaci a soustavnou ochranu soukromí, což naznačuje, že zahraniční zdravotnická zařízení kladou větší důraz na konzistentní postupy pro zajištění bezpečnosti a komfortu chráněných osob.

Oproti tomu podíl respondentů, jejichž zařízení prostory pro chráněné osoby nevyčleňuje, je v zahraničí výrazně nižší než v českém kontextu. Tento rozdíl může odrážet lepší povědomí o potřebách těchto pacientů nebo lepší infrastrukturu a kapacity pro vyčleňování speciálních místností v zahraničí.

Pozoruhodný je také nižší počet zahraničních respondentů, kteří nemají přehled o tom, jak jsou prostory pro chráněné osoby spravovány, což může svědčit o lepší komunikaci a jasněji definovaných interních postupech v zahraničních zařízeních ve srovnání s těmi českými.

Graf 1.7: Rozdíl v péči o chráněné osoby oproti ostatním pacientům; Zdroj: autor (2024)

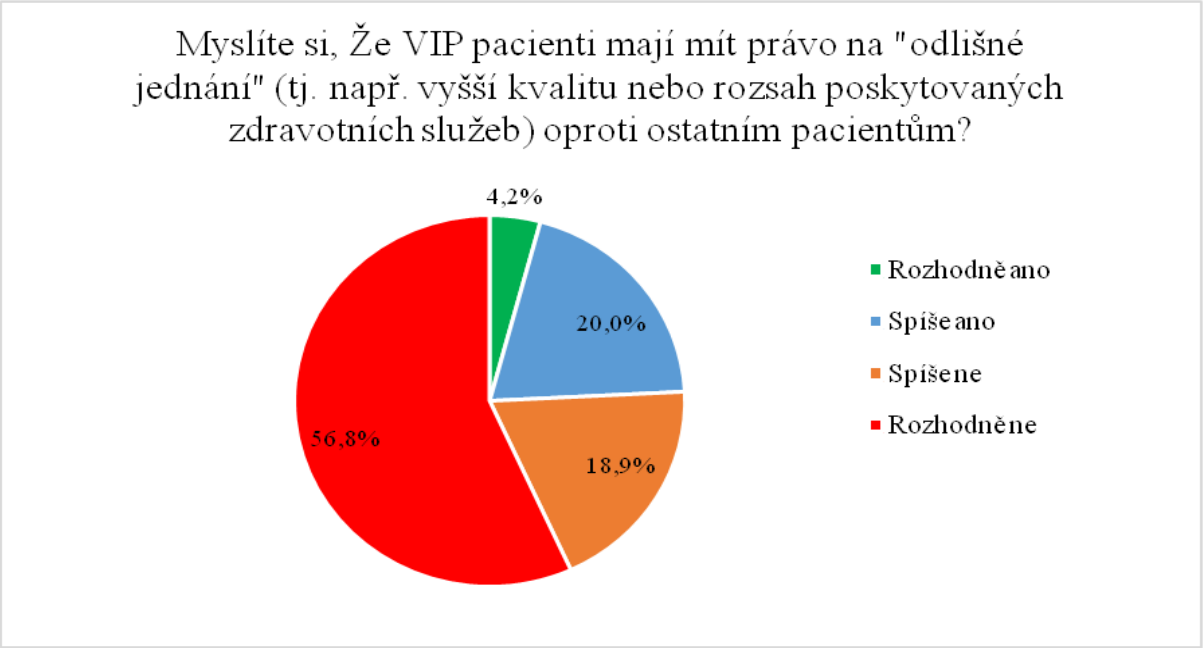


Výsledky této otázky ukazují, že převážná většina respondentů nesouhlasí s tím, aby chráněné osoby měly přístup k odlišné, nadstandardní péči ve srovnání s běžnými pacienty. Tento nesouhlas odráží hluboce zakořeněný názor, že zdravotní péče by měla být poskytována na základě rovnosti, bez ohledu na postavení pacienta. Respondenti tímto preferují zachování spravedlivého přístupu k péči, kdy žádná skupina pacientů není zvýhodňována na úkor druhých.

Nesouhlas s preferenčním zacházením může být také veden obavami z možného porušení etických zásad a rizika vzniku diskriminace. Představa, že by chráněné osoby měly mít lepší přístup k péči než ostatní pacienti, by mohla ohrozit rovnováhu v poskytování zdravotních služeb a narušit důvěru v systém zdravotní péče. Rovnost je zde vnímána jako základní prvek spravedlnosti, což naznačuje, že zdravotnický personál silně podporuje princip rovného přístupu ke zdravotní péči pro všechny pacienty, bez výjimek.

Tento názor odpovídá etickým standardům zdravotní péče, které zdůrazňují, že každý pacient by měl mít stejnou šanci na kvalitní péči, nezávisle na svém společenském nebo politickém postavení.

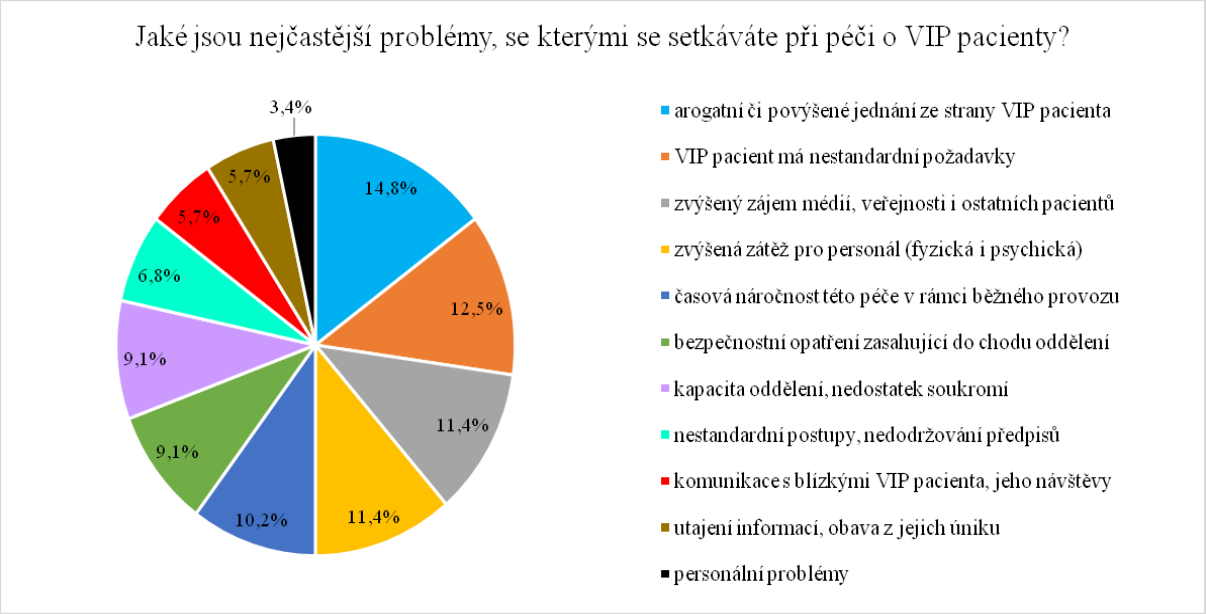
Graf 1.7a: Rozdíl v péči o chráněné osoby oproti ostatním pacientům v zahraničí; Zdroj: autor (2024)



Na základě srovnání českých a zahraničních dat je zřejmé, že v obou skupinách převládá názor, že chráněné osoby by neměly mít nárok na speciální zacházení v rámci zdravotní péče. V českém vzorku tento nesouhlas vyjádřilo 78,2 % respondentů, zatímco zahraniční vzorek ukazuje mírně nižší míru nesouhlasu. Toto svědčí o podobném vnímání rovnosti ve zdravotní péči napříč různými zeměmi. Podíl těch, kteří podporují preferenční přístup, je nižší u zahraničních respondentů ve srovnání s českými respondenty (21,8 %).

Obě skupiny kladou důraz na spravedlivý přístup ke zdravotní péči, čímž se přibližují etickým standardům, které vyzdvihují rovnost bez ohledu na sociální status pacienta. Z výsledků je patrné, že obě skupiny mají obavy z možných nespravedlností a diskriminačních praktik, pokud by určité skupiny pacientů byly upřednostňovány. Tento společný postoj zdůrazňuje nutnost jasně definovaných pravidel a transparentních procedur, které zajistí spravedlivý přístup ke zdravotní péči pro všechny pacienty.

Graf 1.8: Nejčastější problémy při péči o chráněné osoby; Zdroj: autor (2024)



Výsledky této otázky odhalují široké spektrum výzev, se kterými se zdravotnický personál setkává při péči o chráněné osoby. Jedním z hlavních problémů, které respondenti uváděli, bylo nevhodné nebo povýšené chování chráněných osob, což může zdravotní péči komplikovat a vytvářet napětí mezi personálem a pacienty. Nestandardní požadavky pacientů, které se odchylují od běžné zdravotnické praxe, také představují výzvu, zejména pokud nejsou v souladu s běžnými protokoly nebo možnostmi zařízení.

Další výzvou, kterou respondenti zmínili, je zvýšený zájem médií a veřejnosti o péči o chráněné osoby. Tento zvýšený zájem nejenže klade tlak na zdravotnický personál, ale může také narušit soukromí ostatních pacientů. K tomu se přidává zvýšená psychická a fyzická zátěž na personál, který musí zvládat nejen standardní péči, ale i specifické požadavky a bezpečnostní opatření spojená s péčí o chráněné osoby.

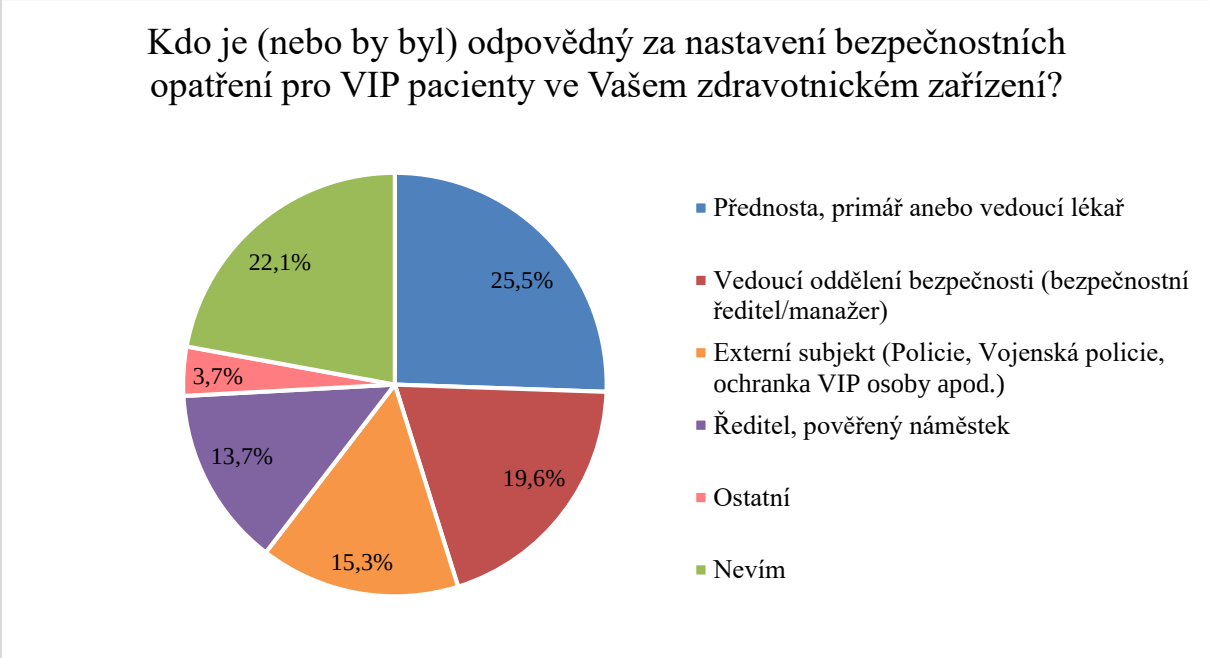
Bezpečnostní opatření, ať už jde o fyzickou ochranu nebo ochranu informací, zasahují do běžného chodu oddělení a mohou komplikovat organizaci péče. To se často projevuje jako problém s kapacitou a nedostatkem soukromí, což zvyšuje tlak na organizaci provozu. Nestandardní postupy, které nejsou v souladu s běžnými předpisy, dále komplikují práci personálu, který se musí rychle přizpůsobit měnícím se podmínkám.

Výsledky také ukazují, že komunikace s blízkými chráněných osob a obavy z úniku citlivých informací jsou sice méně častými, ale stále relevantními problémy. Tyto aspekty poukazují na potřebu nejen standardizovat přístup k péči o chráněné osoby, ale také zajistit důkladné školení

personálu v této oblasti, aby byla péče efektivní a v souladu s etickými a bezpečnostními požadavky.

- **Sekce 2: Fyzická a bezpečnostní opatření chráněných osob**

Graf 2.1: Určení odpovědnosti za nastavení bezpečnostních opatření pro chráněné osoby; Zdroj: autor (2024)



Interpretace výsledků této otázky naznačuje různorodost přístupů k odpovědnosti za nastavení bezpečnostních opatření pro chráněné osoby ve zdravotnických zařízeních. Největší část respondentů uvedla, že za tato opatření odpovídá přednosta, primář nebo vedoucí lékař, což je logické, jelikož tito lékaři přímo řídí péči o pacienty a nesou odpovědnost za jejich bezpečnost. Jejich role zahrnuje rozhodování o klinických aspektech péče i o fyzické bezpečnosti pacientů na odděleních.

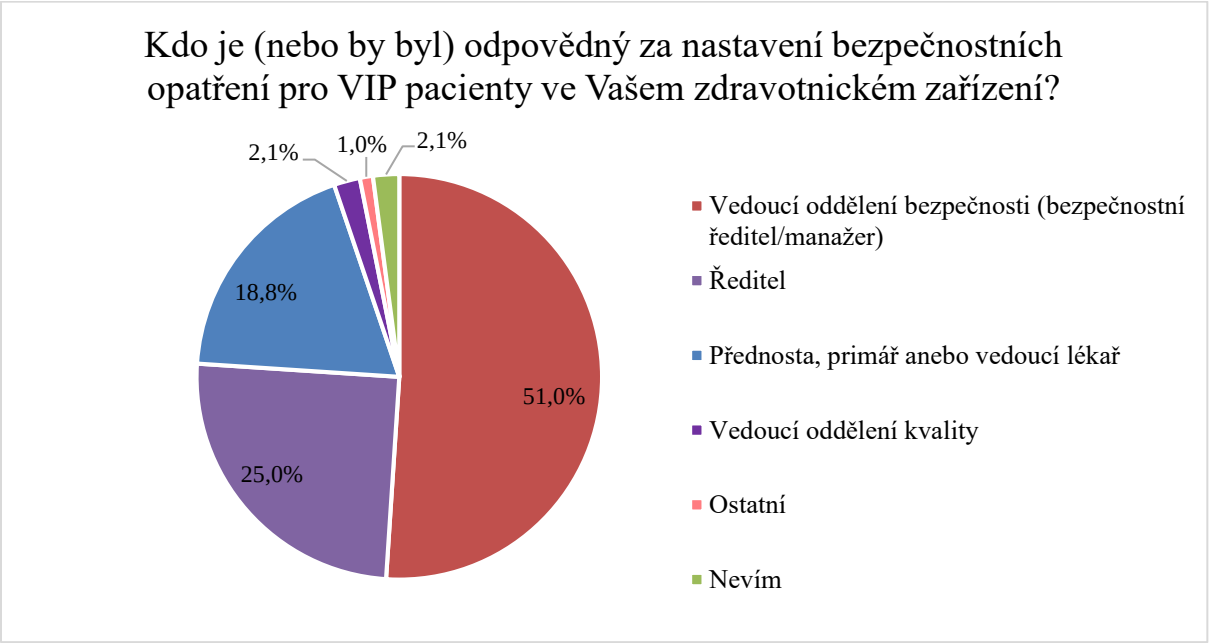
Další velká skupina respondentů uvedla, že neví, kdo je za bezpečnostní opatření odpovědný, což může být indikací nedostatečné komunikace v některých zařízeních nebo chybějícího jasného nastavení odpovědnosti v rámci organizačních struktur. Tento nedostatek povědomí by mohl vést k nejasnostem v případě bezpečnostních hrozeb nebo krizových situací, což je alarmující vzhledem k důležitosti ochrany chráněných osob.

Významná část odpovědí také ukázala na roli vedoucího bezpečnostního oddělení, což naznačuje existenci specifických oddělení pro řízení bezpečnosti ve zdravotnických zařízeních,

zejména v těch, která pečují o vysoce exponované osoby. Zajímavé je, že v některých případech za bezpečnostní opatření odpovídají externí subjekty, jako je policie nebo vojenská policie, což ukazuje na potřebu zapojení vnějších bezpečnostních složek v případech, kdy může být bezpečnostní situace komplexnější nebo spojená s hrozbami zvenčí.

Menší část respondentů přičítá odpovědnost ředitelům nebo náměstkům zdravotnických zařízení, což naznačuje, že v některých případech je bezpečnost chápána jako strategická záležitost vyžadující vedení na nejvyšší úrovni managementu. Tento rozptyl odpovědností napříč zařízeními reflektuje různé organizační struktury a způsoby správy bezpečnosti, které jsou pravděpodobně ovlivněny jak velikostí, tak zaměřením konkrétního zdravotnického zařízení.

Graf 2.1a: Určení odpovědnosti za nastavení bezpečnostních opatření pro chráněné osoby; Zdroj: autor (2024)



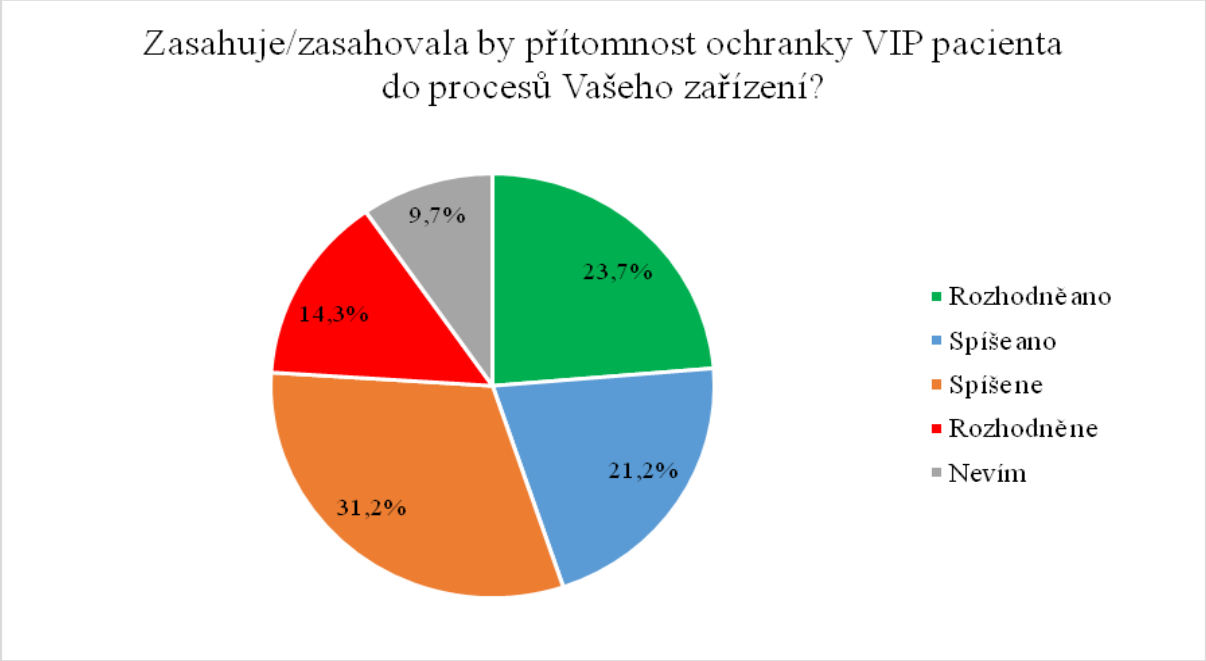
Na základě srovnání českých a zahraničních dat lze identifikovat výrazné rozdíly ve struktuře odpovědnosti za nastavení bezpečnostních opatření pro chráněné osoby. Zahraniční data ukazují, že většina zdravotnických zařízení preferuje specializované bezpečnostní struktury a personál, kdy vedoucí oddělení bezpečnosti nebo bezpečnostní manažer hraje klíčovou roli ve více než polovině případů. Tento přístup naznačuje, že v zahraničních zařízeních je ochrana chráněných osob prioritou, což vede k zavedení specializovaných oddělení s jasnými a formalizovanými postupy.

V českém kontextu však odpovědnost za bezpečnost častěji připadá vedoucím lékařům, přednostům nebo primářům, kteří zajišťují jak lékařskou péči, tak bezpečnostní opatření. Tento rozdíl může ukazovat na menší míru specializace v českých zařízeních, kde bezpečnost není až tak formálně strukturovaná jako v zahraničí.

Dalším zajímavým rozdílem je výrazně vyšší podíl ředitelů zodpovědných za bezpečnost v zahraničních zařízeních, což může ukazovat na to, že bezpečnostní otázky jsou tam chápány jako strategická záležitost řízená na nejvyšší úrovni managementu. Naopak v českých zařízeních je tato odpovědnost spíše distribuována na nižší úrovně vedení, což může reflektovat odlišnou organizační strukturu nebo nižší prioritu, kterou česká zařízení věnují bezpečnostním otázkám ve srovnání s jejich zahraničními protějšky.

Zahraniční zařízení tedy vykazují vyšší míru specializace a jasněji definované odpovědnosti, což vede k efektivnějšímu zajištění bezpečnosti chráněných osob, zatímco česká zdravotnická zařízení mají tendenci tuto odpovědnost více rozdělovat mezi různé vedoucí pozice.

Graf 2.2: Vliv přítomnosti ochranky na procesy zdravotnického zařízení; Zdroj: autor (2024)



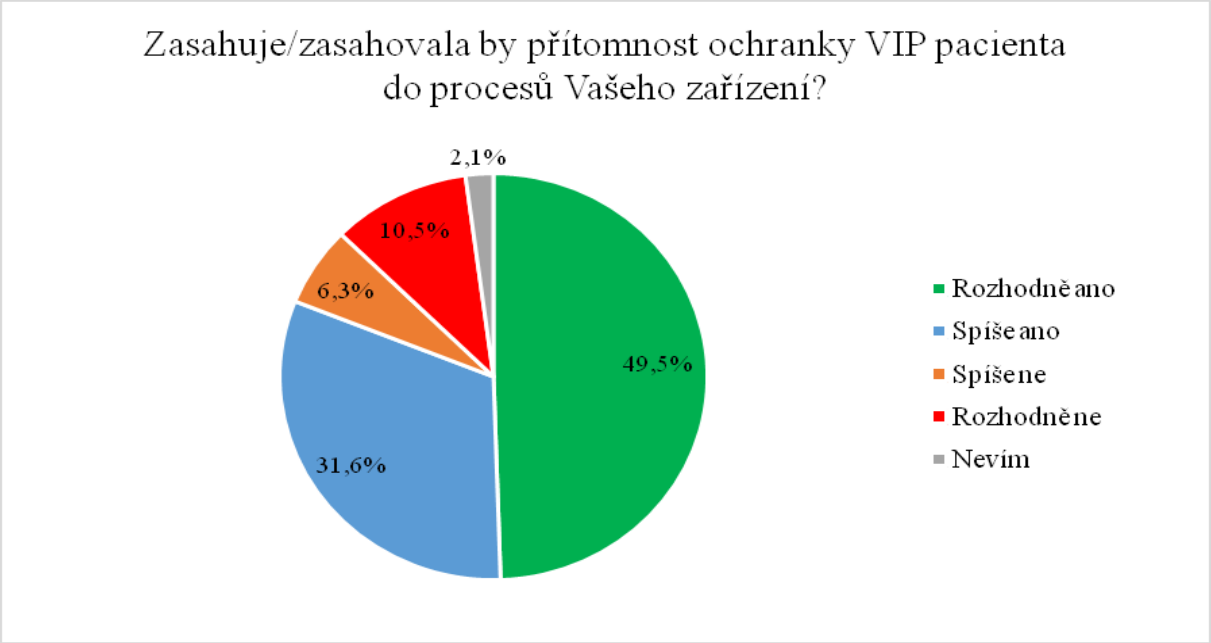
Výsledky této otázky ukazují, že přítomnost ochranky chráněné osoby je vnímána jako faktor, který může mít vliv na běžné procesy zdravotnických zařízení. Přibližně polovina respondentů uvedla, že přítomnost ochranky zasahuje do chodu jejich zařízení. Tento zásah se pravděpodobně projevuje především ve formě bezpečnostních opatření, která vyžadují

přizpůsobení provozních a logistických postupů, což může způsobit určité komplikace. Mezi časté problémy patří například omezený přístup ostatních pacientů nebo zvýšený tlak na personál.

Na druhé straně, přibližně třetina respondentů uvedla, že přítomnost ochranky nemá významný dopad na jejich zdravotnické zařízení, což naznačuje, že některá zařízení mohou mít lépe integrované postupy a protokoly pro práci s chráněnými osobami. Tato zařízení pravděpodobně disponují efektivními metodami, jak zajistit bezpečnost chráněných osob bez narušení běžného provozu.

Ukazuje se, že zkušenost s přítomností ochranky může být značně rozdílná, což je závislé na organizaci, vybavení a školení personálu. Aby se minimalizoval negativní dopad na chod zařízení, je důležité zajistit jasně definované a standardizované postupy a školení pro zdravotnický personál i bezpečnostní pracovníky. To by zajistilo hladký průběh spolupráce a pomohlo efektivně chránit chráněné osoby, aniž by byl ohrožen standardní provoz a péče o ostatní pacienty.

Graf 2.2a: Vliv přítomnosti ochranky na procesy zdravotnického zařízení v zahraničí; Zdroj: autor (2024)



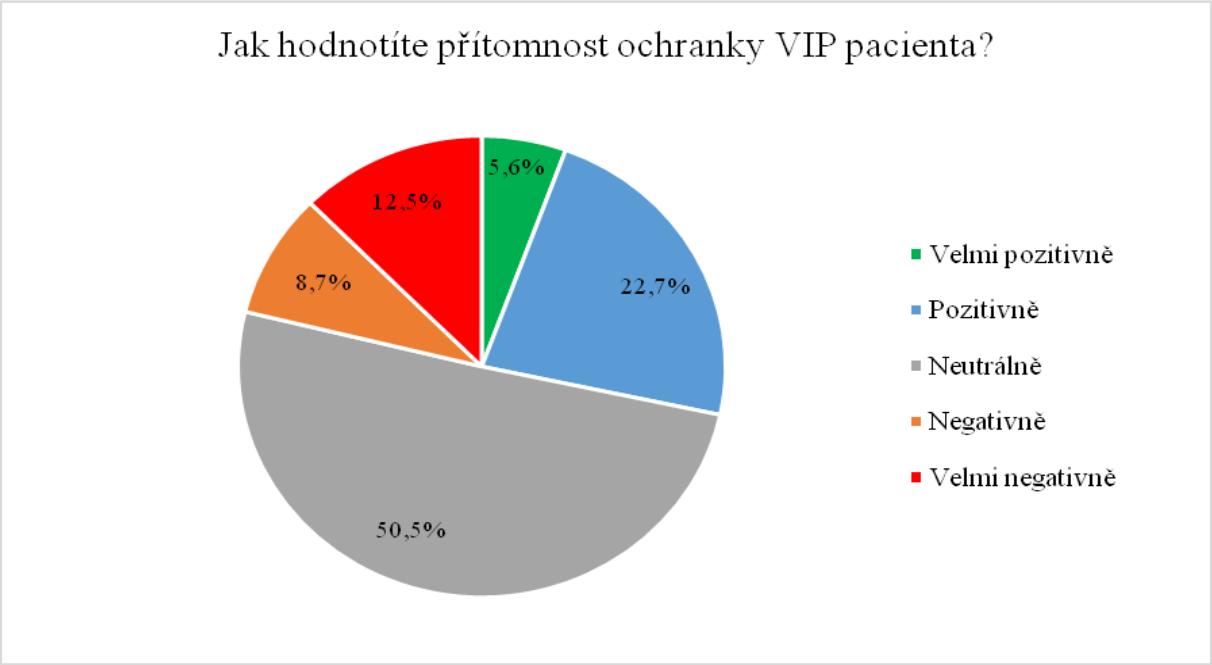
Na základě dat ze zahraničního průzkumu a jejich srovnání s českými výsledky lze říci, že názory na vliv přítomnosti ochranky na procesy ve zdravotnických zařízeních jsou v obou kontextech relativně podobné. V obou skupinách většina respondentů vnímá přítomnost

ochranky jako významný zásah do běžného provozu zařízení. V zahraničních datech skoro polovina respondentů uvádí, že přítomnost ochranky výrazně ovlivňuje jejich zařízení, což je v souladu s českými daty, kde téměř stejný podíl respondentů vyjádřil podobný názor.

Nižší podíl zahraničních respondentů, kteří uvedli, že přítomnost ochranky nemá na jejich zařízení vliv, naznačuje, že v některých zahraničních zdravotnických systémech mohou mít lepší zkušenosti s integrací bezpečnostních opatření do běžného provozu. To může být způsobeno pokročilejšími protokoly, zkušenostmi nebo zdroji, které umožňují minimalizovat narušení chodu zařízení při zajišťování bezpečnosti chráněných osob.

Rozdíl mezi českými a zahraničními zařízeními by také mohl odrážet kulturní přístupy k bezpečnosti nebo organizační struktury, kde se může lišit míra zapojení bezpečnostních složek do každodenního chodu zdravotnických zařízení.

Graf 2.3: Vnímání přítomnosti ochranky zaměstnanci; Zdroj: autor (2024)

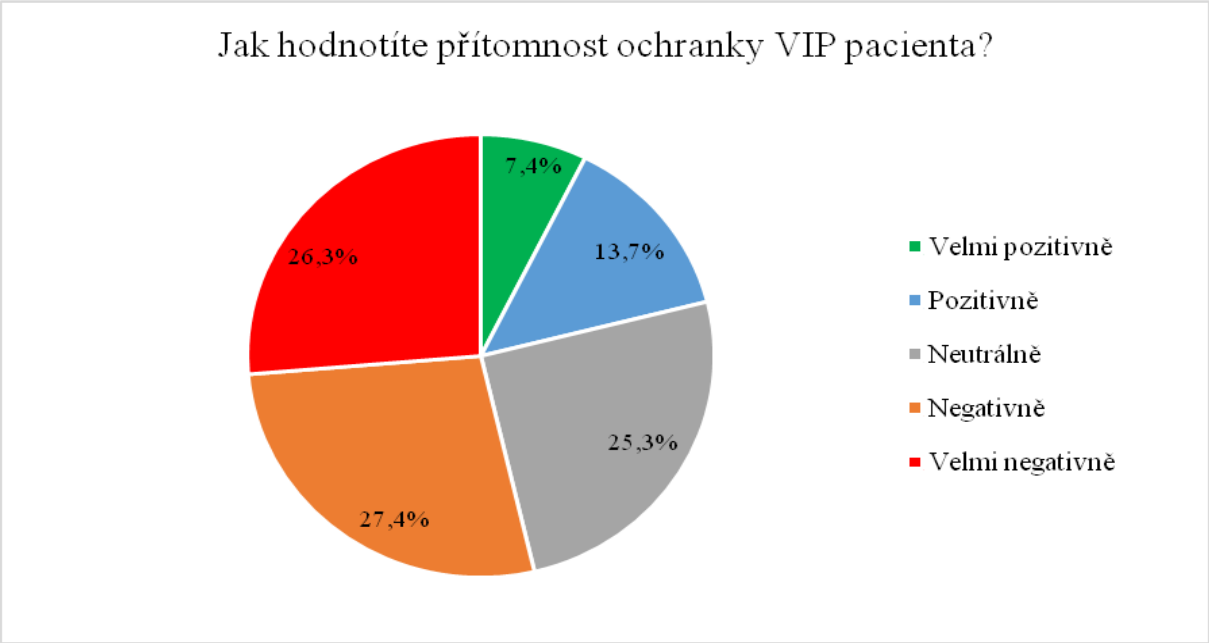


Výsledky této otázky poukazují na to, že vnímání přítomnosti ochranky chráněné osoby ve zdravotnických zařízeních je rozmanité. Přibližně polovina respondentů se k přítomnosti ochranky vyjádřila neutrálně, což naznačuje, že pro mnoho zdravotnických pracovníků není tento faktor významným nebo rušivým elementem v jejich práci. Přibližně třetina respondentů hodnotí přítomnost ochranky pozitivně či velmi pozitivně, což by mohlo naznačovat, že tito zaměstnanci vnímají ochranu chráněných osob jako nezbytnou součást zajištění jejich bezpečnosti a bezproblémového poskytování zdravotní péče. Na druhou stranu, více než pětina

respondentů uvedla, že přítomnost ochranky hodnotí negativně či velmi negativně, což může souviset s obavami z narušení pracovních procesů, zvýšeným stresem či omezením přístupu ke chráněné osobě.

Tato různorodost názorů ukazuje na nutnost hledat vyvážený přístup k otázce bezpečnostních opatření pro chráněné osoby ve zdravotnických zařízeních, který by zohledňoval jak potřeby a komfort pacientů, tak i pracovní pohodu a efektivitu zdravotnického personálu. Důležité je zajistit, aby přítomnost ochranky nevedla k narušení běžného chodu zdravotnického zařízení a aby byla přijata opatření, která minimalizují potenciální negativní dopady na pracovní prostředí.

Graf 2.3a: Vnímání přítomnosti ochranky zahraničními zaměstnanci; Zdroj: autor (2024)



Na základě českých dat jsou názory na přítomnost ochranky chráněných osob ve zdravotnických zařízeních značně rozdělené. Přibližně polovina respondentů hodnotí tento faktor neutrálně, což naznačuje, že pro mnoho zdravotnických pracovníků není přítomnost ochranky významným narušením jejich práce. To by mohlo svědčit o tom, že přítomnost bezpečnostního personálu je běžně akceptovanou součástí péče o chráněné osoby a nenarušuje standardní procesy.

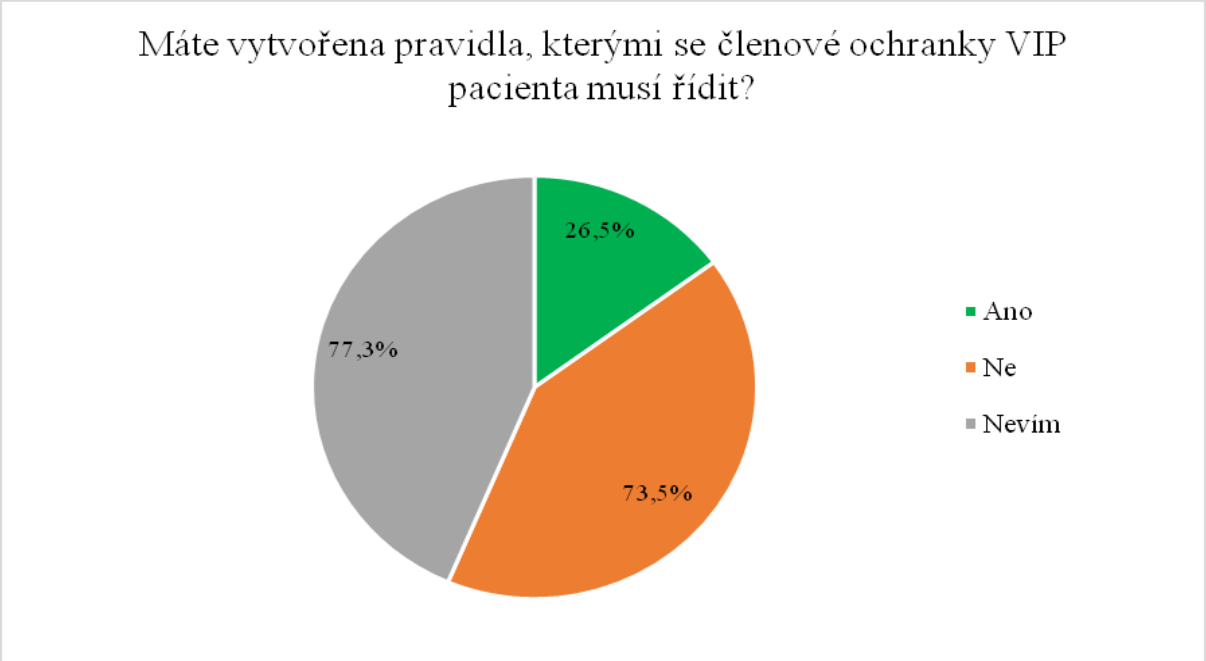
Na druhou stranu, více než pětina českých respondentů vnímá přítomnost ochranky pozitivně. Tito respondenti pravděpodobně vnímají ochranku jako klíčový prvek pro zajištění bezpečnosti chráněných osob a hladkého průběhu jejich léčby, zvláště pokud jsou tyto osoby vystaveny

rizikům ze strany veřejnosti nebo médií. Přítomnost ochranky může také pomoci lékařům a dalším pracovníkům soustředit se na poskytování zdravotní péče bez dalších obav o bezpečnost pacienta.

Naopak více než polovina respondentů vyjadřuje negativní postoj k přítomnosti ochranky, což může být způsobeno obavami z narušení každodenních pracovních procesů, zvýšeného stresu nebo omezení přístupu k pacientům. Tento negativní postoj by mohl odrážet zkušenosti pracovníků s nadměrnými zásahy ochranky, které mohou narušit standardní zdravotnické operace a komunikaci mezi pacienty a zdravotnickým personálem.

Při srovnání s daty ze zahraničních zařízení se zdá, že zahraniční respondenti mají tendenci více vnímat přítomnost ochranky jako významný zásah do každodenních operací, přičemž téměř polovina respondentů uvádí, že přítomnost ochranky má přímý vliv na chod jejich zařízení. Tento rozdíl může být způsoben organizačními a kulturními rozdíly v přístupu k bezpečnosti a péči o chráněné osoby.

Graf 2.4: Existence pravidel činnosti ochranky; Zdroj: autor (2024)

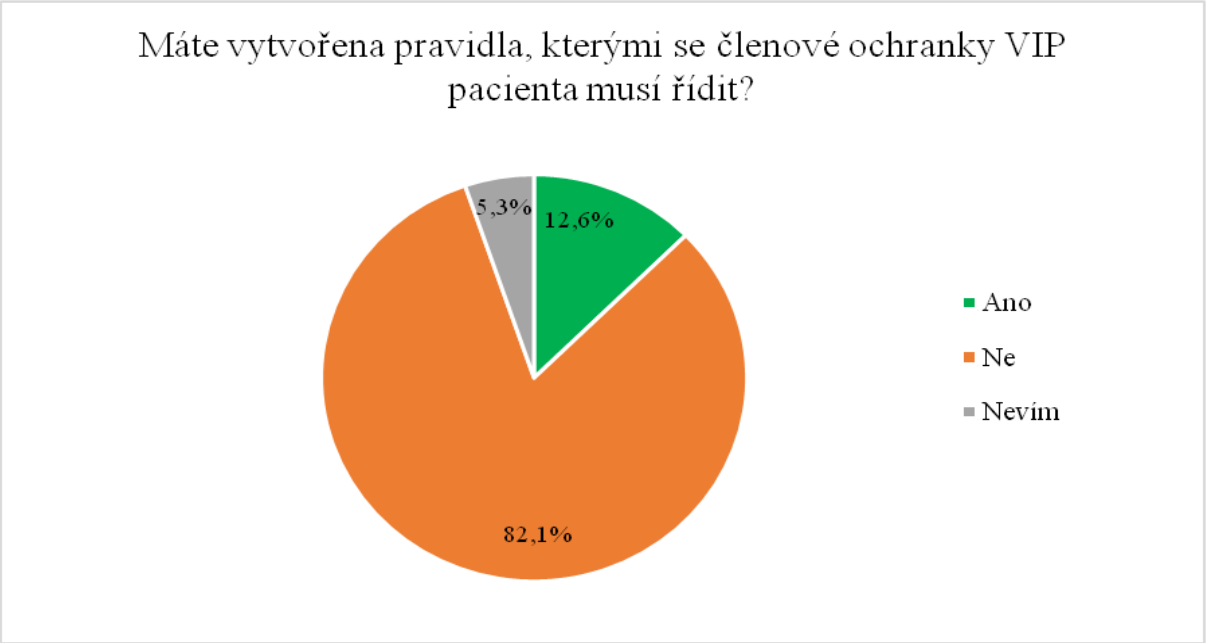


Výsledky otázky, zda mají zdravotnická zařízení nastavena pravidla pro činnost členů ochranky při péči o chráněné osoby, ukazují na výrazný nedostatek organizace v této oblasti. Pouze malá část respondentů potvrzuje, že taková pravidla existují, což svědčí o určité míře strukturovaného přístupu v některých zařízeních. Nicméně většina respondentů, kteří uvedli, že žádná pravidla nejsou nastavena, odhaluje velké mezery v standardizovaných postupech při spolupráci

s ochrankou. Tato absence jasně definovaných pravidel může znamenat rizika nejen pro plynulý chod zařízení, ale i pro samotnou bezpečnost pacientů a personálu.

Navíc zjištění, že většina respondentů ani neví, zda jejich zařízení pravidla pro ochranku má, poukazuje na vážné nedostatky v komunikaci a školení zaměstnanců v této otázce. To může vést k nejasnostem a nesrovnalostem v přístupu k bezpečnosti chráněných osob, což může komplikovat spolupráci mezi zdravotnickým personálem a bezpečnostními složkami. Tyto výsledky zdůrazňují potřebu vytvoření jasných a standardizovaných pravidel pro koordinaci s ochrankou, aby byla zajištěna bezpečnost a efektivita provozu zdravotnických zařízení.

Graf 2.4a: Existence pravidel činnosti ochranky; Zdroj: autor (2024)



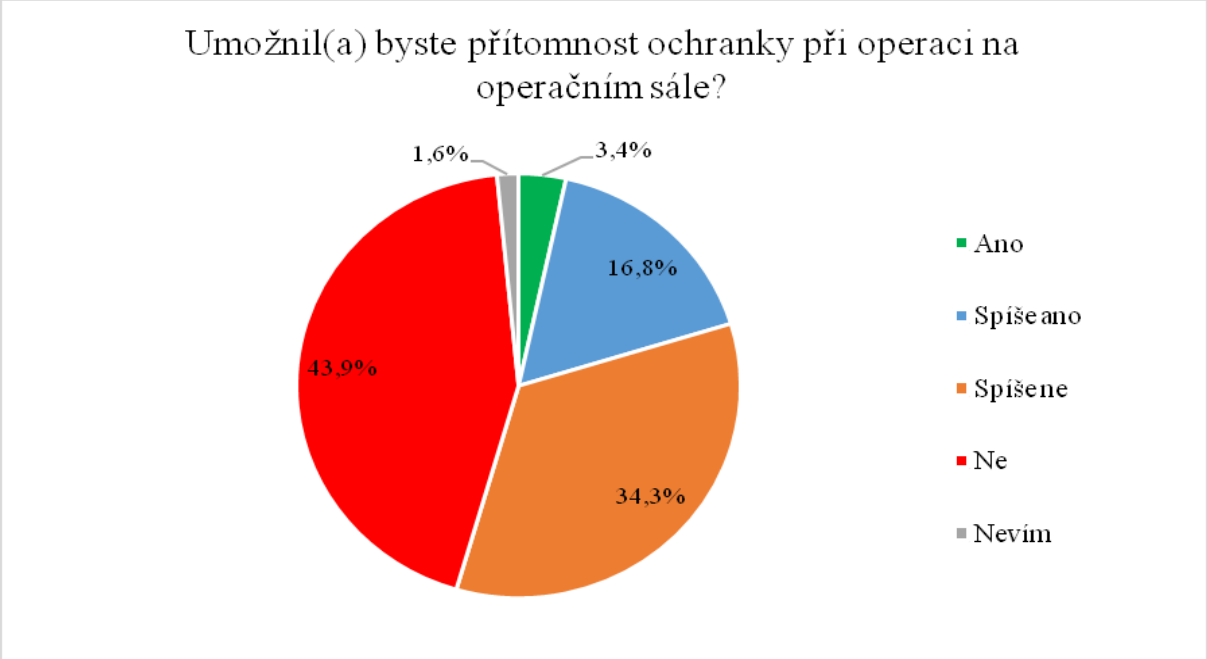
Interpretace zahraničních dat ukazuje, že i ve zdravotnických zařízeních mimo Českou republiku se projevuje nedostatek formálních pravidel pro činnost členů ochranky při péči o chráněné osoby. Pouze malá část respondentů uvedla, že taková pravidla existují, což odráží nízkou úroveň standardizace a organizace bezpečnostních opatření ve zdravotnických zařízeních. To znamená, že i v zahraničí je častým problémem neexistence formálně stanovených postupů, což může vést k obtížné koordinaci mezi bezpečnostním personálem a zdravotnickým týmem.

Na druhou stranu, i když má jen malý počet zahraničních zdravotnických zařízení formální pravidla, je zde nižší míra neinformovanosti o této problematice než v českých zařízeních. Tento rozdíl poukazuje na lepší interní komunikaci ve zdravotnických zařízeních mimo Česko,

přestože v obou případech přetrvává potřeba zlepšit standardizaci postupů a jasněji definovat role bezpečnostních složek při péči o chráněné osoby.

Při porovnání se situací v České republice lze konstatovat, že česká zdravotnická zařízení mají o něco vyšší míru formalizovaných pravidel. To může naznačovat, že zatímco v českých zařízeních existují formální snahy o vytvoření těchto pravidel, stále přetrvává nedostatek jasné komunikace ohledně jejich existence mezi personálem.

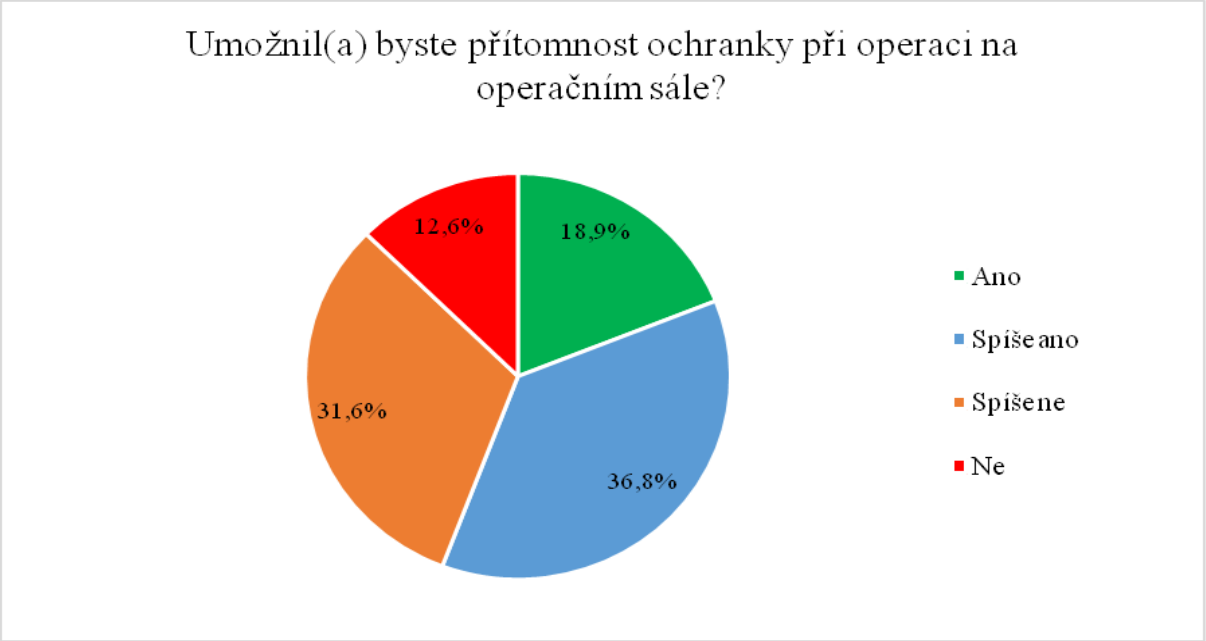
Graf 2.5: Přítomnost ochranky při operaci na operačním sále; Zdroj: autor (2024)



Výsledky této otázky ukazují, že většina zdravotnického personálu se staví proti přítomnosti ochranky na operačním sále. Výrazná část respondentů vyjádřila jednoznačný nesouhlas, což může souviset s obavami z narušení sterilního prostředí, bezpečnosti a klidného průběhu chirurgických výkonů. Mezi důvody mohou patřit také obavy o zachování soukromí pacienta, zajištění intimity při citlivých zákrocích a udržení nekomplikované dynamiky mezi lékaři a pacienty.

Menší část respondentů souhlasila s přítomností ochranky, což může naznačovat, že existují situace, kdy by bezpečnostní opatření byla považována za nezbytná, například u vysoce rizikových osob, ale i zde je zřejmé, že by muselo být zajištěno minimální narušení zdravotnických procesů. Výzkum by se mohl zaměřit na zhodnocení těchto obav a na vytvoření pravidel, která by v konkrétních případech umožnila přítomnost ochranky, aniž by to ohrozilo kvalitu a bezpečnost péče.

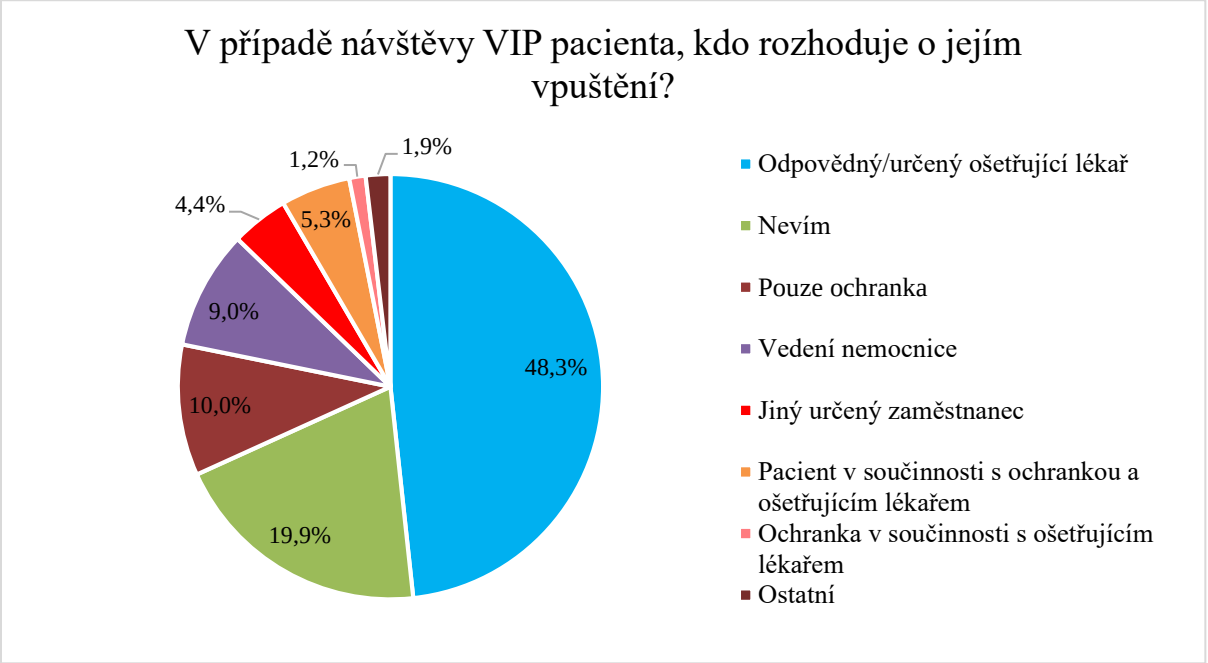
Graf 2.5a: Přítomnost ochranky při operaci na operačním sále; Zdroj: autor (2024)



Zahraniční data ukazují, že názory na přítomnost ochranky na operačním sále jsou mezi zdravotnickým personálem více rozdělené než v českém kontextu. Více než polovina zahraničních respondentů (55,7 %) vyjádřila ochotu umožnit přítomnost ochranky během operací. Tato otevřenost může odrážet větší důraz na bezpečnost v mezinárodním prostředí, zejména pokud jde o vysoce chráněné osoby, u kterých může existovat zvýšené riziko. Na druhou stranu, zbývajících 44,2 % respondentů je proti této praxi, což poukazuje na obavy z potenciálních komplikací spojených s narušením sterility, ohrožením bezpečnosti pacientů nebo zpomalením operací.

Ve srovnání s českými daty, kde až 78,2 % respondentů vyjádřilo nesouhlas s přítomností ochranky na operačním sále, je patrný větší odpor v českém prostředí. Pouze 20,2 % českých respondentů podporuje myšlenku přítomnosti ochranky během operací, což naznačuje výrazně konzervativnější postoj k ochraně sterility a bezpečnosti během chirurgických zákroků. Tento rozdíl může být způsoben kulturními a systémovými rozdíly v přístupu k bezpečnosti, organizaci zdravotnických týmů a ochraně soukromí pacienta.

Graf 2.6: Rozhodnutí o umožnění návštěvy chráněné osoby; Zdroj: autor (2024)



Výsledky této otázky ukazují, že o návštěvách chráněné osoby rozhoduje především ošetřující lékař, což zdůrazňuje jeho klíčovou roli nejen v poskytování zdravotní péče, ale i v organizaci a řízení bezpečnostních opatření. Skutečnost, že téměř polovina respondentů uvedla ošetřujícího lékaře jako hlavního rozhodovatele, odráží důležitost, kterou hraje ve vyvážení potřeb pacienta a bezpečnostních požadavků.

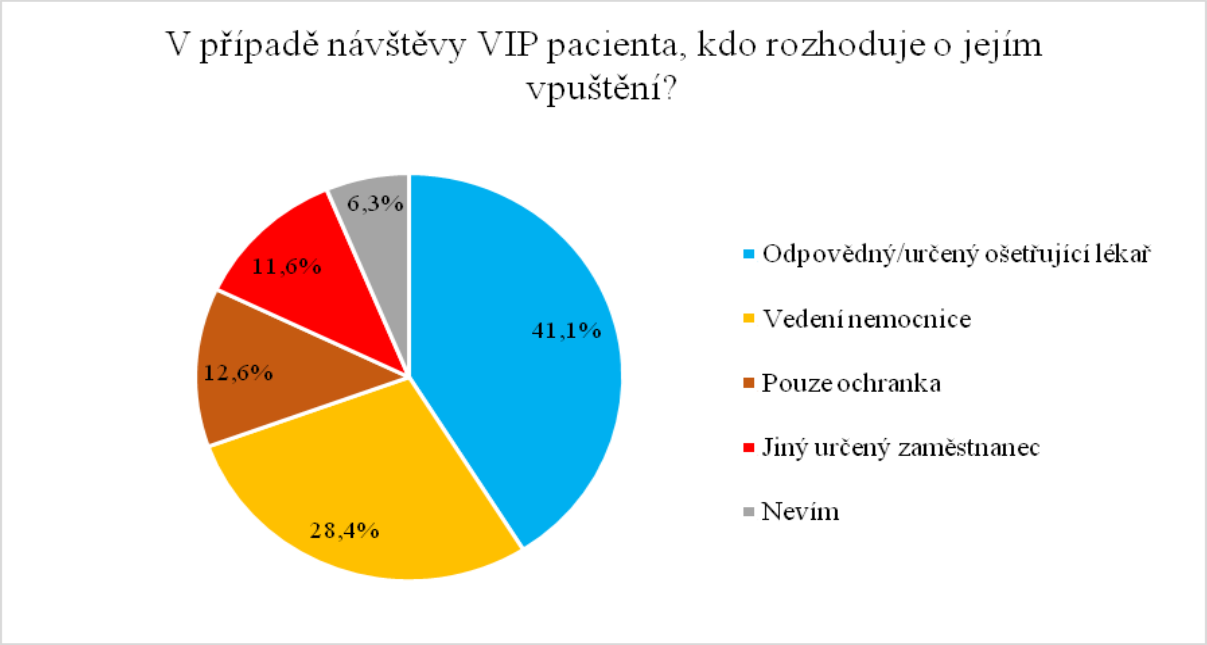
Zároveň téměř pětina respondentů nebyla schopna identifikovat, kdo je za rozhodování o návštěvách zodpovědný, což může poukazovat na nedostatečnou informovanost personálu či absenci jasně definovaných pravidel v některých zdravotnických zařízeních. Toto procento naznačuje, že je v některých institucích třeba zlepšit komunikaci týkající se postupů a odpovědností.

Pouze desetina případů rozhoduje o vpuštění návštěvy bezpečnostní personál, což ukazuje na spíše podpůrnou roli ochranky ve srovnání s rozhodováním lékařů. Vedení nemocnic bylo uvedeno jako rozhodující subjekt v téměř desetině případů, což znamená, že na manažerské úrovni se do těchto záležitostí zasahuje jen v menšině případů.

Tento rozmanitý přístup k rozhodování o návštěvách ukazuje na určitou flexibilitu zdravotnických zařízení, která se přizpůsobuje konkrétním situacím a potřebám chráněných osob. Na druhou stranu však také vytváří prostor pro možné nejasnosti či nedorozumění, což

může vést k potřebě více sjednotit a formalizovat pravidla pro zajištění jednotného postupu ve všech zařízeních.

Graf 2.6a: Rozhodnutí o umožnění návštěvy chráněné osoby; Zdroj: autor (2024)

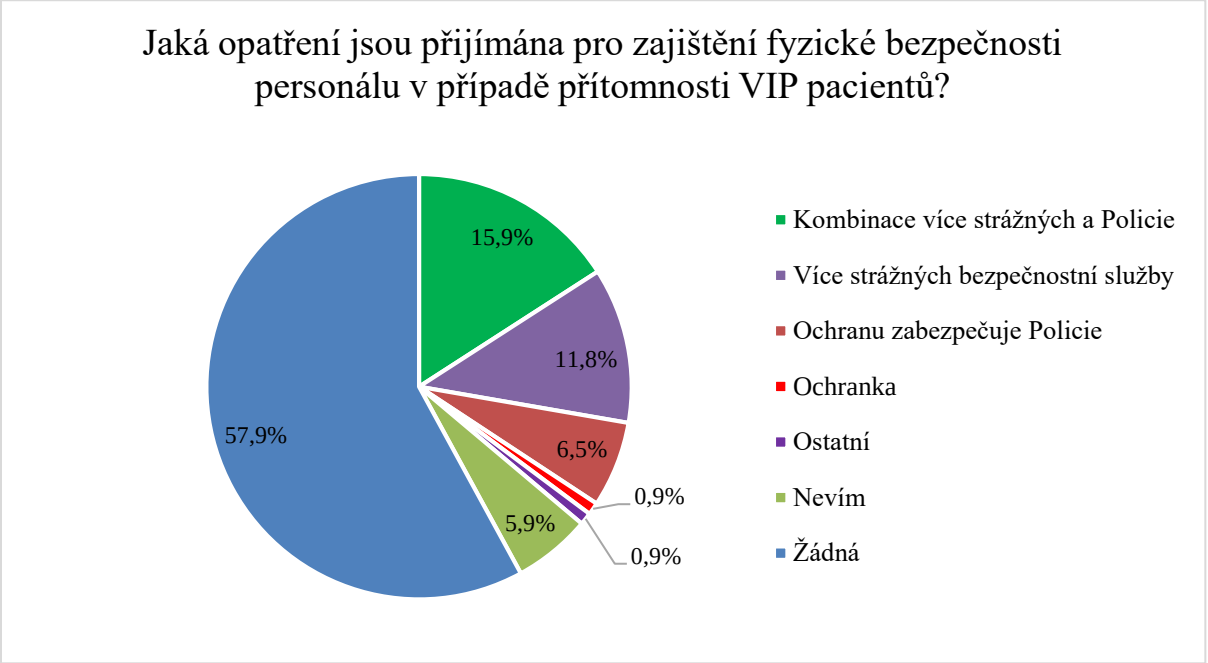


Výsledky zahraničních zdravotnických zařízení ukazují, že rozhodování o vpuštění návštěv chráněných osob nejčastěji spadá pod odpovědného ošetřujícího lékaře, což je podobné jako v českých zařízeních. Zajímavým rozdílem je však větší zapojení vedení zdravotnických zařízení v zahraničí, kde se management aktivně podílí na těchto rozhodnutích téměř v třetině případů. To ukazuje na větší strategickou roli vedení v oblasti bezpečnostních opatření v zahraničních institucích, kdežto v Česku tuto roli hraje především lékařský personál.

Bezpečnostní personál má ve srovnání s lékaři menší podíl na rozhodování o návštěvách, což platí jak pro české, tak pro zahraniční kontexty. Zahraniční zařízení však vykazují nižší podíl respondentů, kteří uvedli, že nevědí, kdo je za tato rozhodnutí odpovědný. To naznačuje, že zahraniční nemocnice mohou mít jasněji definované a komunikované procedury pro práci s chráněnými osobami, což přispívá k lepší organizaci a menší nejistotě mezi zaměstnanci.

Lze říci, že zahraniční zařízení vykazují větší zapojení vyššího managementu do rozhodovacích procesů ohledně návštěv, zatímco česká zařízení spoléhají více na roli ošetřujících lékařů. Obě prostředí se však shodují na relativně menší roli ochranky v těchto otázkách.

Graf 2.7: Opatření pro zajištění fyzické bezpečnosti personálu; Zdroj: autor (2024)

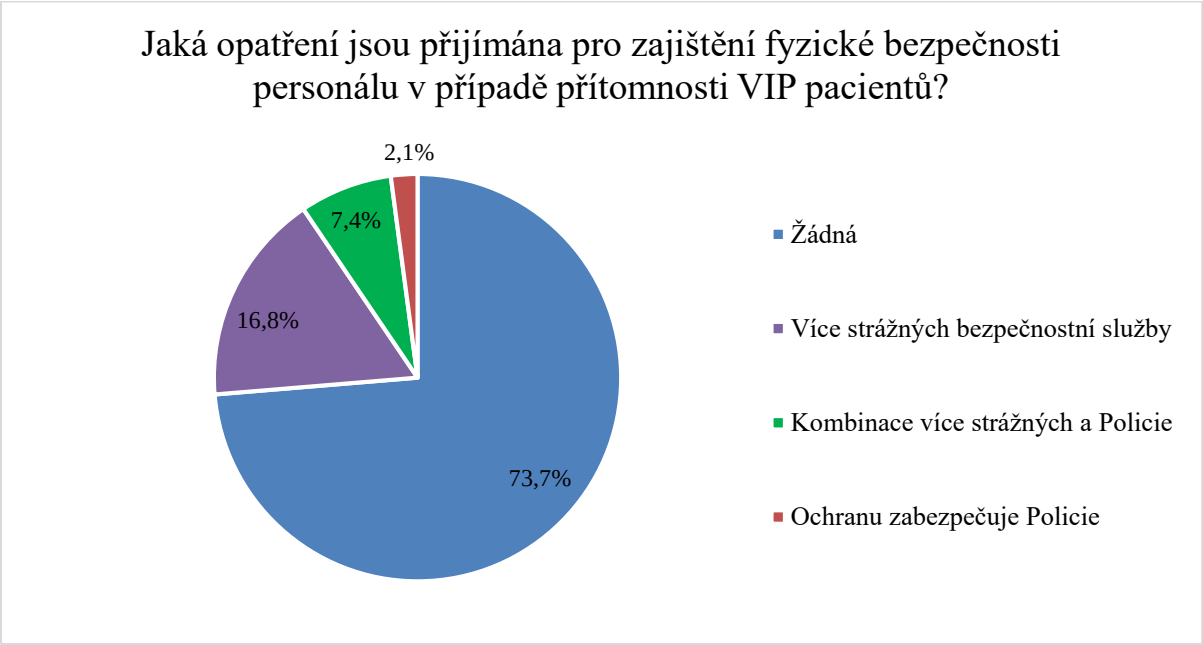


Výsledky této otázky naznačují, že většina zdravotnických zařízení neprovádí žádná specifická opatření k zajištění fyzické bezpečnosti personálu v přítomnosti chráněných osob, což může být dáno jak nedostatkem pokynů, tak i zdrojů na zavedení těchto opatření. Absence jasně stanovených bezpečnostních opatření v 57,9 % případů může rovněž naznačovat, že přítomnost chráněných osob není vnímána jako přímé bezpečnostní riziko, nebo že se zařízení při ochraně spíše spoléhají na běžná bezpečnostní opatření.

Druhá skupina respondentů se zmiňuje o spoléhání se na kombinaci více strážných a policie, což ukazuje na přípravu některých zdravotnických zařízení na zajištění vyšší úrovně bezpečnosti v případě potřeby. Další respondenti zmínili využívání bezpečnostních služeb nebo spolupráci s policií, což odhaluje různorodé přístupy k ochraně personálu. Tento rozmanitý přístup k zajištění bezpečnosti může být ovlivněn specifickými podmínkami, zdroji a prioritami jednotlivých zařízení.

Výsledky naznačují potřebu standardizovaných postupů, které by zajistily jednotný a efektivní přístup k ochraně zdravotnického personálu při přítomnosti chráněných osob. Implementace jasných pokynů by mohla přispět ke zlepšení bezpečnostních opatření, a tím zajistit lepší ochranu jak zdravotnického personálu, tak pacientů.

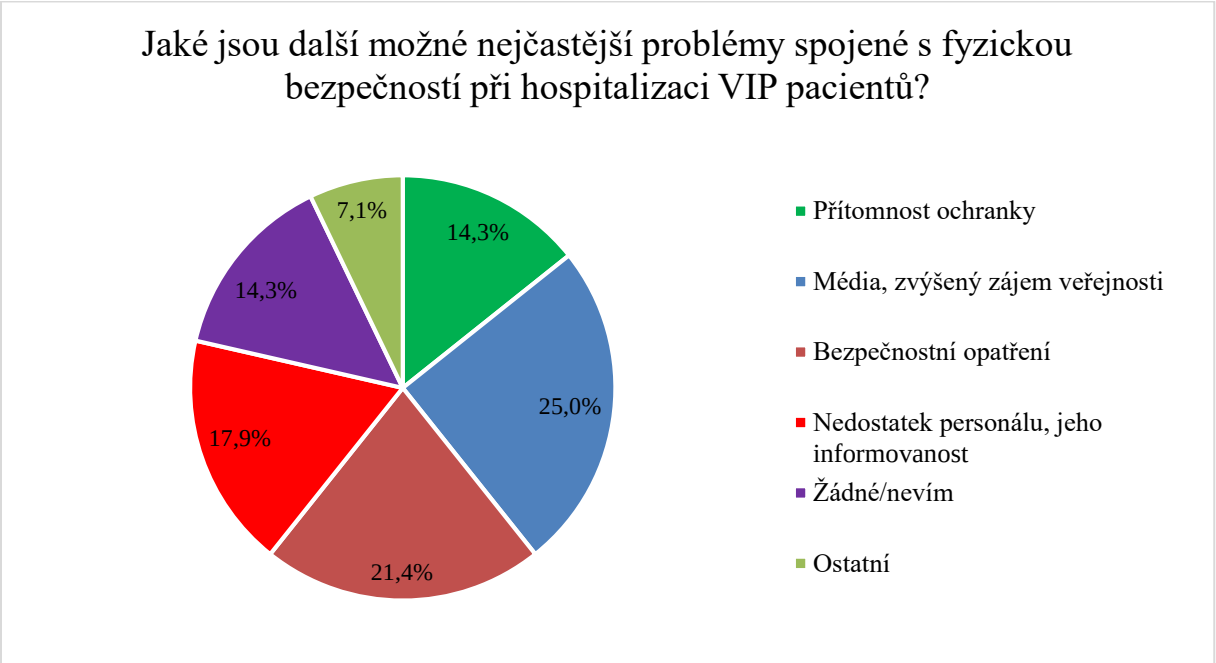
Graf 2.7a: Opatření pro zajištění fyzické bezpečnosti zahraničního personálu; Zdroj: autor (2024)



Zahraniční data ukazují, že ve většině zahraničních zdravotnických zařízení nejsou přijímána specifická opatření pro zajištění fyzické bezpečnosti personálu při přítomnosti chráněných osob. Tato situace naznačuje, že buď zahraniční zařízení nevnímají přítomnost chráněných osob jako rizikový faktor, nebo nemají dostatečné zdroje či zavedené protokoly, které by taková opatření umožnily. Menší část zahraničních zařízení se rozhoduje pro zvýšení počtu strážných nebo spoléhá na kombinaci bezpečnostního personálu a policie, případně armády, což je spíše výjimečný přístup.

V českém kontextu je situace obdobná, většina zdravotnických zařízení rovněž nepřijímá specifická opatření pro ochranu personálu v přítomnosti chráněných osob. Oproti zahraničním zařízením je však patrná mírně větší ochota českých nemocnic implementovat určité bezpečnostní kroky, což může být způsobeno rozdílnou organizační kulturou, vnímáním rizik nebo dostupností zdrojů. Tento rozdíl poukazuje na odlišnosti v přístupech k bezpečnosti mezi českými a zahraničními zařízeními, přičemž obě skupiny zdravotnických zařízení mají prostor pro zlepšení standardizace bezpečnostních opatření.

Graf 2.8: Problémy spojené s fyzickou bezpečností při hospitalizaci chráněných osob; Zdroj: autor (2024)



Výsledky této volitelné otázky odhalily několik klíčových problémů spojených s fyzickou bezpečností při hospitalizaci chráněných osob, jak uvádí 28 respondentů. Nejběžněji zmiňovaným problémem byla přítomnost médií a zvýšený zájem veřejnosti, což ukazuje na to, že veřejná pozornost může negativně ovlivnit provoz a bezpečnostní opatření zdravotnických zařízení. Tento zájem může narušit běžný chod nemocnice a zkomplikovat ochranu soukromí chráněných osob.

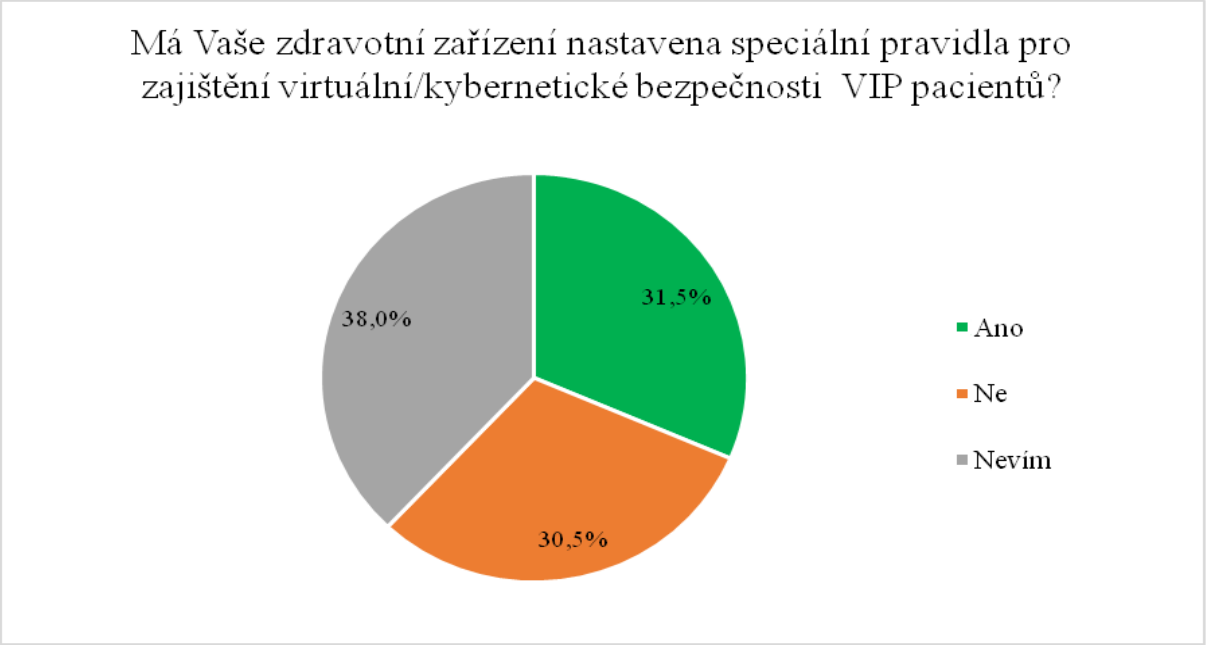
Dalším významným problémem jsou samotná bezpečnostní opatření, která mohou být nedostatečně efektivní nebo správně aplikována, což poukazuje na potřebu lepší implementace a aktualizace stávajících pravidel. Respondenti také upozorňovali na nedostatek personálu a jeho nedostatečnou informovanost, což ukazuje na potřebu lepšího školení personálu ohledně specifik práce s chráněnými osobami.

Přítomnost ochranky a smíšené názory ohledně její efektivity byly zmíněny zhruba stejným počtem respondentů, což může naznačovat, že někteří zdravotníci pochybují o skutečné potřebě a přínosu bezpečnostních složek v těchto případech. Zbývající procenta zahrnovala další problémy, které byly zmíněny pouze okrajově, což naznačuje, že jde spíše o specifické problémy, které nejsou univerzálně vnímány jako hlavní.

Tato zjištění zdůrazňují potřebu zlepšení a standardizace bezpečnostních opatření, která budou efektivně komunikována zdravotnickému personálu a přizpůsobena specifickým potřebám hospitalizace chráněných osob, včetně důrazu na kontrolu vlivu médií a veřejného zájmu.

- **Sekce 3: Virtuální/kybernetická bezpečnost chráněných osob**

Graf 3.1: Pravidla pro zajištění virtuální/kybernetické bezpečnosti chráněných osob; Zdroj: autor (2024)



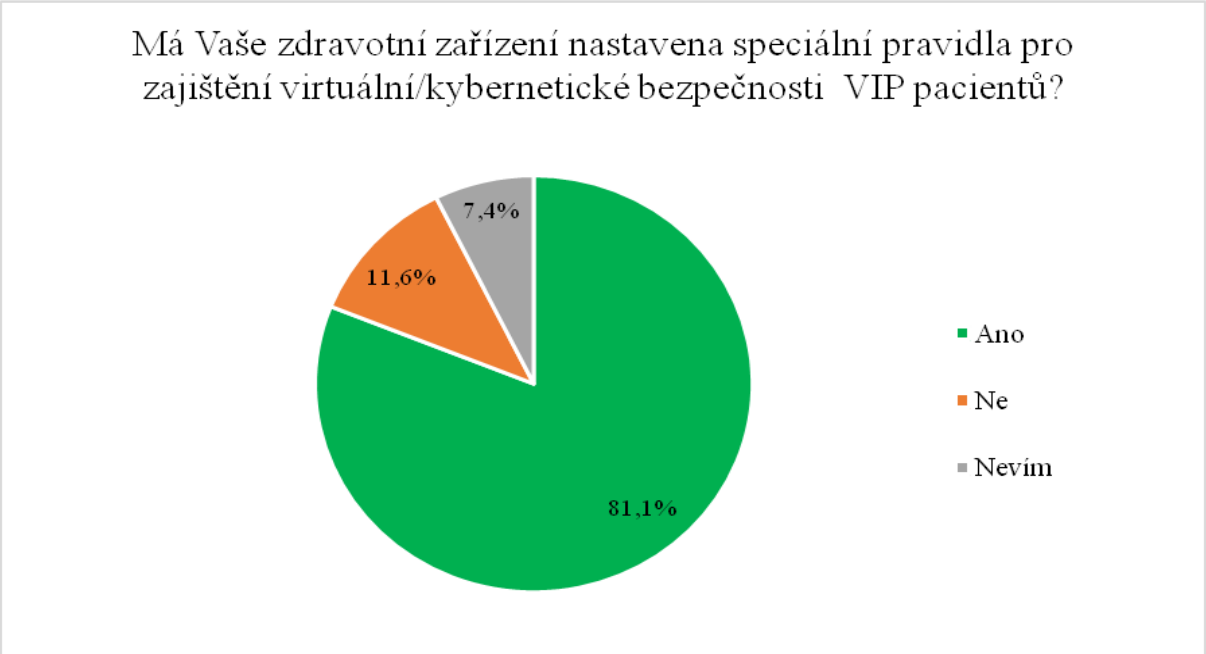
Výsledky této otázky naznačují, že většina respondentů nemá jasnou představu o tom, zda jejich zdravotní zařízení má nastavena speciální pravidla pro zajištění virtuální nebo kybernetické bezpečnosti chráněných osob. Největší skupina respondentů si není jistá, což odhaluje možný nedostatek komunikace nebo informovanosti o těchto zásadních bezpečnostních opatřeních. Tento nedostatek informovanosti může být způsoben tím, že pravidla buď nejsou dostatečně komunikována směrem k personálu, nebo že nejsou plně formalizována.

Část respondentů, která potvrdila existenci těchto pravidel, ukazuje na určitou úroveň povědomí a organizace v oblasti kybernetických hrozeb v některých zařízeních. Přestože tito respondenti potvrzují, že jejich zařízení má zavedená pravidla, relativně vysoký podíl těch, kteří o těchto pravidlech nevědí nebo potvrzují jejich absenci, naznačuje potřebu dalšího vývoje v oblasti kybernetické bezpečnosti.

Tyto výsledky zdůrazňují potřebu zlepšení informovanosti a školení zaměstnanců, aby se zajistila dostatečná ochrana citlivých dat. V době, kdy kybernetické útoky představují rostoucí

hrozbu, je důležité, aby zdravotnická zařízení kladla důraz na ochranu dat, zejména u chráněných osob, jejichž citlivé údaje by mohly mít zásadní dopady na jednotlivce i společnost v případě úniku.

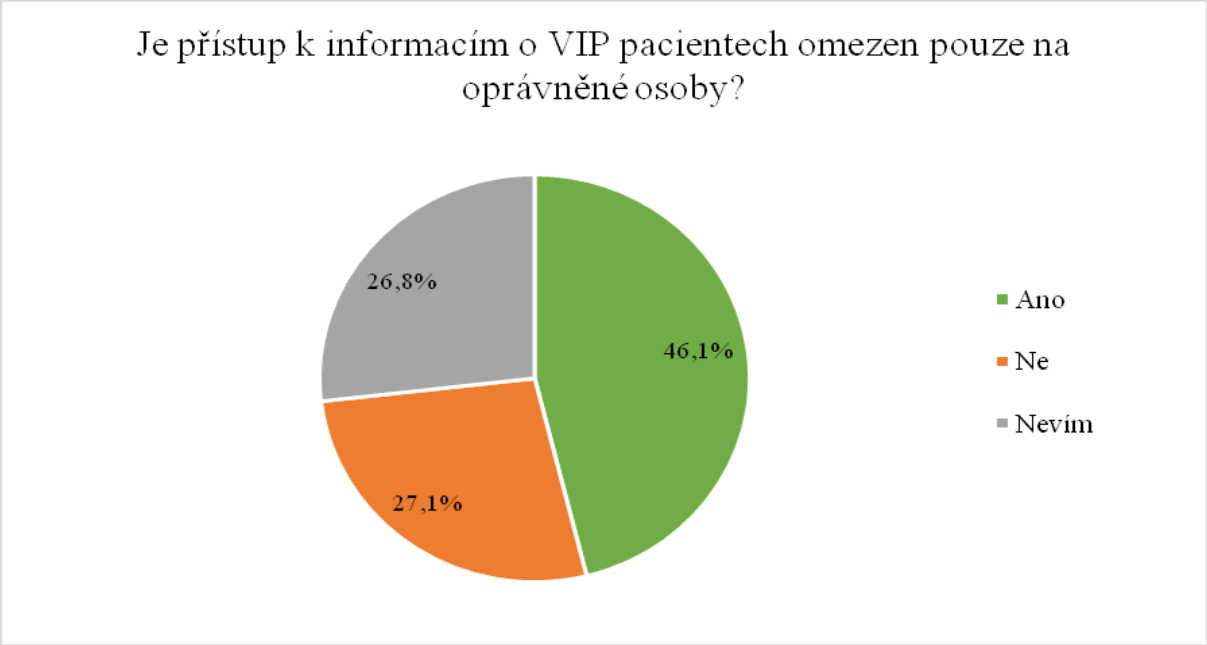
Graf 3.1a: Pravidla pro zajištění virtuální/kybernetické bezpečnosti chráněných osob; Zdroj: autor (2024)



Zahraniční zdravotnická zařízení vykazují výrazně vyšší míru zavedení speciálních pravidel pro zajištění kybernetické bezpečnosti chráněných osob, přičemž většina respondentů uvedla, že taková pravidla mají nastavena. Toto číslo naznačuje, že většina zahraničních zdravotnických zařízení přikládá vysokou důležitost ochraně dat chráněných osob a že tato zařízení pravděpodobně disponují robustními a strukturovanými opatřeními, která mají zajistit bezpečnost citlivých informací. Pouze část respondentů uvedla, že žádná pravidla nastavena nejsou, což je ve výrazném kontrastu k českým datům, kde podobný podíl respondentů odpověděl negativně. Navíc pouze někteří respondenti uvedli, že neví o existenci těchto pravidel, což naznačuje dobrou informovanost zaměstnanců v zahraničních zařízeních.

Porovnání výsledků ukazuje, že zahraniční zdravotnická zařízení mají tendenci přikládat větší význam ochraně dat chráněných osob prostřednictvím speciálních pravidel pro kybernetickou bezpečnost. To může být dáno vyšším povědomím o kybernetických rizicích, lepší dostupností technologií a většími finančními zdroji ve srovnání s českými zařízeními.

Graf 3.2: Omezení přístupu k informacím o chráněných osobách; Zdroj: autor (2024)

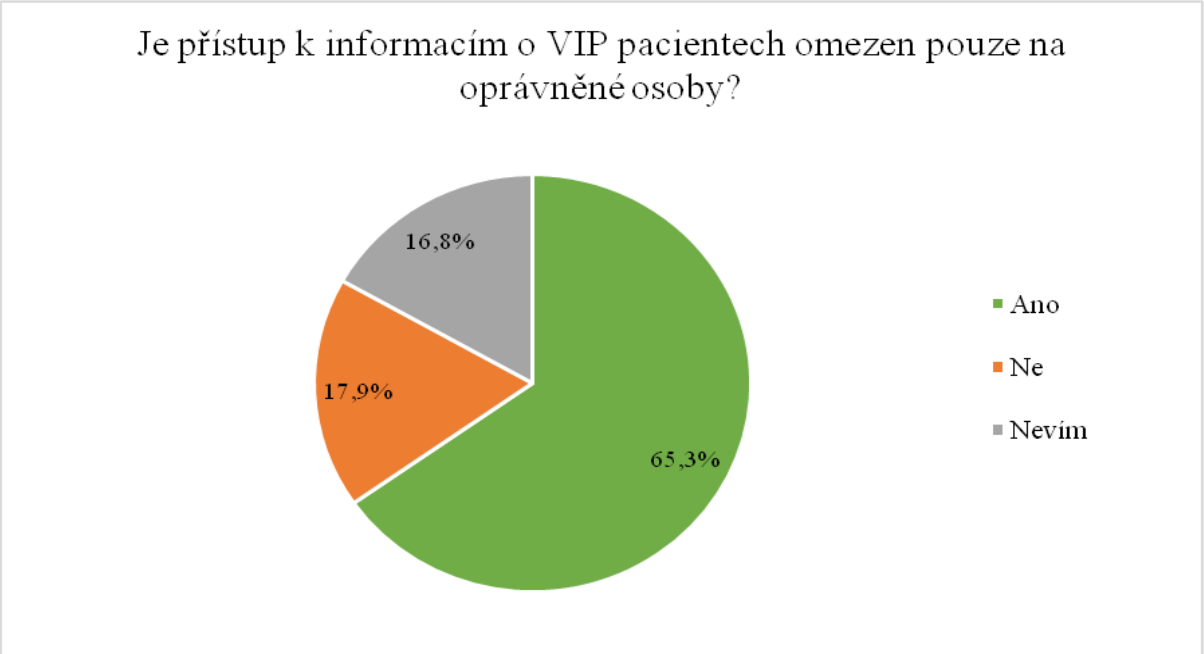


Výsledky této otázky ukazují, že téměř polovina respondentů je si vědoma opatření, která omezují přístup k citlivým informacím o chráněných osobách pouze na oprávněné osoby. Tento nález naznačuje, že v některých zdravotnických zařízeních jsou implementována a zřejmá opatření na ochranu dat, což ukazuje na existenci dobře nastavených bezpečnostních mechanismů.

Na druhou stranu, významná část respondentů uvedla, že přístup k těmto informacím není omezen pouze na oprávněné osoby. To poukazuje na nedostatky v ochraně dat, které mohou být způsobeny buď špatnou implementací bezpečnostních opatření, nebo nedostatečnou komunikací o těchto pravidlech mezi zaměstnanci. Tento nedostatek představuje zvýšené riziko neoprávněného přístupu k citlivým informacím a vyžaduje pozornost, aby byla zajištěna dostatečná úroveň kybernetické bezpečnosti.

Kromě toho se téměř třetina respondentů necítí být dostatečně informována, což naznačuje nedostatek školení nebo přehlednosti o pravidlech, která se týkají ochrany dat v jejich zařízení. Tento nedostatek povědomí může vést k potenciálním bezpečnostním incidentům a podtrhuje potřebu nejen zlepšit technická opatření, ale také zajistit, aby všichni zaměstnanci byli obeznámeni s pravidly a postupy ochrany citlivých údajů.

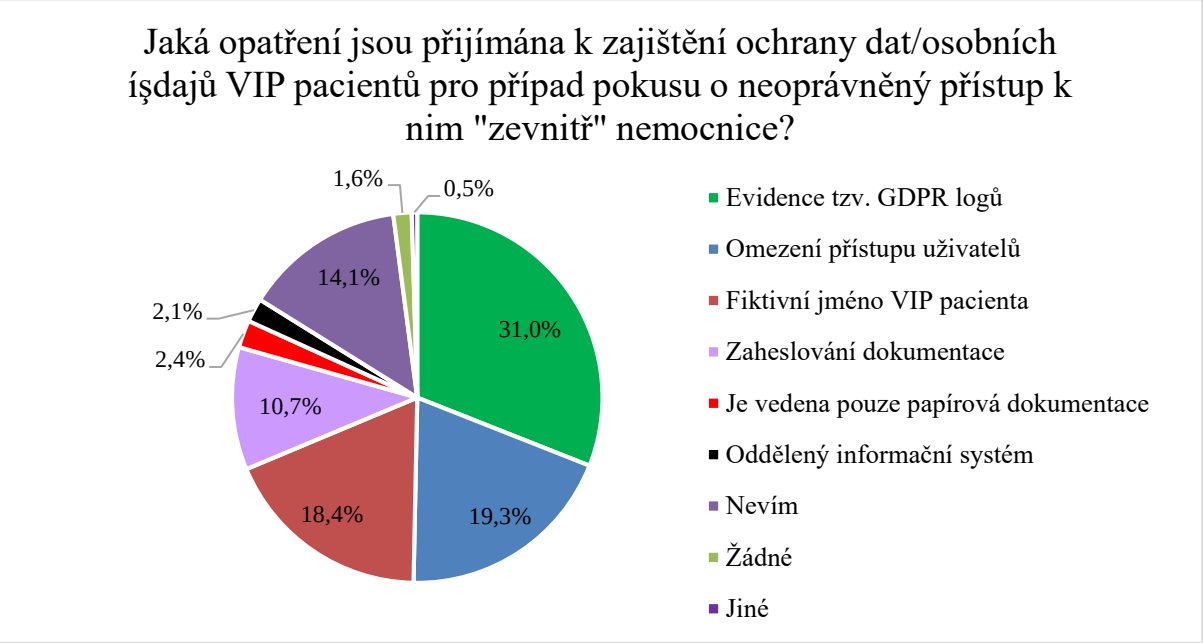
Graf 3.2a: Omezení přístupu k informacím o chráněných osobách v zahraničí; Zdroj: autor (2024)



Zahraniční zdravotnická zařízení obecně vykazují větší míru ochrany citlivých informací o chráněných osobách. Významná část respondentů potvrdila, že přístup k těmto údajům je omezen pouze na oprávněné osoby, což svědčí o zavedení přísnějších pravidel a postupů pro zajištění kybernetické bezpečnosti. Pouze menší část respondentů uvedla, že přístup k těmto informacím není omezen, což naznačuje, že tato zařízení kladou velký důraz na ochranu soukromí a důvěrnosti.

Tento vyšší stupeň omezení přístupu k citlivým datům může být důsledkem lepších technologických systémů, legislativních rámců a vyššího povědomí o rizicích spojených s kybernetickými hrozbami. Na rozdíl od některých českých zařízení, která vykazují nižší míru organizovanosti v této oblasti, zahraniční instituce pravděpodobně zavedly efektivnější a strukturovanější systémy ochrany, čímž minimalizují riziko neoprávněného přístupu k důležitým informacím o chráněných osobách.

Graf 3.3: Vnitřní opatření k zajištění ochrany dat/osobních údajů chráněných osob; Zdroj: autor (2024)



Výsledky této otázky naznačují širokou škálu opatření používaných k ochraně osobních údajů chráněných osob v různých zdravotnických zařízeních. Nejčastější metodou je evidence tzv. GDPR logů, která slouží k monitorování přístupů k datům a jejich ochraně. To svědčí o snaze o větší transparentnost a sledovatelnost přístupů k citlivým informacím.

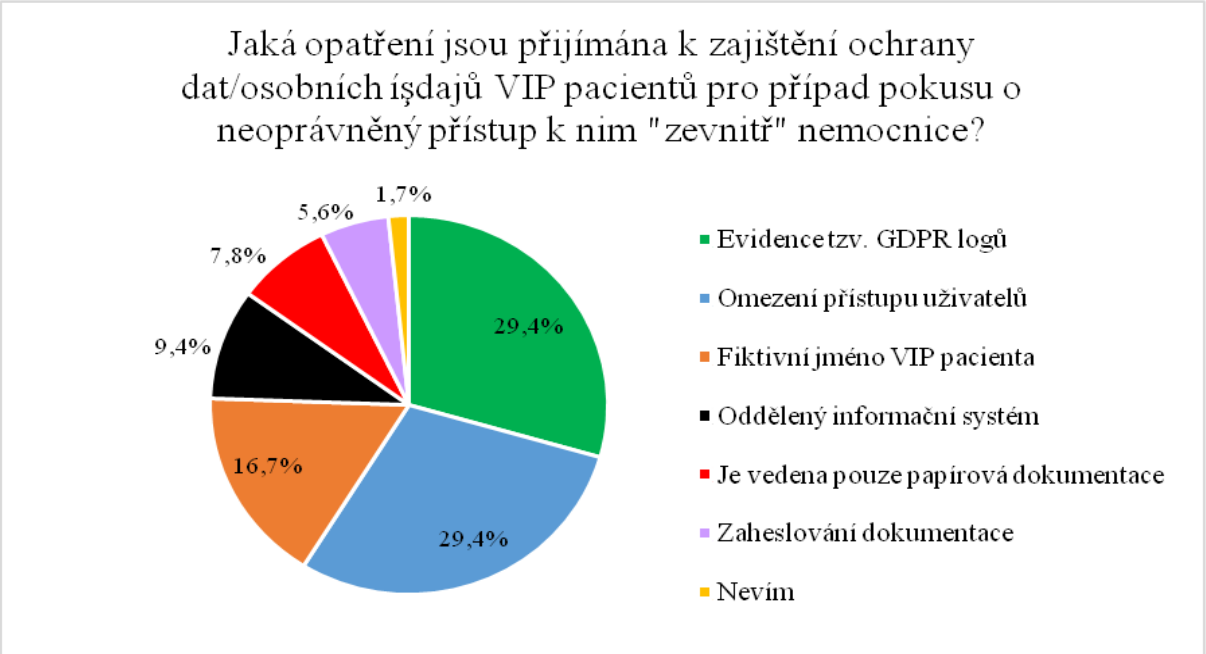
Další častou metodou je omezení přístupu uživatelů, kdy pouze vybraní zaměstnanci mají oprávnění k těmto údajům, což přispívá k lepší kontrole a ochraně dat. Některá zařízení také používají fiktivní jména chráněných osob jako další krok k anonymizaci a skrytí identity, což se jeví jako důležitý preventivní mechanismus.

Zaheslování dokumentace je dalším opatřením zvyšujícím bezpečnost. Přestože se digitální záznamy zdají být pohodlnější, stále existují zařízení, která se spoléhají na papírovou dokumentaci, byť v menší míře.

Relativně nízká informovanost některých zaměstnanců o tom, jaká opatření jsou implementována, poukazuje na potenciální slabinu v oblasti interní komunikace a školení. To představuje příležitost ke zlepšení prostřednictvím zvýšení povědomí o bezpečnostních opatřeních a jasnější definice postupů.

Tyto výsledky ukazují na celkovou snahu o zabezpečení citlivých dat, avšak poukazují také na oblasti, kde by mohla být vylepšena komunikace a povědomí zaměstnanců o zavedených postupech.

Graf 3.3a: Vnitřní opatření k zajištění ochrany dat/osobních údajů chráněných osob v zahraničí; Zdroj: autor (2024)



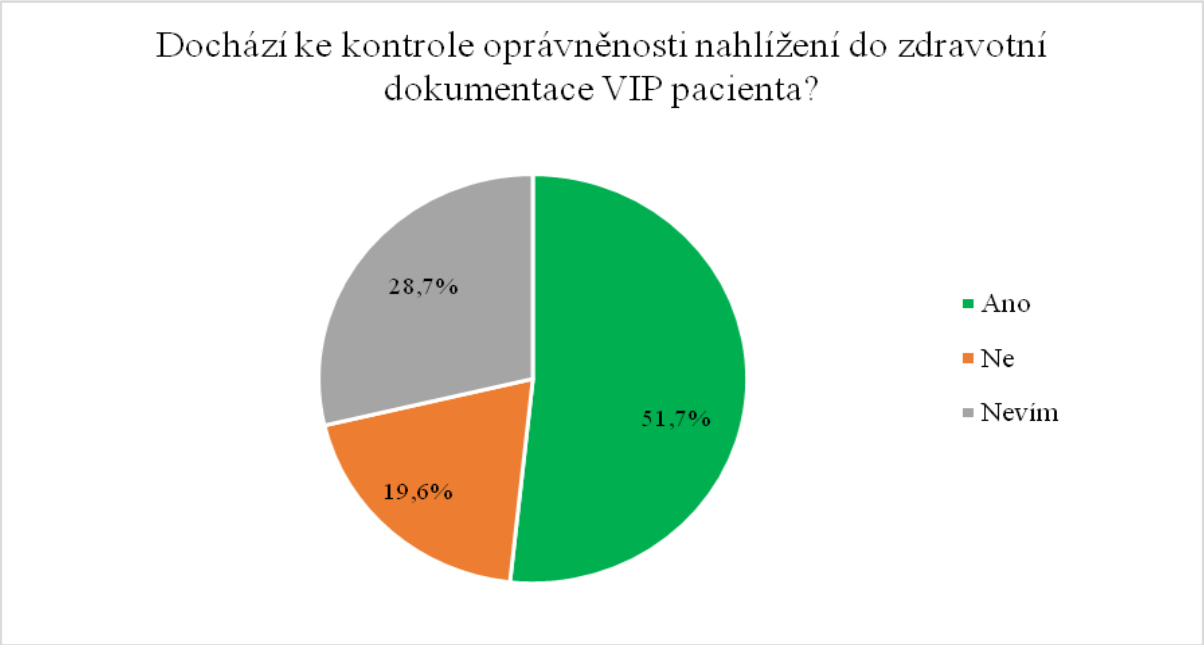
Ve srovnání s českými daty, která ukazují, že značná část zdravotnických zařízení využívá GDPR logy k monitorování přístupů a omezování přístupu uživatelů, zahraniční data vykazují podobný trend. Opatření jako sledování přístupů a omezení přístupu k citlivým informacím jsou rozšířená jak v českých, tak zahraničních zdravotnických zařízeních, což potvrzuje jejich univerzální důležitost při ochraně osobních údajů.

Zajímavé rozdíly se objevují v přístupu k anonymizaci dat, kde zahraniční zařízení méně často používají fiktivní jména pacientů, což může souviset s různými přístupy ke kybernetické bezpečnosti a ochraně soukromí. To by mohlo být způsobeno rozdílnými kulturními nebo systémovými normami mezi jednotlivými zeměmi.

Dalším rozdílem je preference pro papírovou dokumentaci, která je v českých zařízeních méně častá než v zahraničí. Tento rozdíl může být způsoben odlišnými technologickými možnostmi nebo vnímáním rizik spojených s digitálními záznamy. Zahraniční zařízení však více spoléhají na oddělené informační systémy, což ukazuje, že v zahraničí je tato technologie vnímána jako efektivní způsob ochrany dat. Tyto výsledky zdůrazňují různé přístupy ke správě a ochraně

citlivých údajů, přičemž obě skupiny preferují ověřené metody zabezpečení dat, ale každá má své specifické preference a postupy.

Graf 3.4: Kontrola oprávněnosti nahlížení do zdravotní dokumentace chráněných osob; Zdroj: autor (2024)

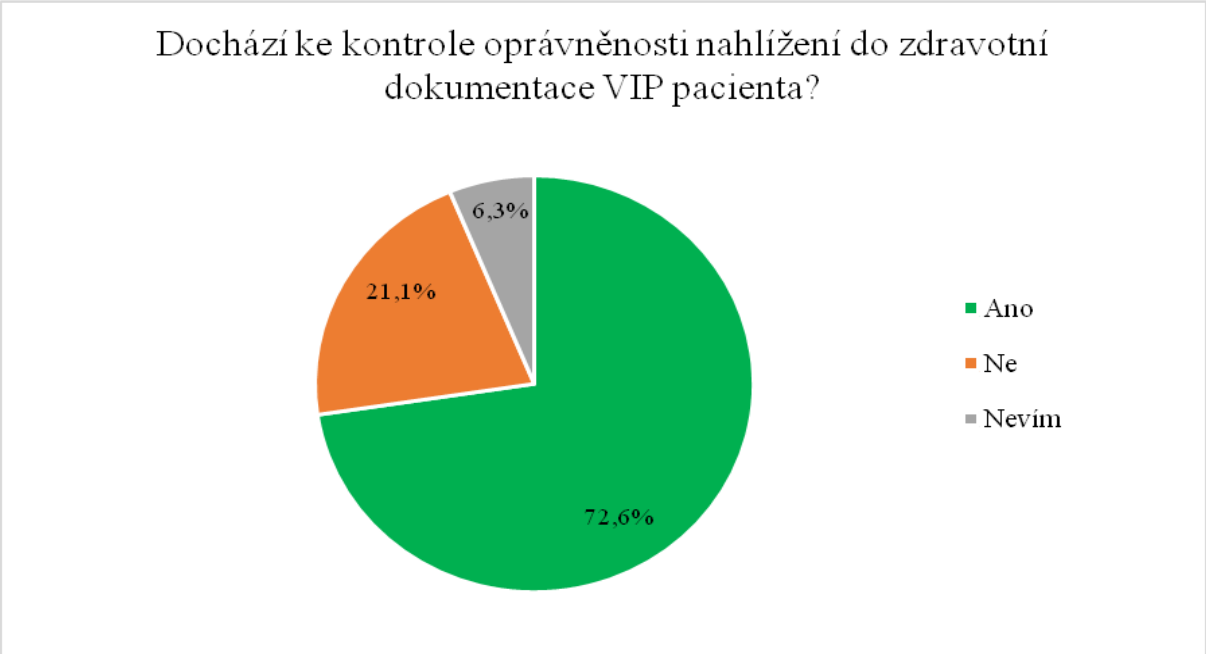


Výsledky této otázky naznačují, že více než polovina zdravotnických zařízení provádí pravidelné kontroly oprávněnosti přístupu k zdravotní dokumentaci chráněných osob, což ukazuje na široké povědomí o důležitosti ochrany citlivých údajů. Tyto kontrolní mechanismy slouží k tomu, aby přístup k dokumentaci měly pouze oprávněné osoby, a přispívají tak k ochraně soukromí pacientů.

Nicméně, téměř třetina respondentů uvedla, že si není jistá, zda takové kontroly v jejich zařízení probíhají. Tento údaj může naznačovat nedostatek komunikace nebo nejasné směrnice, které by zaměstnancům poskytly přesné informace o bezpečnostních postupech. Skutečnost, že přibližně pětina respondentů uvedla, že žádné kontroly nejsou prováděny, představuje potenciální riziko pro ochranu citlivých dat, což může vést k neoprávněnému přístupu nebo úniku informací o zdravotním stavu chráněných osob.

Tato zjištění podtrhují důležitost zlepšení bezpečnostních opatření, včetně školení zaměstnanců, aby byla zajištěna maximální ochrana soukromí pacientů a aby všichni pracovníci měli jasné povědomí o implementovaných pravidlech a kontrolních mechanismech.

Graf 3.4a: Kontrola oprávněnosti nahlížení do zdravotní dokumentace chráněných osob v zahraničí; Zdroj: autor (2024)

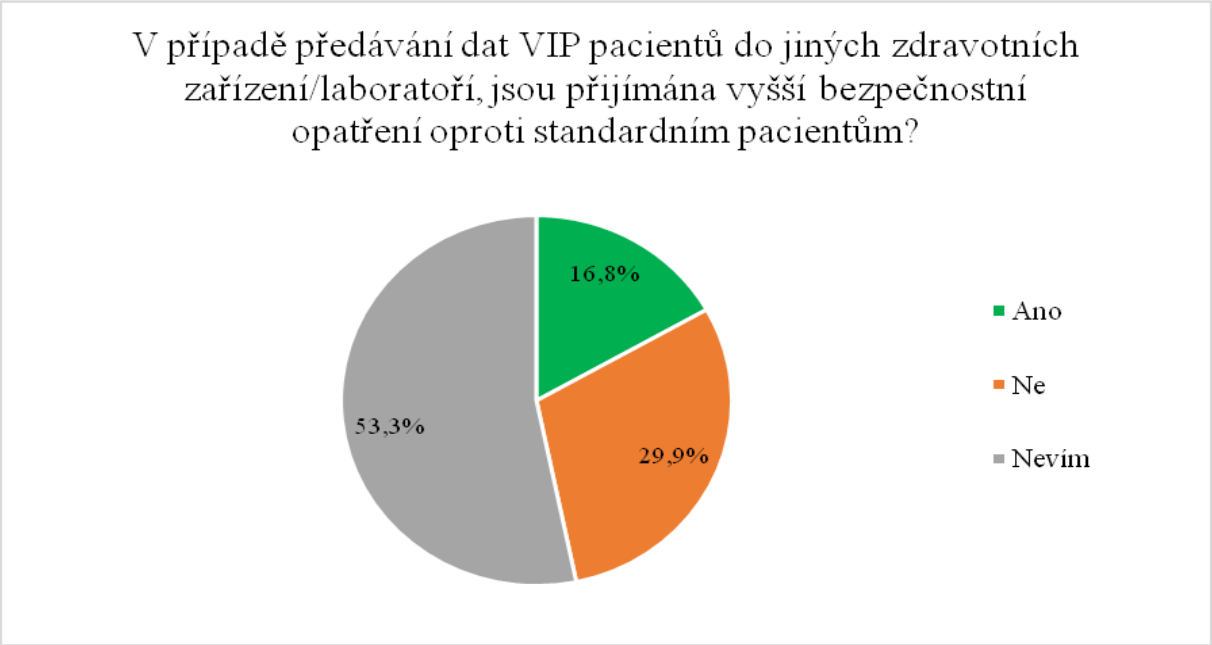


V zahraničních zdravotnických zařízeních je kontrola oprávněnosti přístupu k dokumentaci chráněných osob zavedena ve většině případů, což odráží jejich vysokou úroveň ochrany citlivých dat. Tato zařízení důsledně aplikují kontrolní mechanismy, které zajišťují, že pouze oprávněné osoby mají přístup k těmto informacím. To ukazuje na systematický a efektivní přístup k ochraně dat, který podporuje bezpečnostní protokoly a minimalizuje riziko neoprávněného přístupu.

Nicméně přestože většina zařízení má zavedené postupy, stále existuje určité procento zařízení, kde kontroly neprobíhají, což může zvyšovat riziko potenciálních úniků dat. Tato zranitelnost ukazuje na prostor pro zlepšení v oblasti implementace kontrolních mechanismů a školení personálu. Důraz na ochranu dat je v zahraničí větší ve srovnání s českými zdravotnickými zařízeními, kde kontrola probíhá v menší míře. Rozdíly mezi jednotlivými zařízeními a zeměmi mohou odrážet různé investice do technologií a bezpečnostních opatření, což má vliv na úroveň ochrany citlivých informací.

Zahraniční zařízení se jeví jako více zaměřená na prevenci a ochranu dat, což přispívá k budování důvěry mezi pacienty a zdravotnickými pracovníky.

Graf 3.5: Komparace bezpečnostních opatření při sdílení dat oproti standardním pacientům; Zdroj: autor (2024)

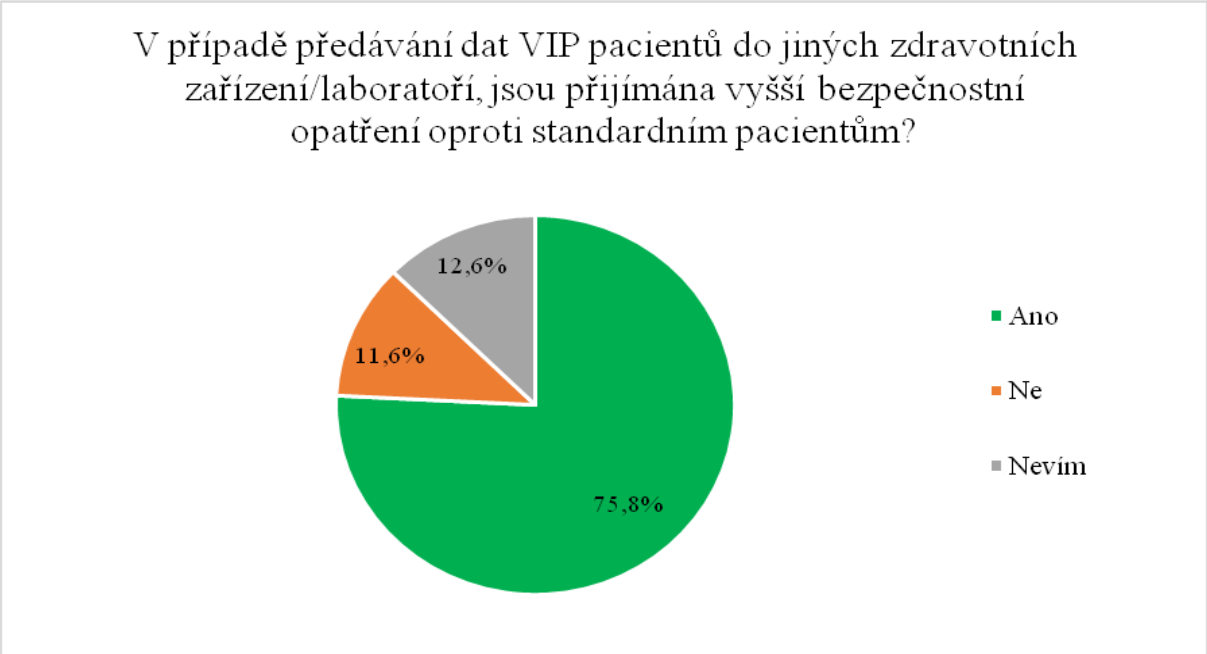


Výsledky této otázky odhalují, že zavádění vyšších bezpečnostních opatření při předávání dat chráněných osob mezi různými zdravotnickými zařízeními nebo laboratořemi není zcela běžnou praxí. Pouze malý podíl respondentů potvrdil, že jejich zařízení taková opatření implementuje, zatímco větší část uvedla, že žádná opatření nejsou přijímána. Navíc více než polovina respondentů si nebyla jistá, zda k zavádění bezpečnostních opatření dochází.

Tato nejistota naznačuje nedostatek jasné komunikace nebo zavedených pravidel o tom, jak jsou citlivá data chráněna při jejich přenosu mezi různými zařízeními. Absence nebo nedostatečná povědomost o takových opatřeních může představovat riziko pro ochranu soukromí a bezpečnosti dat chráněných osob, což je zvláště důležité v kontextu stále rostoucích kybernetických hrozeb.

Je zřejmé, že mnoho zdravotnických zařízení by mohlo získat benefity ze zavedení přísnějších bezpečnostních protokolů a zlepšení informovanosti zaměstnanců o postupech spojených s ochranou dat při jejich přenosu.

Graf 3.5a: Komparace zahraničních bezpečnostních opatření při sdílení dat oproti standardním pacientům; Zdroj: autor (2024)

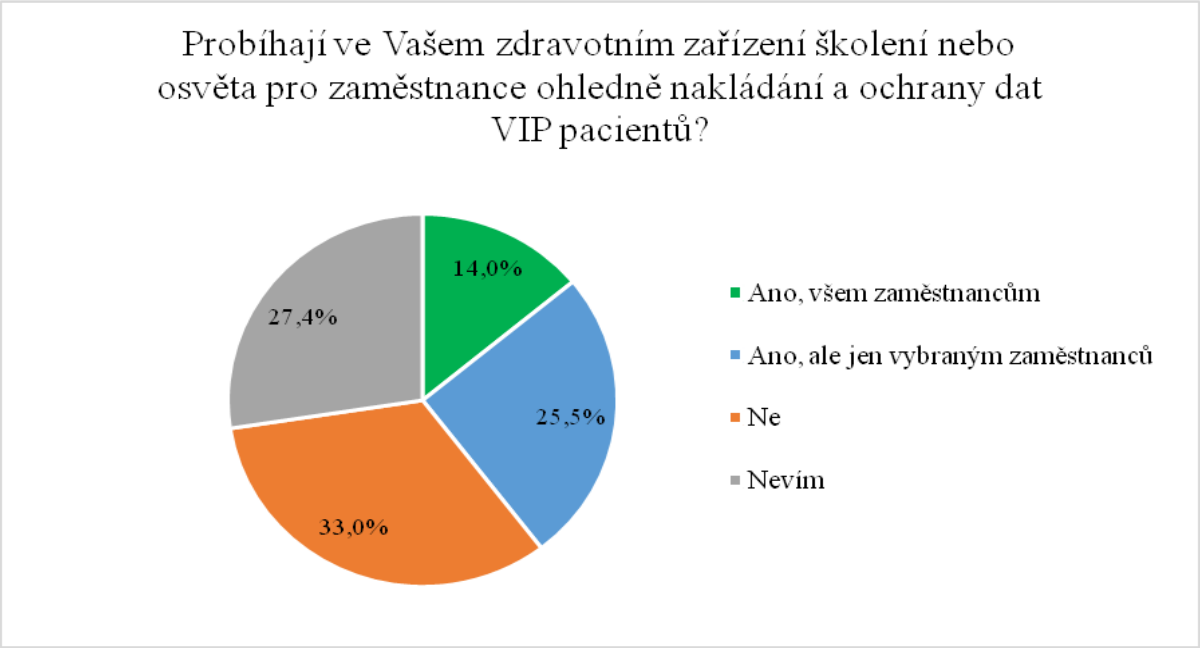


Výsledky ze zahraničních zdravotnických zařízení ukazují, že většina z nich přijímá přísnější bezpečnostní opatření při předávání dat chráněných osob mezi zařízeními, což je výrazně častější praxe než v domácích zdravotnických zařízeních. Tento rozdíl může naznačovat vyšší úroveň regulace nebo technologické zázemí v zahraničí, které umožňuje lepší ochranu citlivých údajů během přenosu.

Zatímco většina zahraničních respondentů potvrzuje zavedení přísných opatření, domácí data ukazují, že velká část respondentů si není jistá, zda jejich zařízení tato opatření zavádějí, nebo tato opatření chybí. To naznačuje potřebu lepší komunikace a školení v oblasti ochrany dat v domácích zdravotnických zařízeních, aby zaměstnanci jasně rozuměli zavedeným bezpečnostním protokolům a byli schopni efektivně chránit citlivé údaje, zejména v kontextu rostoucích hrozeb kybernetických útoků.

Tento rozdíl podtrhuje potřebu domácích zařízení vyrovnat se mezinárodním standardům v oblasti ochrany dat a kybernetické bezpečnosti. Zavedení lepších technologií, školení a jasnějších pravidel pro zaměstnance by mohlo zvýšit úroveň ochrany citlivých informací a snížit riziko jejich neoprávněného přístupu nebo zneužití.

Graf 3.6: Školení zaměstnanců ohledně nakládání a ochrany dat chráněných osob; Zdroj: autor (2024)

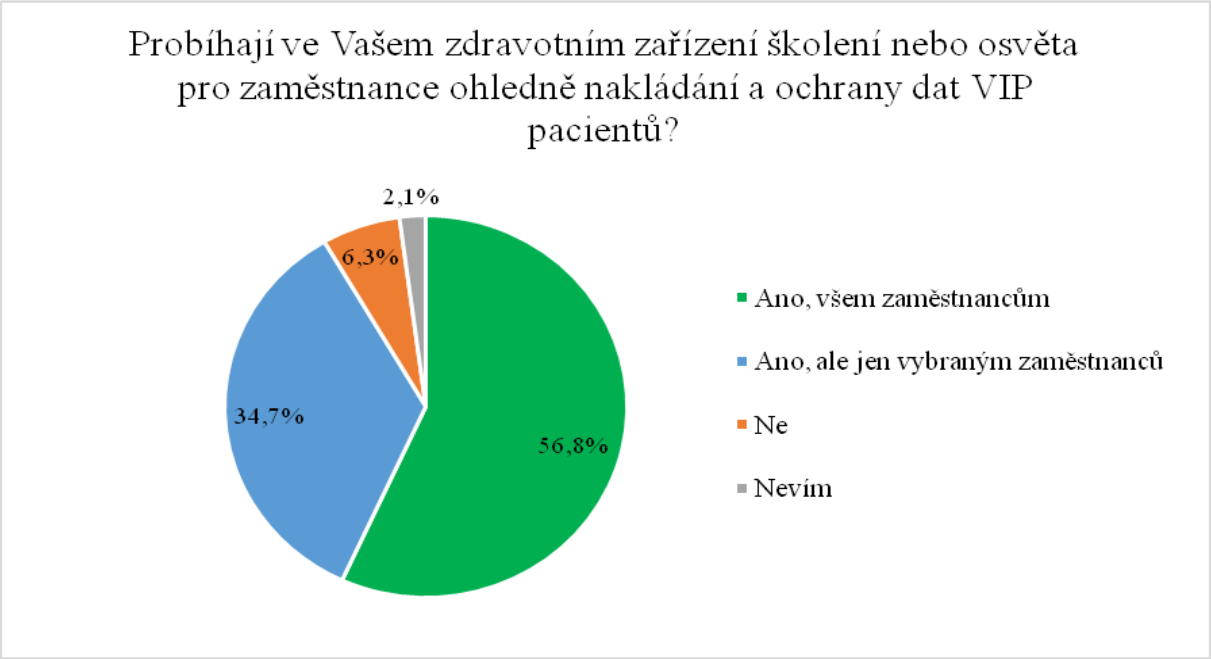


Výsledky této otázky ukazují, že jen menší část zdravotnických zařízení poskytuje školení nebo osvětu o ochraně dat chráněných osob všem svým zaměstnancům. Některá zařízení poskytují tato školení pouze vybraným skupinám zaměstnanců, zatímco v dalších zařízeních tato školení vůbec neprobíhají. Další část respondentů uvedla, že o existenci těchto školení nemá dostatečné informace.

Tento stav naznačuje, že mnoho zdravotnických zařízení nevěnuje dostatečnou pozornost vzdělávání svých zaměstnanců v oblasti ochrany citlivých dat. Přitom školení zaměřená na bezpečnost dat jsou klíčová pro to, aby zdravotnický personál rozuměl rizikům a důsledkům neoprávněného přístupu k citlivým informacím. Systematické školení by zlepšilo připravenost zařízení čelit kybernetickým hrozbám a přispělo k lepšímu zabezpečení údajů chráněných osob.

Je tedy nutné, aby se školení v oblasti ochrany dat stala standardní praxí ve zdravotnických zařízeních a byla dostupná pro všechny zaměstnance, včetně lékařů a zdravotnického personálu, kteří s těmito informacemi pravidelně pracují. Tímto způsobem by se výrazně zvýšila úroveň ochrany dat a zajištění kybernetické bezpečnosti ve zdravotnictví.

Graf 3.6a: Školení zahraničních zaměstnanců ohledně nakládání a ochrany dat chráněných osob; Zdroj: autor (2024)



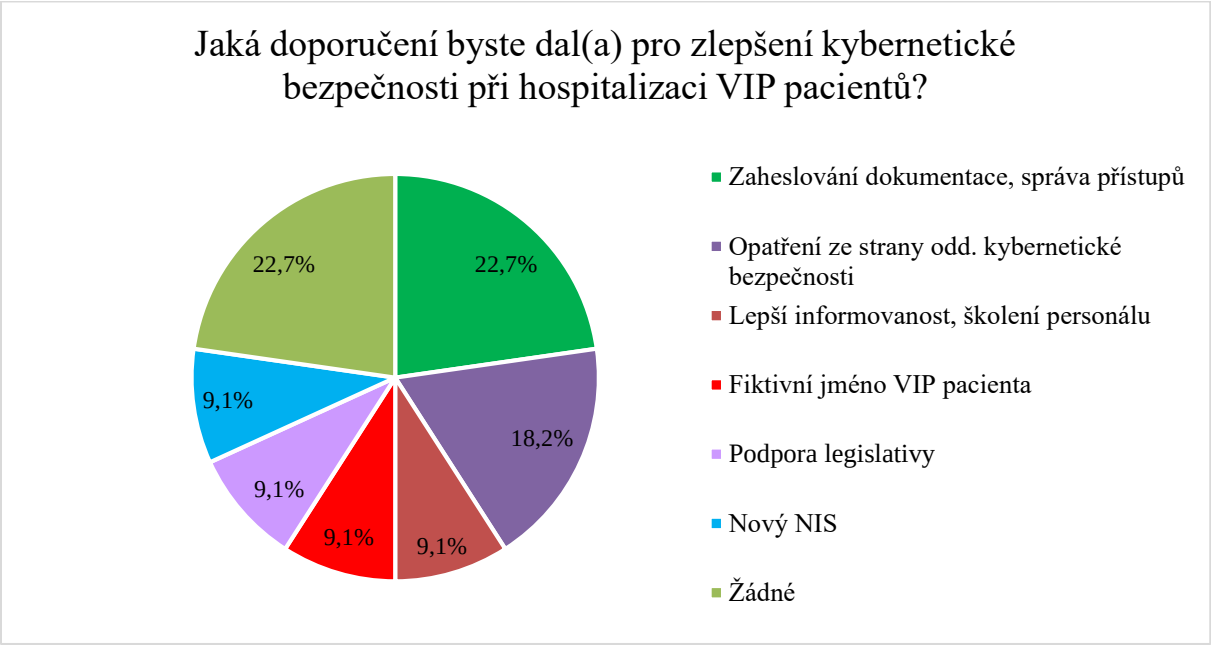
Zahraniční data ukazují, že více než polovina zdravotnických zařízení systematicky školí všechny své zaměstnance v oblasti ochrany dat chráněných osob, což je výrazný rozdíl oproti českým zařízením, kde tato školení probíhají méně často. Zahraniční zařízení tak kladou větší důraz na to, aby se zaměstnanci ve všech úrovních byli obeznámeni s postupy, které zajišťují bezpečnost citlivých informací.

Další skupina zahraničních zařízení poskytuje tato školení pouze vybraným zaměstnancům, což je praxe, kterou sledují i některá česká zařízení. Tímto přístupem se zajišťuje, že klíčoví zaměstnanci, kteří pracují s citlivými daty, jsou dostatečně vyškoleni, i když to nezahrnuje všechny pracovníky.

Zásadní rozdíl mezi zahraničními a českými zařízeními se však projevuje v tom, že jen malé procento zahraničních respondentů uvedlo, že žádná školení neprobíhají, zatímco v Česku je tento podíl výrazně vyšší. To naznačuje, že zahraniční zdravotnické systémy jsou obecně lépe připraveny na problematiku ochrany dat, pravděpodobně v důsledku přísnějších regulačních požadavků a větší investice do vzdělávání.

Tento rozdíl podtrhuje potřebu, aby česká zdravotnická zařízení zlepšila své vzdělávací programy zaměřené na ochranu dat, čímž by se zvýšila celková bezpečnost a snížilo riziko kybernetických hrozeb.

Graf 3.7: Doporučení pro zlepšení kybernetické bezpečnosti při hospitalizaci chráněných osob; Zdroj: autor (2024)



Výsledky této otázky, na kterou odpovědělo 22 respondentů, odhalují několik oblastí, ve kterých respondenti vidí příležitosti pro zlepšení kybernetické bezpečnosti během hospitalizace chráněných osob. Mezi nejčastěji doporučovanými opatřeními bylo zaheslování dokumentace a efektivní správa přístupů. To naznačuje, že zajištění přístupu k citlivým údajům pouze oprávněným osobám by mohlo zásadně přispět ke zvýšení bezpečnosti.

Další návrhy zahrnovaly zlepšení spolupráce s odděleními kybernetické bezpečnosti, což ukazuje na potřebu vybudování specializovaných týmů a zavedení odpovídající infrastruktury pro ochranu dat. Zásadní důraz byl také kladen na vzdělávání a lepší informovanost zdravotnického personálu o bezpečnostních postupech, což potvrzuje důležitost školení a osvěty v oblasti kybernetické bezpečnosti.

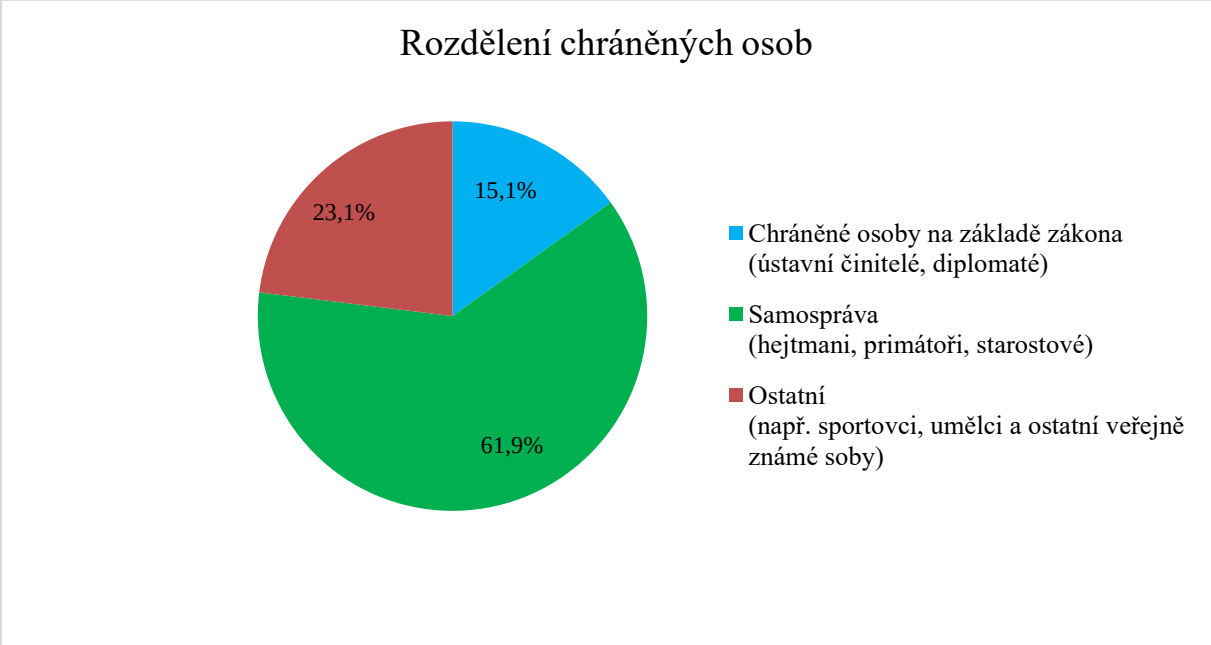
Anonymizace pacientů prostřednictvím použití fiktivních jmen byla dalším zmíněným opatřením, které by mohlo pomoci chránit identitu chráněných osob. Někteří respondenti zdůrazňovali potřebu legislativní podpory a modernizace nemocničních informačních systémů, což by umožnilo lepší zajištění dat a prevenci kybernetických hrozeb.

Tato data ukazují na potřebu komplexního přístupu k ochraně citlivých informací, který by zahrnoval jak technologická řešení, tak vzdělávací aktivity a legislativní podporu.

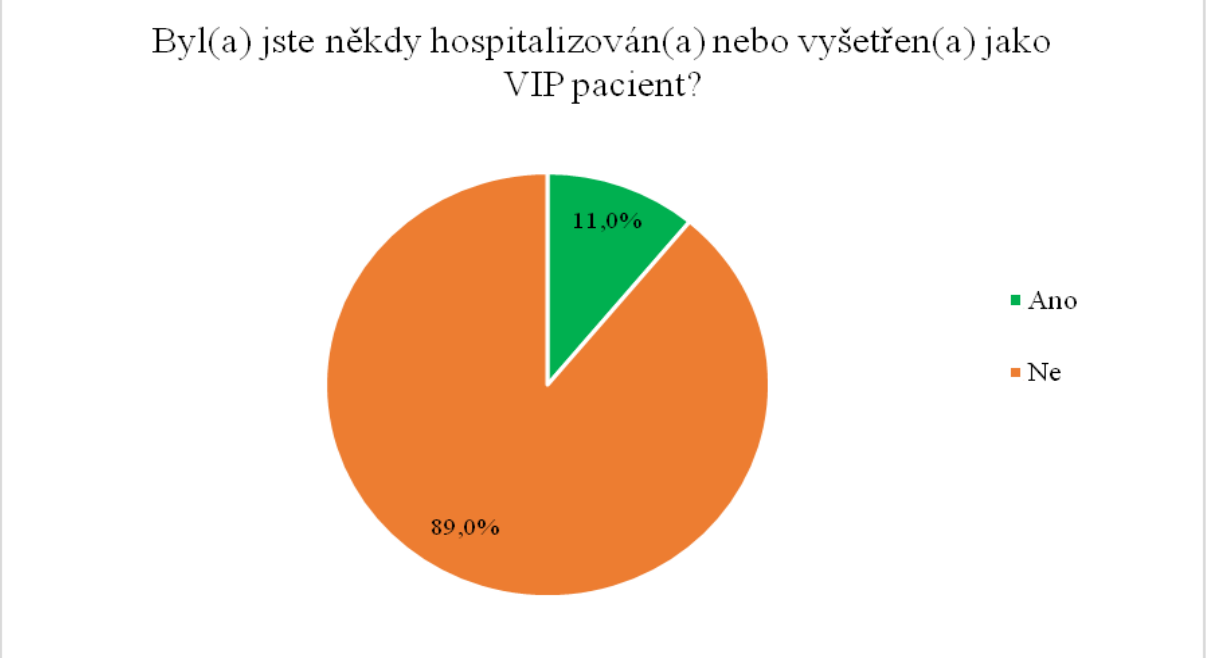
3.6.2 Dotazník pro chráněné osoby

Dotazník pro chráněné osoby vyplnilo celkem 616 respondentů z České republiky (viz kapitola 3.4.2).

Graf 4: Rozdělení chráněných osob; Zdroj: autor (2024)

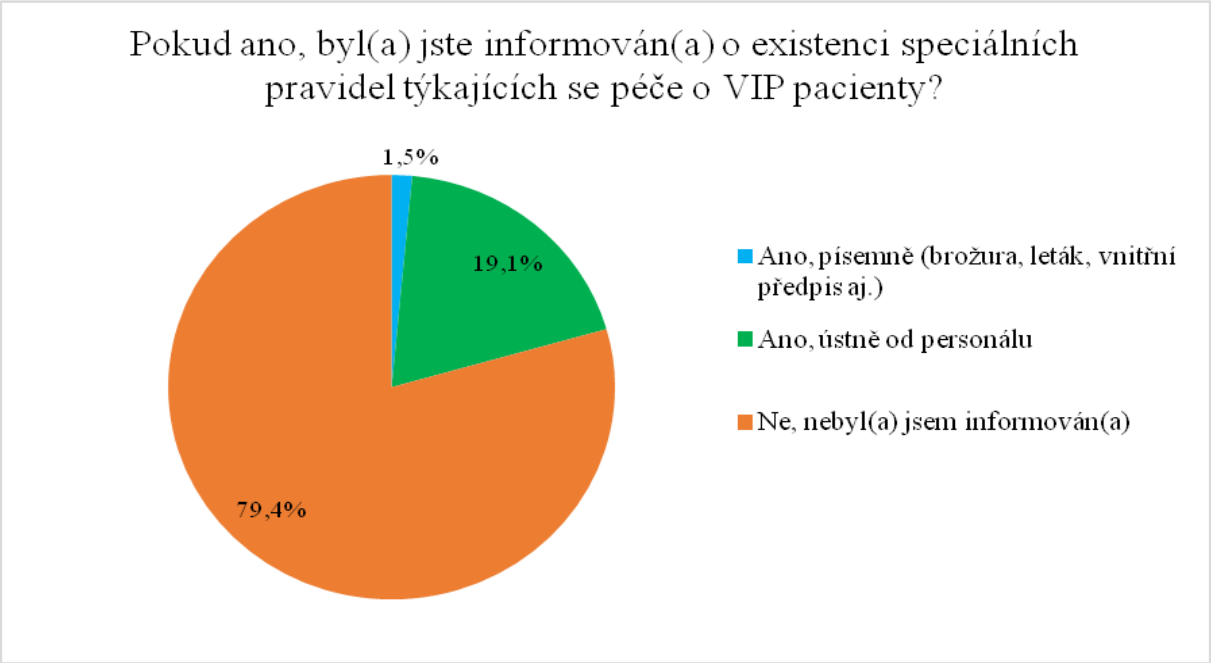


Graf 4.1: Informace o hospitalizaci nebo vyšetření chráněných osob; Zdroj: autor (2024)



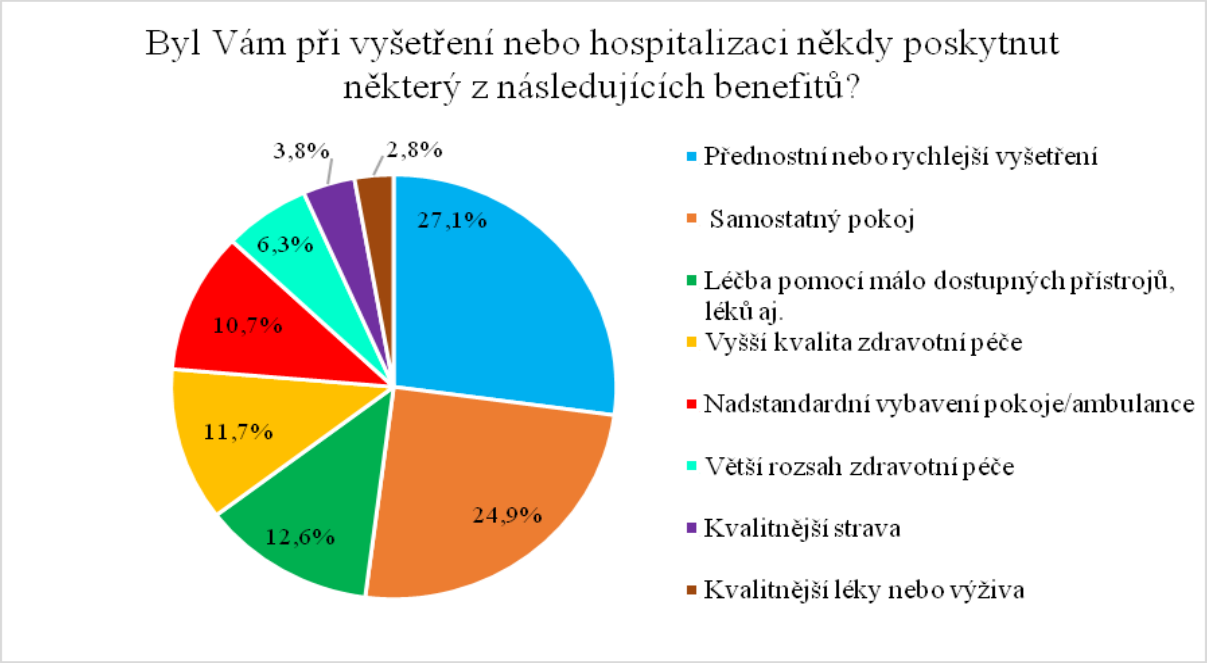
Výsledky této otázky ukazují, že jen menší část respondentů má osobní zkušenost s hospitalizací nebo vyšetřením jako „VIP pacienti“, zatímco většina tuto zkušenost nemá. Tento nízký podíl osob, které byly ošetřeny s „VIP statutem“, může souviset s omezenou dostupností tohoto statutu, který je často vyhrazen specifickým situacím nebo určité skupině lidí. Naproti tomu drtivá většina respondentů nikdy nečerpala výhody plynoucí z „VIP ošetření“, což odráží realitu, kde je pro většinu pacientů poskytována standardní péče bez zvláštních výhod.

Graf 4.2: Informace o existenci speciálních pravidel týkajících se péče o chráněné osoby; Zdroj: autor (2024)



Výsledky této otázky ukazují, že většina chráněných osob nebyla informována o existenci speciálních pravidel týkajících se jejich péče. Pouze malá část respondentů obdržela ústní informace od personálu a jen zanedbatelné množství dostalo písemné informace ve formě brožur nebo jiných dokumentů. Tento výrazný nedostatek informovanosti naznačuje, že zdravotnická zařízení neklade dostatečný důraz na komunikaci pravidel, která by měla být jasně sdělena těmto pacientům. Absence formální informovanosti může vést k nejistotě a nejasnostem ohledně práv a výhod, které chráněné osoby mohou mít. Pro zlepšení péče je klíčové zvýšit úroveň komunikace a zajistit, že jsou chráněné osoby plně obeznámeny s pravidly, která se jich týkají.

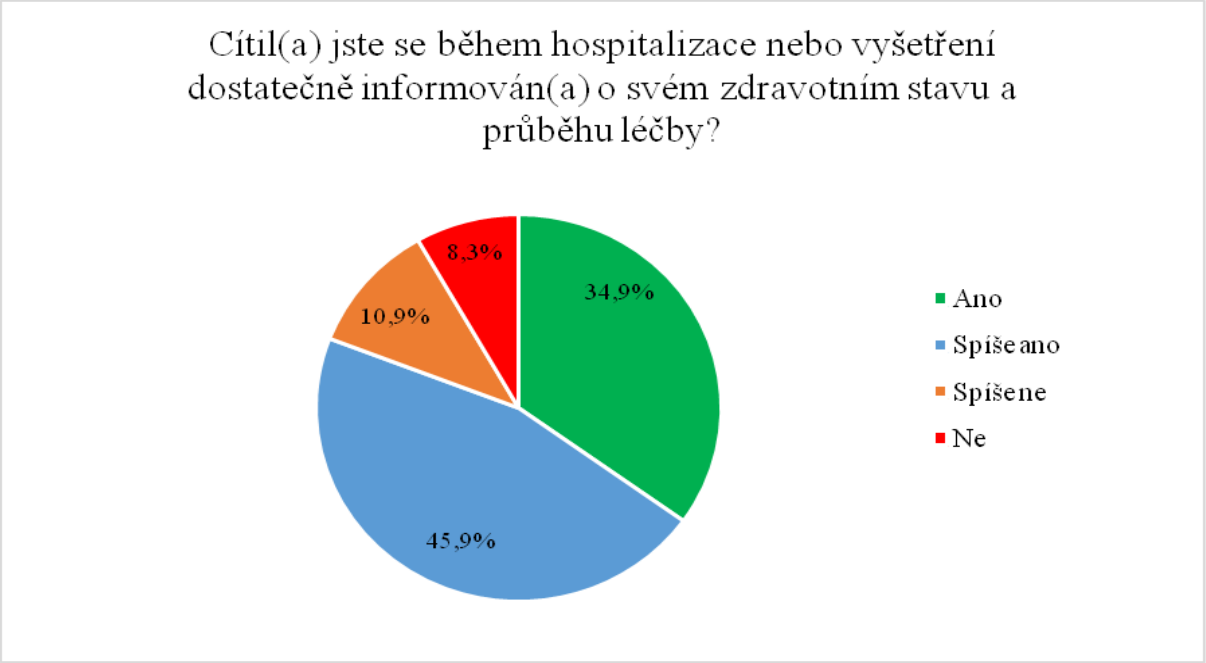
Graf 4.3: Benefity poskytované chráněným osobám; Zdroj: autor (2024)



Výsledky této otázky naznačují, že některé chráněné osoby skutečně zažily zvláštní výhody během svého vyšetření nebo hospitalizace. Nejčastěji zmíněným benefitem bylo přednostní nebo rychlejší vyšetření, což potvrzuje, že chráněné osoby měly urychlený přístup ke zdravotní péči. Další často uváděnou výhodou byl samostatný pokoj, který poskytuje vyšší úroveň soukromí a komfortu během pobytu v nemocnici. Někteří respondenti také zmiňovali přístup k pokročilým medicínským technologiím nebo specializovaným léčebným metodám, což ukazuje na preferenční zacházení z hlediska dostupnosti špičkových zdravotnických zařízení.

Menší, ale stále významný počet respondentů uvedl přístup k nadstandardnímu vybavení a vyšší kvalitě zdravotní péče, což potvrzuje, že chráněné osoby mohou mít lepší podmínky během hospitalizace. Další výhody zahrnovaly lepší stravu, kvalitnější léky či výživu, což naznačuje, že i aspekty související s komfortem a podporou zdraví během hospitalizace byly u chráněných osob upřednostněny. Celkově tato data ukazují, že chráněné osoby měly v některých případech přístup k vyšším standardům zdravotní péče, což potvrzuje existenci preferenčního zacházení pro tuto skupinu pacientů.

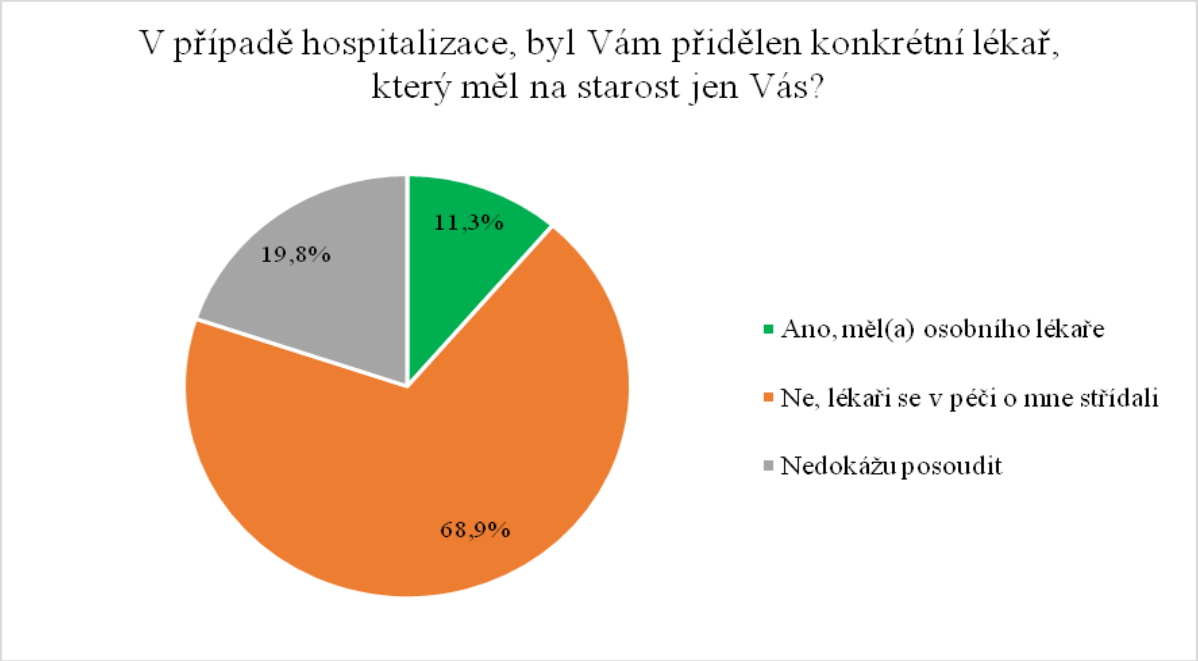
Graf 4.4: Informování chráněných osob; Zdroj: autor (2024)



Výsledky této otázky ukazují, že většina chráněných osob se během hospitalizace nebo vyšetření cítila dostatečně informována o svém zdravotním stavu a průběhu léčby. Významná část respondentů uvedla, že měli jasné a srozumitelné informace o svém zdraví, přičemž téměř všichni uvedli, že byli plně nebo částečně informováni. Tento pozitivní pocit z informovanosti může svědčit o efektivní komunikaci ze strany zdravotnického personálu, který se snažil pacientům poskytnout dostatek detailů o jejich zdravotním stavu a léčbě.

Na druhou stranu menší skupina respondentů vyjádřila, že se necítila dostatečně informována. Tito pacienti zmiňovali nedostatek informací nebo nedostatečnou srozumitelnost sdělovaných údajů. Tento názor menšiny naznačuje, že je stále prostor pro zlepšení, zejména v oblastech jasné a přímé komunikace, která by zajistila, že všechny chráněné osoby rozumí svému zdravotnímu stavu a léčebným postupům, které podstupují.

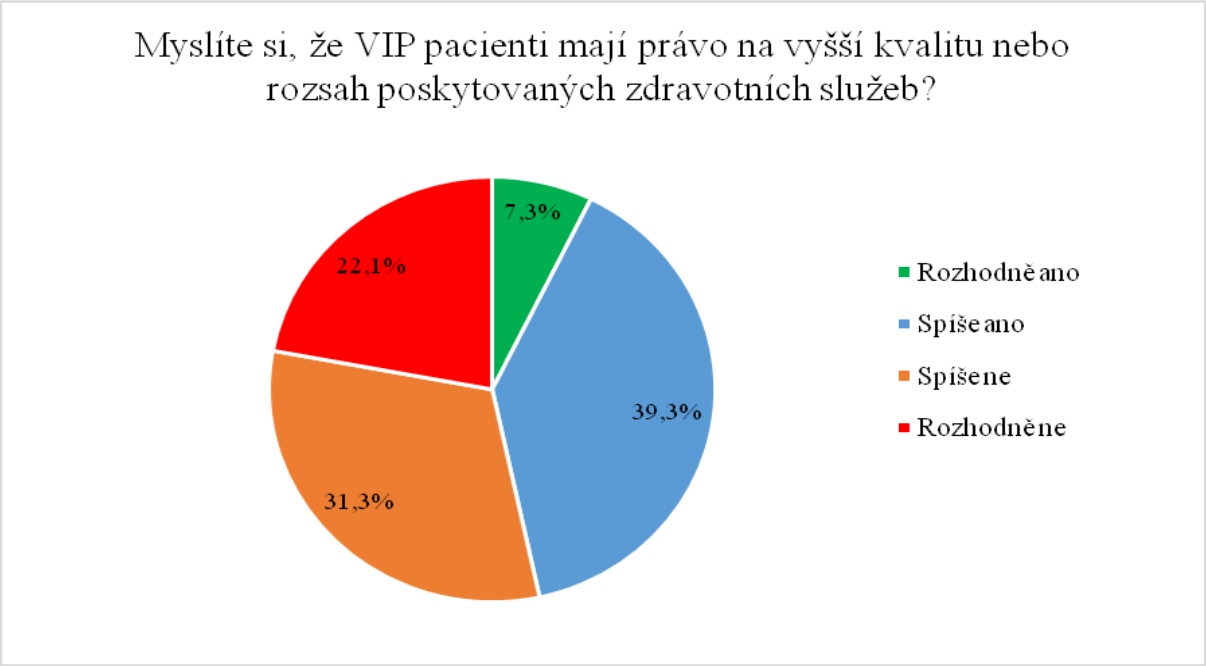
Graf 4.5: Přidělení osobního lékaře chráněným osobám; Zdroj: autor (2024)



Z výsledků vyplývá, že jen malý počet pacientů měl během hospitalizace přiděleného konkrétního lékaře, který se o ně výhradně staral. Většina respondentů uvedla, že o ně pečovalo více lékařů, což může být výsledkem snahy o efektivní využití dostupných zdravotnických kapacit. Nicméně tento přístup může také vytvářet problémy s kontinuitou péče, kdy různí lékaři nemusí mít dostatečný přehled o celkovém průběhu léčby.

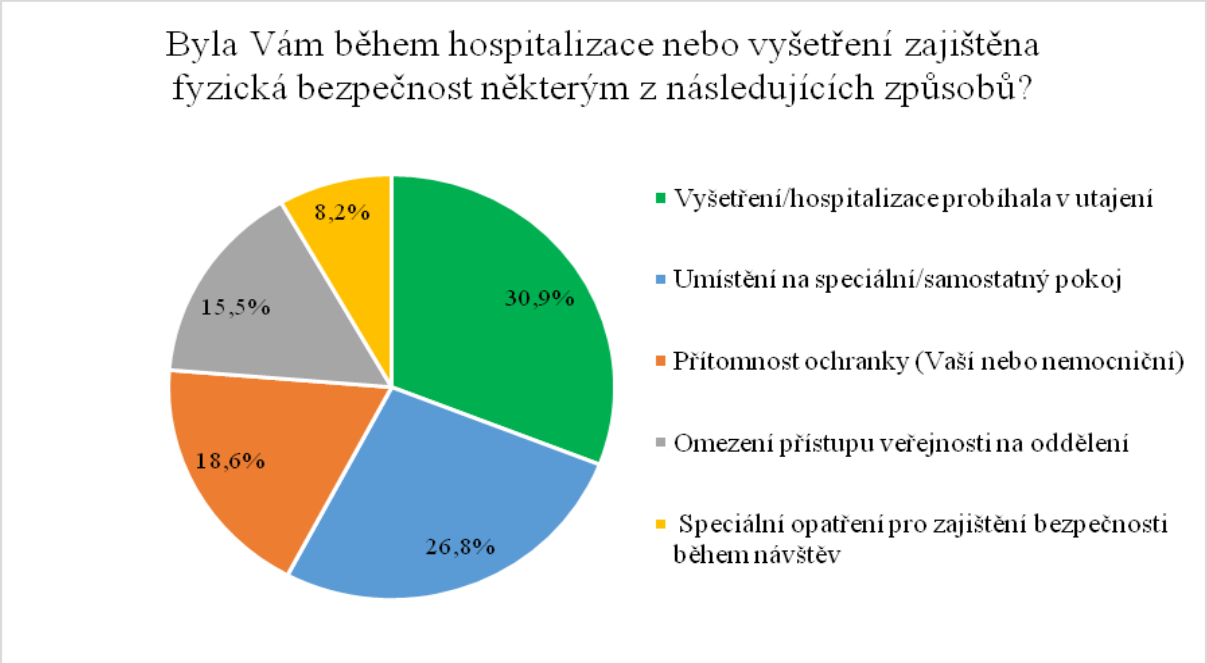
Část respondentů nedokázala určit, zda měli přiděleného konkrétního lékaře, což naznačuje buď nedostatek jasných informací, nebo neadekvátní komunikaci zdravotnického personálu s pacienty. Tento fakt může vést k pocitu nejistoty a nižší spokojenosti s poskytovanou péčí.

Graf 4.6: Vnímání práva na vyšší rozsah nebo kvalitu zdravotní péče ze strany chráněných osob; Zdroj: autor (2024)



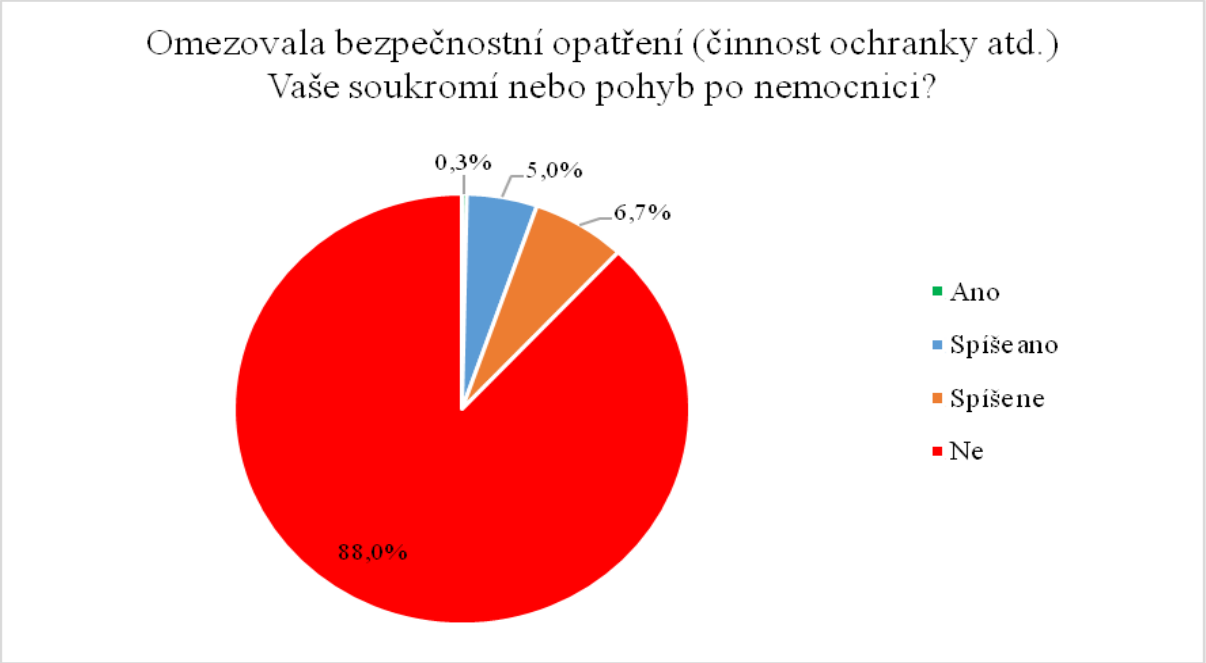
Názory respondentů na otázku, zda by „VIP pacienti“ měli mít nárok na vyšší kvalitu nebo rozsah zdravotní péče, jsou značně rozdělené. Přibližně polovina respondentů se domnívá, že „VIP pacienti“ by měli mít právo na lepší péči, což může odrážet vnímání, že osoby s vyšším postavením nebo specifickými potřebami mohou vyžadovat určité výhody či rychlejší přístup ke zdravotním službám. Na druhou stranu, zhruba stejný počet respondentů nesouhlasí s preferenčním zacházením pro „VIP pacienty“, což vyjadřuje přesvědčení, že zdravotní péče by měla být poskytována rovnoměrně pro všechny, bez ohledu na sociální či ekonomický status. Tento názor zdůrazňuje snahu o zajištění spravedlnosti a rovnosti v přístupu ke zdravotním službám. Data ukazují na výraznou polarizaci ve vnímání této problematiky mezi zdravotnickým personálem i veřejností.

Graf 4.7: Bezpečnost při hospitalizaci nebo vyšetření chráněných osob; Zdroj: autor (2024)



Výsledky otázky ukázaly, že zdravotnická zařízení používají různé způsoby pro zajištění bezpečnosti chráněných osob. Nejčastější metodou bylo vedení hospitalizace nebo vyšetření v utajení, což zdůrazňuje důležitost diskrétnosti v ochraně chráněných osob. Další běžnou praxí bylo umístění pacientů na speciální či samostatné pokoje, což poskytuje jak soukromí, tak lepší kontrolu nad přístupem k pacientům. V některých případech byla přítomna osobní nebo nemocniční ochranka, což naznačuje fyzickou ochranu chráněných osob, pokud to situace vyžaduje. Omezení přístupu veřejnosti na oddělení bylo dalším krokem pro ochranu bezpečnosti, i když se méně často zmiňovala zvláštní opatření při návštěvách. Tato opatření se zdají být volena na základě konkrétních potřeb a situací jednotlivých chráněných osob.

Graf 4.8: Omezení soukromí ochrankou; Zdroj: autor (2024)



Výsledky této otázky naznačují, že velká většina respondentů nepociťovala žádná významná omezení v soukromí nebo pohybu po zdravotnickém zařízení v důsledku přijatých bezpečnostních opatření či přítomnosti ochranky. To může znamenat, že opatření byla implementována způsobem, který nezasahoval do běžného chodu pacientů, ani nenarušoval jejich komfort. Menší část respondentů uvedla, že pociťovali jistá omezení, ale šlo o marginální zkušenosti, které nepovažovali za výrazné překážky. Jen velmi malý podíl respondentů vyjádřil, že bezpečnostní opatření měla vliv na jejich soukromí nebo volný pohyb, což naznačuje, že u většiny pacientů byla tato opatření vnímána jako nenápadná a neinvazivní.

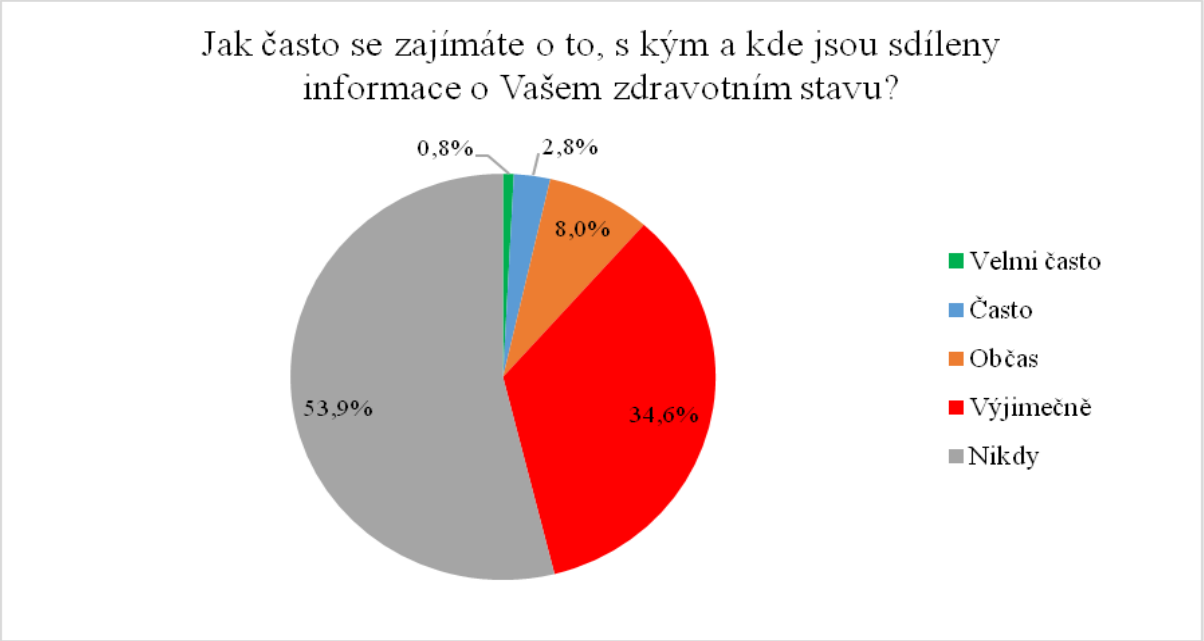
Graf 4.9: Informování o bezpečnosti dat chráněných osob; Zdroj: autor (2024)

Výsledky této otázky ukazují, že téměř všichni respondenti nebyli informováni o opatřeních týkajících se kybernetické bezpečnosti jejich osobních a zdravotních údajů ze strany zdravotnických zařízení. Tento výrazný nedostatek komunikace může u pacientů vyvolávat nejistotu a obavy ohledně toho, jak jsou jejich citlivé informace chráněny. Pouze malá část respondentů potvrdila, že obdržela informace o bezpečnostních opatřeních, což podtrhuje potřebu zlepšit informovanost pacientů a transparentnost v oblasti ochrany dat. V situaci, kdy digitální bezpečnost hraje stále větší roli, by jasná komunikace o ochraně osobních údajů mohla zvýšit důvěru pacientů ve zdravotnická zařízení.

Graf 4.10: Kontrola nahlížení do zdravotní dokumentace chráněných osob; Zdroj: autor (2024)

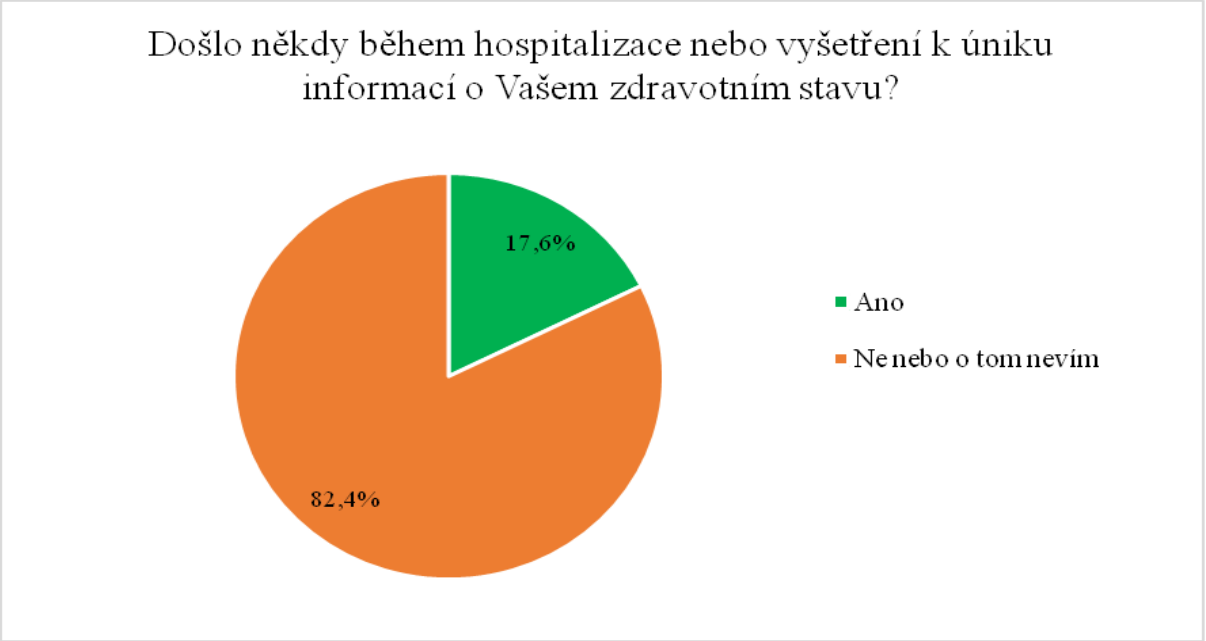
Výsledky této otázky ukazují, že většina respondentů nevěnovala pozornost tomu, zda do jejich zdravotní dokumentace nahlíželi pouze oprávnění zaměstnanci. Tento nezájem může naznačovat důvěru pacientů v bezpečnostní a personální postupy zdravotnických zařízení, nebo také nedostatek povědomí o tom, kdo může mít přístup k jejich citlivým informacím. Pouze malá část respondentů projevila aktivní zájem o tuto problematiku, což zdůrazňuje potřebu zvýšit informovanost pacientů o jejich právech v oblasti ochrany osobních údajů. Zdravotnická zařízení by se mohla více zaměřit na vzdělávání pacientů o možnostech kontroly přístupů ke své dokumentaci, čímž by se zvýšila důvěra a ochrana osobních dat.

Graf 4.11: Informace o sdílení pacientských dat chráněných osob; Zdroj: autor (2024)



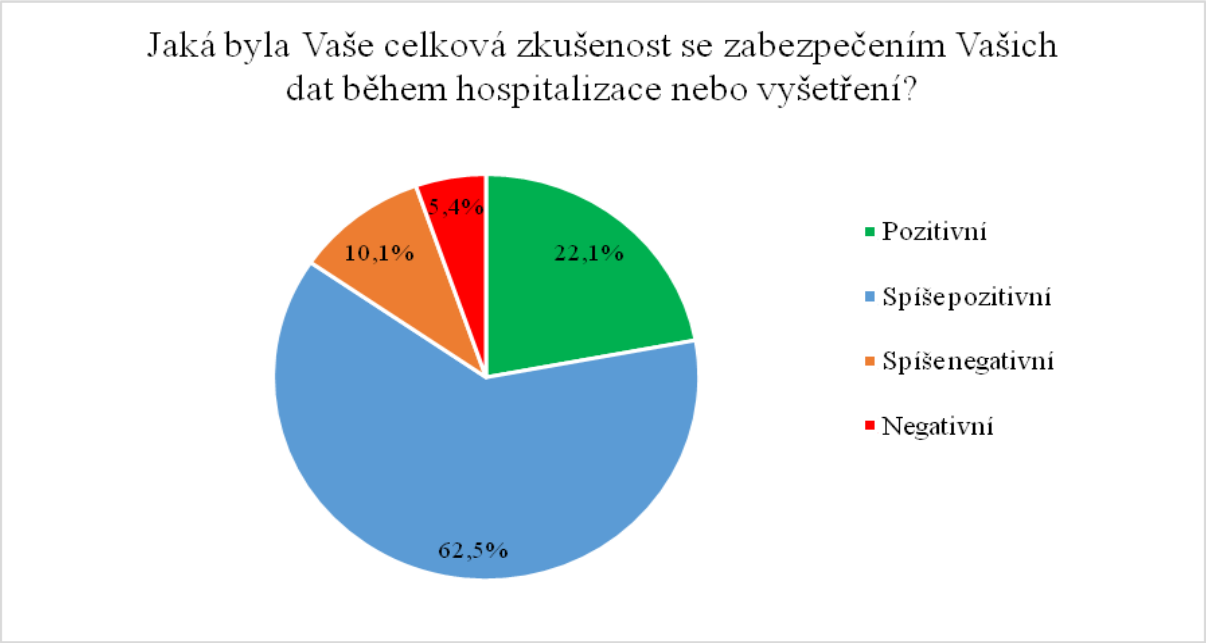
Z výsledků této otázky vyplývá, že většina respondentů se nezajímá o to, s kým a kde jsou sdíleny informace o jejich zdravotním stavu. Tento postoj může odrážet buď vysokou míru důvěry v zdravotnický systém, nebo nedostatečné povědomí o možných rizicích spojených s únikem osobních údajů. Pouze menší skupina pacientů projevuje aktivní zájem o to, jak jsou jejich citlivé údaje zpracovávány a sdíleny. Tento nedostatek zájmu může vést k potenciální zranitelnosti pacientů, pokud by došlo k neoprávněnému přístupu k jejich zdravotním datům, a ukazuje na potřebu lepší komunikace a vzdělávání pacientů o právech na ochranu osobních informací a bezpečnostních postupech ve zdravotnických zařízeních.

Graf 4.12: Únik zdravotních dat chráněných osob během hospitalizace; Zdroj: autor (2024)



Výsledky této otázky naznačují, že většina respondentů, kteří byli hospitalizováni, neměla žádnou specifickou zkušenost s událostmi nebo podmínkami, jež byly zmíněny v dotazníku. Většina z respondentů uvedla, že nečelili žádné z uvedených situací. Na druhou stranu, menší podíl respondentů potvrdil, že měli s těmito podmínkami nebo událostmi zkušenost. Tyto údaje ukazují, že většina hospitalizovaných neměla během svého pobytu v nemocnici specifické problémy nebo podmínky uvedené v dotazníku, ale existuje určité procento pacientů, které mělo s těmito situacemi přímou zkušenost, což může poukazovat na ojedinělé výjimky nebo individuální případy vyžadující větší pozornost.

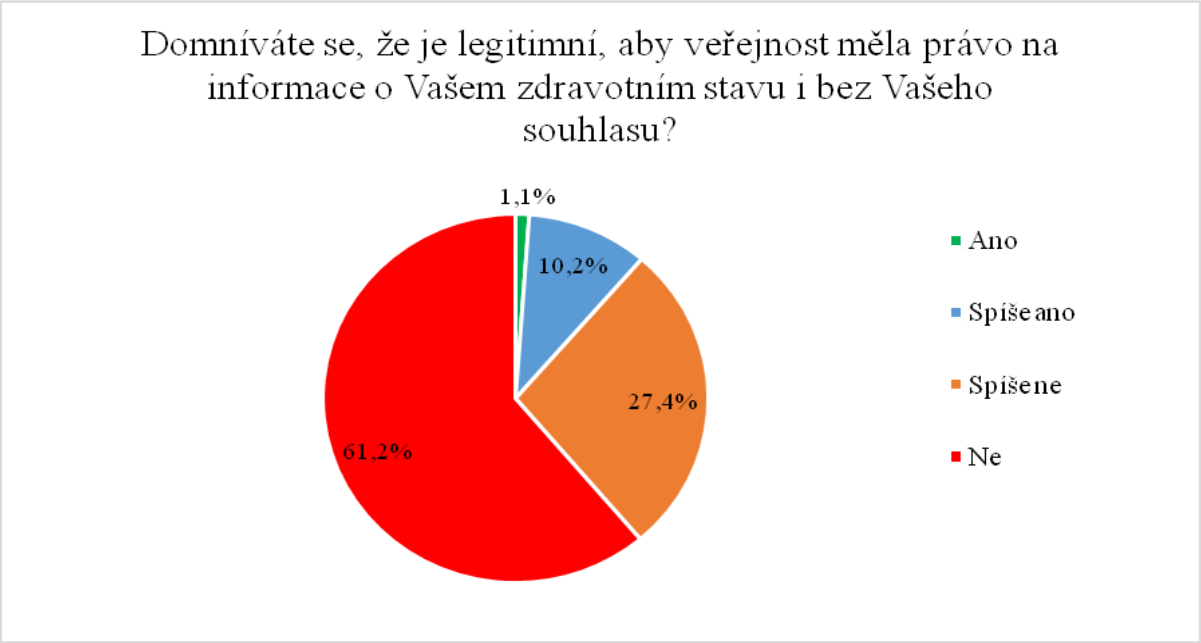
Graf 4.13: Zkušenosti chráněných osob se zabezpečením jejich zdravotních dat; Zdroj: autor (2024)



Z odpovědí vyplývá, že většina respondentů měla převážně pozitivní zkušenosti se zabezpečením svých dat během hospitalizace nebo vyšetření. Většina respondentů své zkušenosti hodnotila jako velmi pozitivní nebo spíše pozitivní, což naznačuje, že zdravotnická zařízení z velké části efektivně chrání citlivé údaje pacientů. Tento pozitivní přístup může zvyšovat důvěru pacientů ve zdravotní péči a v systémy na ochranu osobních údajů.

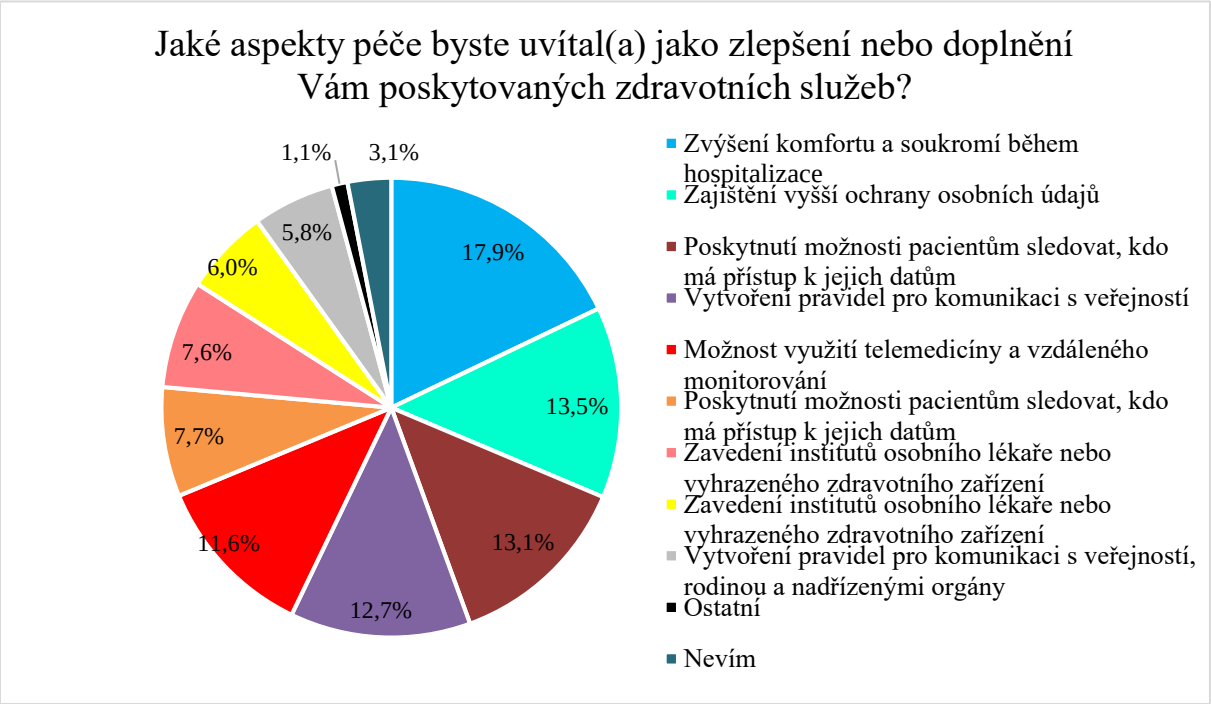
Na druhé straně menší skupina respondentů uvedla, že jejich zkušenosti se zabezpečením dat byly spíše negativní nebo vyloženě negativní. To ukazuje na určité nedostatky nebo obavy týkající se ochrany osobních dat, které by si zasloužily větší pozornost a mohly by být řešeny zlepšením postupů a opatření pro ochranu dat.

Graf 4.14: Otázka legitimnosti zveřejnění informací o zdravotním stavu chráněných osob; Zdroj: autor (2024)



Z výsledků této otázky je patrné, že většina respondentů nesouhlasí s tím, aby veřejnost měla přístup k jejich zdravotním informacím bez jejich výslovného souhlasu. Významná část respondentů se postavila proti této myšlence a jen nepatrné množství osob považuje za přijatelné, aby jejich zdravotní údaje byly zpřístupněny bez jejich svolení. Tyto výsledky jasně ukazují silnou preferenci respondentů pro zachování soukromí a ochranu osobních údajů, což odráží obecnou snahu o ochranu soukromí a bezpečnost citlivých informací.

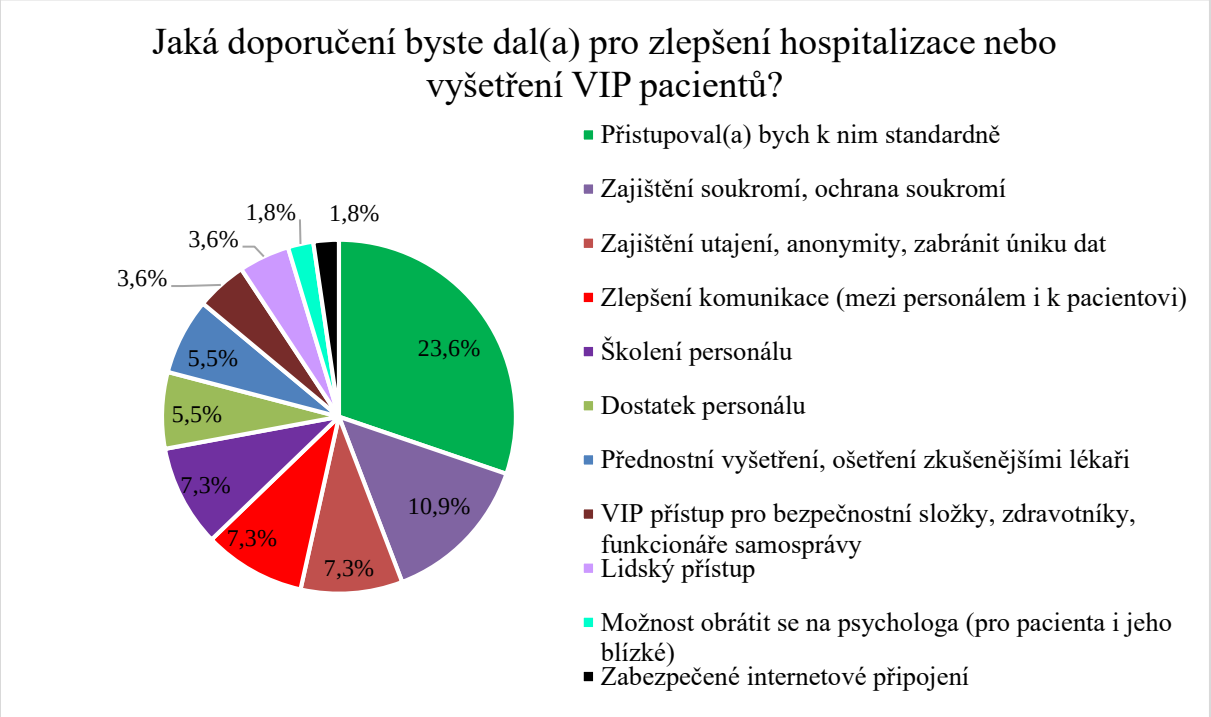
Graf 4.15: Návrh opatření pro zlepšení poskytovaných zdravotních služeb; Zdroj: autor (2024)



Z odpovědí respondentů vyplývá, že mezi hlavními prioritami pro zlepšení zdravotnické péče během hospitalizace je zvýšení komfortu a soukromí, což naznačuje význam klidu a pohodlí pro pacienty. Tento požadavek je často spojován s pocitem bezpečí a pohodlí, který může pozitivně ovlivnit proces zotavování. Ochrana osobních údajů je také důležitou oblastí zájmu, kdy respondenti chtějí mít jistotu, že jejich citlivé informace jsou chráněny před neoprávněným přístupem. Transparentnost v tom, kdo má přístup k jejich datům, je další klíčová otázka, která zdůrazňuje touhu po kontrole nad vlastními informacemi.

Zavedení pravidel pro komunikaci s veřejností by podle některých respondentů mohlo přinést lepší řízení sdílení informací a posílit důvěru pacientů ve zdravotnický systém. Preference moderních technologií, jako je telemedicína a vzdálené monitorování, rovněž ukazují na rostoucí poptávku po digitálních nástrojích, které by umožnily větší flexibilitu a dostupnost péče. Ostatní zmíněné návrhy, jako je možnost osobního lékaře nebo vyhrazeného zdravotnického zařízení, naznačují touhu po více personalizovaném přístupu ke zdravotní péči.

Graf 4.16: Doporučení pro zlepšení hospitalizace nebo vyšetření chráněných osob; Zdroj: autor (2024)



Výsledky naznačují, že nejčastějším doporučením mezi respondenty je přistupovat k chráněným osobám standardně, bez zvláštního zacházení. To ukazuje na preferenci rovnosti v poskytované péči a na názor, že není nutné uplatňovat odlišný přístup k těmto pacientům.

Další významná skupina respondentů zdůrazňuje důležitost zajištění soukromí a ochrany citlivých informací chráněných osob. Někteří navrhují zavedení opatření pro utajení a anonymitu, aby se předešlo úniku informací o zdravotním stavu, což odráží obavy týkající se bezpečnosti osobních údajů.

Někteří respondenti se zaměřují na zlepšení komunikace mezi zdravotnickým personálem a pacienty, což naznačuje potřebu efektivnějšího sdílení informací a lepšího porozumění mezi oběma stranami. Důraz je také kladen na zajištění dostatečného počtu kvalifikovaného personálu a preferenci, aby vyšetření nebo ošetření prováděli zkušení lékaři. Zmíněná doporučení ukazují na široké spektrum názorů na péči o chráněné osoby, s důrazem na standardizaci přístupu, ochranu soukromí, bezpečnost dat a kvalitní komunikaci.

4 Model přenosu pacientských dat chráněných osob v rámci virtuální hospitalizace

Na základě provedeného výzkumu a získaných informací, které byly analyzovány s výstupy teoretické části práce, se autor v této části disertační práce pokusí navrhnout možnosti pro přenos pacientských dat chráněných osob v rámci virtuální hospitalizace. Tato kapitola vychází rovněž z výsledků a závěrů uvedených v publikaci *„Virtual War Medicine – A Key Element of Modern Warfare“*. Článek byl přijat k publikaci v rámci mezinárodní vědecké konference *Challenges to National Defence in Contemporary Geopolitical Situation*[37], která se uskutečnila ve dnech 11. – 13. září 2024 v Brně. Tento článek, který je součástí autorova výzkumu v rámci doktorského studia na Českém vysokém učení technickém v Praze, Fakultě biomedicínského inženýrství, představuje klíčový zdroj pro rozpracování konceptu přenosu dat v rámci virtuální hospitalizace chráněných osob v rámci vojenských konfliktů.

Jelikož jednou z exponovaných skupin chráněných osob jsou také vojáci, je možné a zejména vhodné popsané možnosti modelovat na nich. V této souvislosti a s odkazem na provedené rozhovory s odborníky lze odkázat na aktuální ukrajinské zkušenosti s vývojem elektronických systémů, které představují nesmírně cenný zdroj poznatků. Ten může posloužit jako inspirace pro vývoj systémů ostatních armád NATO. Zmíněné systémy by měly umožnit přenos dat nejen o zdravotním stavu vojáků na bojišti přímo do informačních systémů vojenských poskytovatelů zdravotních služeb. Implementace takových systémů je nezbytná jak pro sekci vojenského zdravotnictví NATO, tak pro jednotlivé armádní složky, a to za účelem efektivnějšího sběru a analýzy fyziologických dat přímo z těl vojáků. K tomuto účelu mohou sloužit technologie IoT, jako jsou biosenzory a čidla, která umožňují monitorovat nejen zdravotní parametry, ale i podmínky okolního prostředí.

Tato zjištění jsou podpořena výsledky autorova výzkumu a rozhovorů provedených v rámci disertační práce, které jasně ukázaly na potřebu zavedení efektivních a interoperabilních systémů přenosu dat pro vojenské zdravotnictví. V rámci těchto rozhovorů se ukázalo, že jedním z klíčových požadavků je zajištění bezpečného a rychlého přenosu dat o zdravotním

[37] Dále jen „konference CNDCGS 2024“.

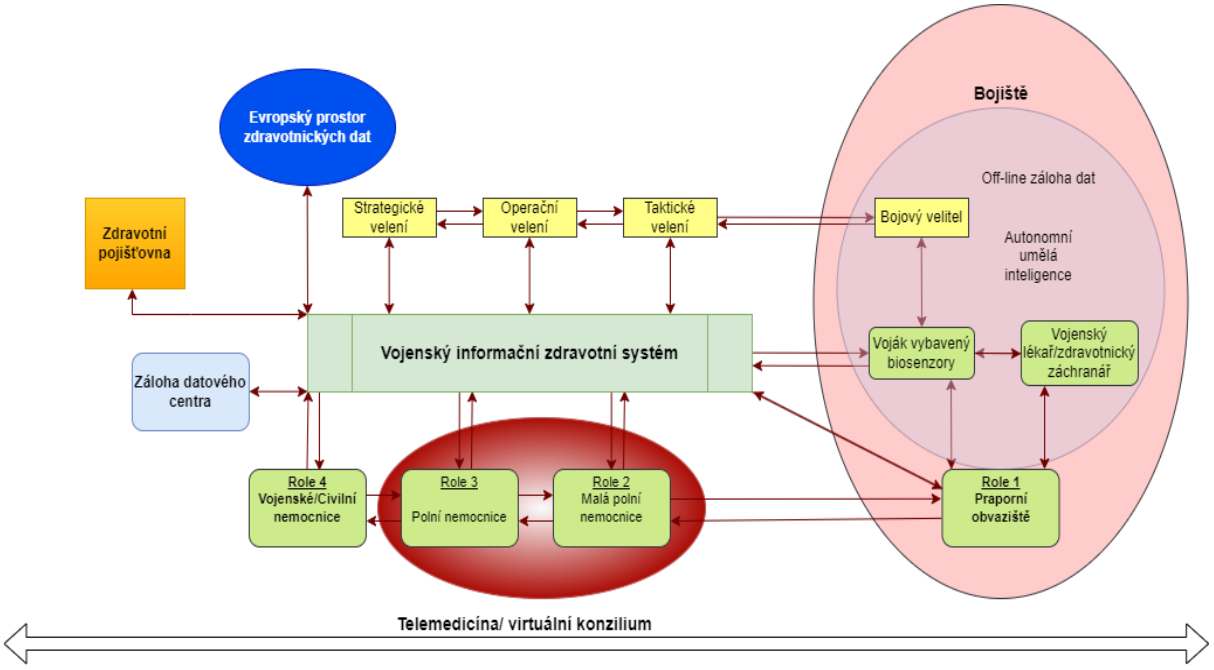
stavu vojáků z bojiště do zdravotnického zařízení, což umožní lékařům rychle reagovat na měnící se situace.

Data získaná z těchto systémů by měla být bezpečně přenášena a ukládána do databází ambulantních nebo nemocničních informačních systémů vojenských zdravotnických zařízení. K tomu je důležité využívat protokoly, které v ideálním případě odpovídají předem stanoveným interoperabilním standardům. Takový přístup zajistí, že data budou snadno přístupná a kompatibilní napříč různými zdravotnickými zařízeními a vojenskými jednotkami, což je klíčové pro rychlé a efektivní rozhodování v krizových situacích.

Personalizované vyhodnocování zdravotního stavu jednotlivých vojáků na základě těchto dat umožní nejen přesnější a rychlejší diagnostiku, ale také predikci vývoje zdravotního stavu a včasné zahájení účinné terapie. To by mohlo zahrnovat i následnou rehabilitaci, což je zvláště důležité pro dlouhodobé zotavení zraněných vojáků. Klíčovým prvkem tohoto modelu je schopnost fungovat decentralizovaně, což znamená, že systém by měl být přístupný jak na individuální úrovni vojáků, tak na úrovni velení. To zajistí kvalitnější péči o zraněné ve válečných podmínkách a optimalizuje proces jejich evakuace a následné hospitalizace v nemocničních zařízeních.

Digitalizace a telemedicína hrají v této strategii klíčovou roli. Umožní nejen výrazné rozšíření možností válečné medicíny, ale také zvýší šance na přežití vojáků. Díky včasným a cíleným zdravotnickým zásahům na základě real-time analýz zdravotních dat se může snížit potřeba okamžitého převozu do polních nemocnic. Real-time data o zdravotním stavu vojáků umožní lékařům a zdravotnickému personálu včasnou reakci, a to i na dálku, což může být rozhodující v situacích, kdy fyzická přítomnost zdravotníků není možná.

Celý model přenosu dat by měl být logicky navázán na nemocniční informační systém vojenského poskytovatele zdravotních služeb. Jakmile to okolnosti dovolí, mělo by dojít k hospitalizaci zraněného vojáka v takovém zařízení, kde budou veškerá potřebná data k dispozici pro pokračování v péči a léčbě. Tento systém zajistí, že péče o vojáky bude nejen efektivní, ale také bezpečná, což je základním předpokladem pro úspěch v moderním válečnictví. Zmíněný model je znázorněn na následujícím diagramu.



Obr. 1: Model přenosu a využití zdravotnických údajů chráněných osob (vojáků) v rámci virtuální hospitalizace; Zdroj: autor (2024).[256]

Diagram zobrazený na obrázku č. 1 vychází z konceptu modelu přenosu dat v rámci virtuální hospitalizace[38] a byl autorem dopracován na základě informací získaných z kvalitativní části výzkumu. Představuje dílčí modul navržený autorem práce pro přenos a správu dat (obsahových, ale i metadat) o zdravotním stavu vojáků z místa jejich nasazení (bojiště, zahraniční mise atd.) do různých úrovní rolí vojenské zdravotnické služby vybrané armády, který je integrovaný do širšího vojenského zdravotního informačního systému. Tento systém v kritickém časovém intervalu umožní zajistit sběr, zachycení, analýzu a efektivní předání životně důležitých zdravotních údajů vojáků, a to jak zdravotníkům, tak jejich velitelům na všech úrovních. Model zároveň **umožňuje vytvoření bezpečného virtuálního prostředí pro přenos všech typů požadovaných dat, včetně realizace virtuálních konsilií či poskytování zdravotních služeb formou telemedicíny**. Je efektivním nástrojem pro realizaci virtuální hospitalizace raněného vojáka do doby, nežli bude možná jeho hospitalizace u vojenského poskytovatele zdravotních služeb i fyzicky.

[38] Viz Miklas, L., Kolouch, J. (2024) *Virtual War Medicine – A Key Element of Modern Warfare*. Doposud nepublikovaný článek.

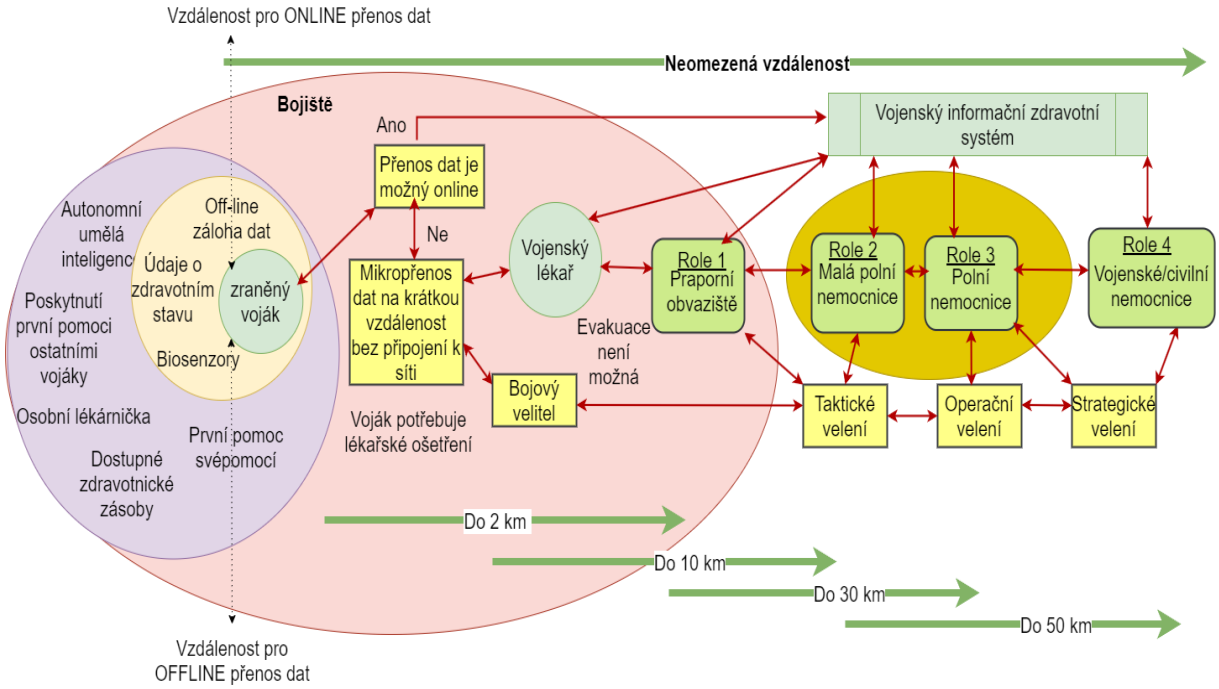
Na jednotlivých úrovních velení je možné získaná data ze senzorů vojáků využít pro další vyhodnocení a rozhodování o jejich nasazení či poskytnutí zdravotnické pomoci. Celý koncept vytváří celistvý ekosystém, jehož centrálním uzlem je vojenský zdravotní informační systém, který sbírá, zpracovává a dále distribuuje zdravotní data vojáků oboustranně až do nemocničního informačního systému vojenského poskytovatele zdravotních služeb. Tento systém komunikuje s různými úrovněmi velení, vojenskými i nevojenskými poskytovateli zdravotních služeb, což umožňuje poskytovat rychlý přístup k datům a rozhodování v reálném čase. **V případě výpadku vojenského zdravotnického systému však mohou být data stále uchována a předávána na jednotlivé role**. Výhodou využití centralizovaného systému je **okamžitá distribuce dat** oprávněným osobám a jeho nezávislost na tomto centrálním prvku.

Bezpečnostní aspekt datových toků musí zahrnovat aplikaci robustních šifrovacích standardů a firewallové ochrany, aby se zabránilo neoprávněnému přístupu nebo úniku dat, a to jak v době míru, tak zejména v době ozbrojeného konfliktu. Takovéto řešení nutně zahrnuje i bezpečnostní protokoly pro autorizaci, autentizaci a identifikaci oprávněných osob, jakož i úrovně jejich oprávnění, což zajistí přístup a verifikaci pouze oprávněných uživatelů či subjektů, které mohou data zpracovávat a přenášet. Z pohledu kybernetické bezpečnosti je krátkodobý horizont fungování počítačového systému ideální, nicméně pro účely trvalejšího využití bude nezbytné, ze strany příslušných členských států, vybudování infrastruktury informačních technologií a vytvoření příslušných právních předpisů upravujících jak oblast bezpečnosti a standardů jeho fungování, tak oblast ochrany osobních údajů, které se tento systém bezprostředně dotýká.

Na základě získaných informací z provedeného výzkumu, zejména z realizovaných rozhovorů s experty, je pak zcela zásadní, aby předávání dat probíhalo způsobem, který bude bezpečný z pohledu zjištění geolokačních dat. **Vysílání musí být realizováno ideálně v minimálním časovém intervalu**, během kterého však dojde k přenosu velkého objemu dat. **Interval přenosu dat by měl být v řádech mikrosekund**; mělo by docházet k tzv. mikropřenosu velkého objemu dat, a to právě z důvodu nemožnosti lokace vysílajícího subjektu. Naopak je možné, aby data byla přijímána.

Prezentovaný model předpokládá využití částečně virtualizovaného a cloudového prostředí, které může nabídnout vysokou úroveň diversifikace a zároveň dostupnosti dat a informací o skupinách chráněných osob – pacientů. Takovéto řešení se jeví jako vhodné pro vojenské cloudové platformy navržené speciálně pro odolnost proti kybernetickým hrozbám a se schopností fungovat v různých prostředích – od stabilních datových center až po mobilní

a nasazené operační jednotky, které vyžadují vysokou úroveň redundance a rychlou adaptabilitu na měnící se podmínky. Jak již bylo uvedeno, předávání dat a informací však není na cloudovém prostředí závislé a umožňuje i alternativní způsob předávání dat a informací, právě z důvodu mikropřenosu dat v případě, kdy to bude nezbytné.



Obr. 2: Model offline mikropřenosu zdravotních dat chráněných osob; Zdroj: autor (2024).[256]

Diagram uvedený na obrázku č. 2 vychází z konceptu modelu offline přenosu dat v rámci virtuální hospitalizace[39] a byl autorem dopracován na základě informací získaných z kvalitativní části výzkumu. Ilustruje možnosti procesu přenosu zdravotních dat z bojiště do různých úrovní vojenské zdravotnické služby, až do nemocničního informačního systému vojenského poskytovatele zdravotních služeb. V prvním kroku jsou zdravotní data zraněného vojáka shromážděna pomocí biosenzorů; mohou být doplněna o informace týkající se první pomoci nebo o autonomní první pomoci s využitím umělé inteligence. Pokud je možný online přenos, data jsou ihned poslána do vojenského zdravotního informačního systému bez ohledu na vzdálenost. V případě, že online přenos není možný, například z technických, taktických

[39] Miklas, L., Kolouch, J. (2024) *Virtual War Medicine – A Key Element of Modern Warfare*. Doposud nepublikovaný článek.

nebo bezpečnostních důvodů, **data jsou uchovávána offline a přenášena bezpečně pomocí mikropřenosu velkého objemu dat na krátkou vzdálenost** (až do 2 km) k vojenskému lékaři, který je na bojišti nebo v jeho blízkosti, kde je může vyhodnotit a zpracovat pro další použití. Cestou vojenského lékaře se data mohou dále přenášet do systému vojenské zdravotnické služby, který je rozdělen do několika rolí. Role 1 je praporní obvaziště, které může být umístěno až 10 km od bojiště.

Dle dat získaných z výzkumu lze usoudit, že Role 2, která představuje malou polní nemocnici, a Role 3 představující plnohodnotnou polní nemocnici, prakticky nelze bezpečně využít blízko bojiště, a to z důvodu zkušeností z ukrajinského bojiště. Nepřítel totiž při zjištění polohy Role 2 nebo Role 3 může provádět cílené útoky i na tyto pozice. Dle vyjádření jednoho z respondentů dnes prakticky již nelze spoléhat na uvedenou strukturu a mělo by docházet k přenosu dat z Role 1 přímo na Roli 4. Přenos dat a využití Role 2 a Role 3 je možný pouze za předpokladu zajištění bezpečnosti jejich pozic. Role 4 představuje vojenská nebo civilní zdravotnická zařízení, kde jsou data konečně integrována do širšího vojenského zdravotního informačního systému, v rámci kterého plně probíhá virtuální proces hospitalizace raněného vojáka. V systému vojenské zdravotnické služby jsou data koordinována a analyzována na taktické, operační a strategické úrovni velení, což umožňuje informované rozhodování ohledně léčby a možností evakuace zraněných vojáků. Zdravotní informační systém slouží jako základ pro sběr, uchovávání a analýzu dat, což umožňuje telemedicínské konzultace a poskytování virtuální lékařské péče – virtuální hospitalizace chráněných osob.

Dle vyjádření respondentů lze ze zkušeností z ukrajinského bojiště totiž předpokládat, že tento systém nebude možné na bojišti udržovat relativně stále v režimu on-line. Obrázek č. 1 ilustruje sofistikovaný systém pro přenos a využití vojenských zdravotních dat, který je navržen tak, aby odolal výzvám, s nimiž se mohou potýkat chráněné osoby v bojových podmínkách. Musí být totiž navržen tak, aby zůstal funkční i za nepříznivých podmínek v rámci konfliktů vysoké intenzity, kde okamžitá evakuace zraněných není možná a je nutné využít prostředků virtuální hospitalizace raněných vojáků. Zahrnuje off-line / semi off-line řešení pro shromažďování a uchovávání dat, která umožní průběžné sledování zdravotního stavu vojáků a které zajistí zálohování a obnovu dat pro případ potřeby do doby, kdy je bude možné zase bezpečně sdílet a připojit se k armádní síti. S uvedeným souvisí i možnost napojení technologií umělé inteligence, která by dokázala bez připojení do sítě po určitou dobu pomoci s poskytováním zdravotních služeb raněnému vojákovi přímo na bojišti autonomně.[113] Předpokladem je, že

umělá inteligence bude schopna provést vojáky provádějící ošetření předdefinovanými kroky, které budou variabilně vyhodnocovány na základě měnící se situace (viz využití dat generativní AI), k maximální možné stabilizaci zraněné osoby vedoucí ke stabilizaci zdravotního stavu do doby možného transportu. Generativní AI by bylo možné využít jako prostředek pro konzultace či pomoc vojenským zdravotníkům na bojišti při jejich činnostech. To vše při zajištění maximální možné bezpečnosti přenosu dat pomocí mikropřenosů, které zabezpečení nemožnost lokalizace vysílajícího zařízení a zároveň umožní přenos velkého objemu dat.

Kombinace výše uvedeného a jednotlivých prvků procesu virtuální hospitalizace, umělé inteligence a telemedicíny může dle názoru autora práce významně zvýšit procentuální šance raněných vojáků na přežití. Využití simulací, virtuálních konsilií a dálkově ovládané lékařské technologie by mohlo umožnit provádět chirurgické zákroky a poskytovat nezbytnou neodkladnou zdravotní péči i v nepřístupném nebo izolovaném prostředí bojiště, a to vše za předpokladu bezpečného přenosu dat chráněných osob.

Navržený systém zohledňuje požadavky civilní i vojenské sféry – zachovává přísné bezpečnostní normy a zároveň poskytuje flexibilitu a integraci potřebnou pro civilní léčebná zařízení, což usnadňuje přechod a pokračování z virtuální hospitalizace do té fyzické, a to rovněž pro poskytování péče pro vojenské pacienty v civilním zdravotním systému, například v rámci rehabilitace nebo v případě nutnosti využití civilních zdravotnických zařízení pro vojenské účely. Uvedený model lze využít analogicky na jakoukoliv jinou skupinu chráněných osob, nejen vojáků.

Zcela **zásadní je ovšem bezpečnost dat chráněných osob při virtuální hospitalizaci**, a to nejen z pohledu jejich možného úniku, **ale také z pohledu jejich přenosu a nemožnosti lokalizace vysílajícího nebo přijímajícího subjektu**. V této oblasti je velmi žádoucí vývoj nových technologií, které takový mikropřenos dat umožní.

5 Doporučení pro praxi

V této kapitole zaměřené na doporučení autor podává přehled o závěrech, ke kterým dospěl na základě teoretických poznatků a vlastního výzkumu. Autor se systematicky věnoval analýze problematiky týkající se ochrany citlivých zdravotních údajů chráněných osob, virtuální hospitalizace a bezpečnostních opatření, která by měla být implementována ve zdravotnických zařízeních. Na základě rozsáhlé rešerše dostupných pramenů z celosvětového prostředí, kombinované s kvalitativními a kvantitativními výzkumnými metodami, došel k návrhům konkrétních opatření, která reflektují potřebu zlepšit současný stav.

Autor nejprve zkoumal teoretický rámec, který zahrnoval klíčové aspekty, jako je právní úprava zdravotní péče, role chráněných osob a aplikace fyzických i kybernetických bezpečnostních opatření. Tento teoretický základ byl následně propojen s informacemi získanými z výzkumu, který zahrnoval dotazníky distribuované mezi zdravotnické pracovníky i chráněné osoby a následnou analýzu získaných dat. Tyto výzkumné metody umožnily detailně porozumět potřebám a problémům, kterým čelí zdravotnický personál při péči o chráněné osoby, a identifikovat slabiny v oblasti ochrany osobních údajů.

V průběhu svého výzkumu autor analyzoval řadu případů a trendů týkajících se virtuální hospitalizace a přenosu zdravotních dat, přičemž kladl důraz na jednotlivá bezpečnostní opatření a postupy. Doporučení, která jsou v této kapitole podrobně rozpracována, se opírají o praktické zkušenosti z praxe a vycházejí z kombinace inovativních technologických přístupů a nezbytných právních opatření.

Autor se zabýval návrhy, které zahrnují nejen technická opatření, jako je šifrování a ochrana dat pomocí moderních technologií, ale také organizační přístupy, včetně školení zaměstnanců a zavedení pravidelných bezpečnostních auditů. Doporučení jsou strukturována tak, aby zajišťovala efektivní a bezpečné poskytování zdravotní péče chráněným osobám, a to s minimálním dopadem na provoz zdravotnických zařízení a na kvalitu poskytované péče.

5.1 Zavedení standardizovaných postupů a regulací

Zdravotnická zařízení by měla implementovat jednotné standardy pro ochranu dat chráněných osob, a to v souladu s mezinárodními normami, jako je HL7. Tyto standardy by zahrnovaly následující prvky:

Šifrování dat: Všechna data, zejména citlivá osobní a zdravotní data, by měla být chráněna silným šifrováním jak při přenosu, tak při uchovávání.

Omezení přístupu: Přístup k citlivým informacím by měl být omezen pouze na oprávněné osoby podle předem definovaných pravidel.

Pravidelné audity a kontroly: Implementace pravidelných auditů zaměřených na dodržování bezpečnostních pravidel a detekci potenciálních rizik. Audity by měly být nejen technické, ale i organizační, aby se zajistila kompletní ochrana dat.

Dynamické řízení přístupu: Přístupy k datům by měly být přizpůsobitelné na základě aktuálních bezpečnostních podmínek a potřeb. Tento přístup by zahrnoval například automatickou změnu přístupových oprávnění při zvýšení rizika (např. kybernetického útoku).

Dále by bylo vhodné standardy upravovat a aktualizovat v reakci na nové technologie a hrozby. Autor doporučuje také zavedení minimálních požadavků na ochranu dat na úrovni státu, přičemž tato opatření by byla pravidelně revidována a aktualizována příslušným ministerstvem.

5.2 Vytvoření oddělených sítí pro citlivá data chráněných osob

Pro zajištění vyšší ochrany citlivých dat vybraných skupin chráněných osob by měla být vytvořena oddělená a izolovaná síť, která nebude propojena s běžnou komunikační infrastrukturou zdravotnického zařízení. Tato síť by zahrnovala:

Samostatné servery: Zřízení fyzicky nebo virtuálně oddělených serverů pro ukládání a přístup k citlivým datům chráněných osob.

Omezený přístup: Přístup do těchto sítí by měl být povolen pouze na základě dvoufaktorové autentizace nebo biometrických systémů, aby se minimalizovalo riziko neoprávněného přístupu.

Cloudová řešení: Pokud je využíván cloud, je důležité, aby byl vysoce zabezpečen a aby přístupová práva byla důsledně monitorována. Mělo by být zváženo využití šifrovaných cloudových řešení, která by byla pravidelně kontrolována bezpečnostními složkami. Dle doporučení autora práce by před využitím cloudu měla být provedena důkladná analýza rizik nebo balanční analýza.

Decentralizované ukládání dat: Implementace systémů, které využívají principy blockchainu[40] k bezpečnému ukládání a sledování přístupů k datům, čímž se zajistí větší transparentnost a ochrana před neoprávněnými úpravami či přístupem.

5.3 Rozšíření a specializace školení zaměstnanců

Pravidelné a specializované školení zaměstnanců zaměřené na ochranu citlivých dat chráněných osob je klíčové. Školení by mělo být strukturováno následovně:

Simulace kybernetických útoků: Praktická cvičení, která zaměstnancům umožní rozpoznat kybernetické hrozby, jako je phishing, malware nebo sociální inženýrství, a naučí je, jak na tyto situace reagovat.

Zaměření na specifické hrozby: Školení by měla být zaměřena na konkrétní rizika, která mohou postihnout chráněné osoby (všechny typy „VIP pacientů“).

Gamifikace školení: Interaktivní školení prostřednictvím herních simulací, kde se zaměstnanci dostávají do různých scénářů kybernetických hrozeb a musí najít správná řešení. Autor práce doporučuje využití technologie rozšířené virtuální reality přímo v prostředí zdravotnického zařízení. Tento přístup zvyšuje zapojení a efektivitu školení.

5.4 Pravidelná aktualizace bezpečnostních protokolů

Zdravotnická zařízení by měla zajistit pravidelnou aktualizaci bezpečnostních protokolů, která bude zahrnovat:

Sledování nových technologií a hrozeb: Neustálé monitorování vývoje kybernetických hrozeb a rychlá implementace odpovídajících protiopatření.

Pravidelné revize protokolů: Každých 6 až 12 měsíců by měly probíhat revize a aktualizace bezpečnostních protokolů, které by zohledňovaly nové hrozby a inovace v technologickém prostředí.

Prediktivní kybernetická bezpečnost: Využití strojového učení a umělé inteligence pro predikci potenciálních kybernetických útoků a automatizaci reakcí na hrozby, což umožní zdravotnickým zařízením rychle reagovat na hrozby dříve, než způsobí škodu.

[40] Blockchain je distribuovaná a decentralizovaná technologie, která umožňuje bezpečné, transparentní a nezměnitelné uchovávání a sdílení dat.

5.5 Analýza rizik a hodnocení bezpečnostních opatření

Pravidelná analýza rizik by měla být nedílnou součástí bezpečnostní strategie zdravotnických zařízení v oblasti zajištění bezpečnosti chráněných osob. Měla by zahrnovat:

Dynamická analýza rizik: Průběžné hodnocení aktuálních a budoucích rizik spojených s vývojem nových technologií nebo změnami v organizaci zdravotní péče.

Hodnocení nových technologií: Každá nově implementovaná technologie by měla projít bezpečnostním testováním příslušného oddělení zdravotnického zařízení, aby bylo zajištěno, že nebude zvyšovat zranitelnost systému.

Automatizovaná analýza rizik: Implementace systémů, které budou automaticky analyzovat bezpečnostní rizika na základě aktuálních bezpečnostních dat a budou doporučovat opatření k jejich snížení. Autor práce doporučuje zavést monitorování veřejného prostoru a pro případ hospitalizace či ošetření chráněné osoby automatickou detekci takové osoby v prostředí zdravotnického zařízení. Toto opatření umožní efektivně reagovat na neplánovanou přítomnost chráněné osoby.

5.6 Zlepšení ochrany citlivých dat a zvýšení kybernetické bezpečnosti

Zavedení moderních technologií je nezbytné pro ochranu citlivých dat chráněných osob. To zahrnuje:

Šifrovací systémy: Všechny citlivé údaje by měly být chráněny silným šifrováním během přenosu i při uložení.

Efektivní správa přístupů: Měly by být zavedeny přísné mechanismy řízení přístupů k datům, včetně dvoufaktorové autentizace a biometrických metod. Rovněž lze doporučit ověření přístupu k datům chráněných osob ze strany nadřízených nebo odpovědných zaměstnanců.

Systémy detekce anomálií: Využití pokročilých systémů umělé inteligence, které budou nepřetržitě sledovat a detekovat neobvyklé chování v přístupech k datům a budou schopny včas detekovat potenciální bezpečnostní incidenty.

5.7 Vypracování specifických protokolů pro ochranu soukromí a bezpečnosti

Specifické protokoly pro ochranu citlivých informací chráněných osob by měly zahrnovat:

Postupy minimalizace úniku informací: Striktní pravidla pro ukládání a přenos citlivých dat, zahrnující šifrování a omezený přístup.

Standardizované komunikační kanály: Zavedení bezpečných komunikačních platforem mezi zdravotnickým personálem a bezpečnostními složkami, které zajistí ochranu dat během jejich výměny.

Zavedení pravidel pro kontrolované sdílení dat: Použití blockchainových technologií pro sledování každého přístupu k datům a jejich změn.

5.8 Minimalizace vlivu bezpečnostních opatření na léčbu

Bezpečnostní opatření by měla být integrována do běžného provozu zdravotnických zařízení tak, aby nenarušovala poskytování péče:

Školení ochranky: Ochranka by měla být pravidelně školena v oblasti spolupráce se zdravotnickým personálem a měla by znát základní specifika léčebných procesů.

Zavedení plánů pro nouzové situace: Nastavení jasných krizových plánů, které budou zahrnovat postupy, jak zajistit bezpečnost chráněné osoby bez narušení léčby ostatních pacientů.

Využití automatických systémů pro správu bezpečnosti: Implementace technologií, které automaticky koordinují bezpečnostní opatření s provozními plány zdravotnických zařízení.

5.9 Zlepšení komunikace a koordinace mezi personálem a ochrankou

Efektivní spolupráce mezi zdravotnickým personálem a ochrankou je klíčová pro zajištění bezpečnosti i plynulosti péče. Doporučuje se:

Pravidelná setkání a školení: Zavést pravidelné schůzky mezi vedením, zdravotnickým personálem a ochrankou (odpovědnými státními subjekty) pro zlepšení komunikace.

Simulace krizových scénářů: Vytvořit cvičení a simulace krizových situací, aby všechny zúčastněné strany věděly, jak postupovat v případě hrozby.

Integrované digitální platformy: Aplikace, které umožní okamžitou a bezpečnou komunikaci mezi personálem a ochrankou v reálném čase, aby byla zajištěna rychlá reakce na incidenty.

5.10 Zavedení specifických opatření pro ochranu zdravotnického personálu

Zdravotnický personál by měl být chráněn stejně jako pacienti, zejména při péči o chráněné osoby, které mohou být vystaveny riziku útoku nebo zvýšeného veřejného zájmu. Konkrétní opatření zahrnují:

Fyzická ochrana personálu: Zajištění přítomnosti bezpečnostních složek v rizikových situacích, například při péči o veřejně známé osobnosti, kdy může být vyšší riziko narušení bezpečnosti. Tato ochrana by měla zahrnovat fyzickou přítomnost ochranky a pravidelné monitorování bezpečnostních opatření.

Využití moderních technologií pro sledování bezpečnosti: Zdravotnický personál by mohl být vybaven nositelnými zařízeními (například chytrými hodinkami), která by upozornila na potenciální hrozby nebo poskytovala rychlý přístup k bezpečnostním složkám v případě nouze.

5.11 Vytvoření jasných pravidel pro přítomnost ochranky při lékařských výkonech

Zdravotnická zařízení by měla mít jasně definovaná pravidla ohledně přítomnosti ochranky při lékařských výkonech, zejména při citlivých nebo invazivních procedurách, jako jsou operace nebo citlivá vyšetření (např. kolonoskopie). Pravidla by měla zahrnovat:

Přítomnost pouze v nezbytných případech: Ochranka by měla být přítomna pouze v situacích, kde je to z bezpečnostního hlediska nutné, a měla by se držet mimo sterilní prostředí, aby nebyl narušen léčebný proces ani sterilita prostředí.

Komunikační protokoly: Vytvoření specifických komunikačních kanálů mezi zdravotnickým zařízením a ochrankou chráněné osoby, aby byla zajištěna koordinace při přítomnosti během lékařských výkonů.

Diskrétní monitorovací technologie: Využití technologií, které umožní ochrance sledovat zdravotní stav pacienta na dálku pomocí bezpečnostních kamer nebo senzorů mimo operační sál, což sníží riziko narušení výkonu, aniž by došlo k ohrožení bezpečnosti.

5.12 Pravidelné školení a cvičení

Pravidelné školení a simulace jsou nezbytné pro zajištění připravenosti zdravotnického personálu i ochranky. Tato školení by měla:

Obsahovat simulace krizových situací: Praktické cvičení, při kterých by personál i ochranka trénovali své reakce na různé scénáře (např. bezpečnostní hrozba, evakuace, kybernetický útok).

Aktualizovat se na základě aktuálních hrozeb: Školení by měla reflektovat nejnovější bezpečnostní trendy a rizika, aby zaměstnanci byli připraveni na nové typy hrozeb.

Rozšířená/virtuální realita: Implementace simulací virtuální reality, které by umožnily zdravotnickému personálu a ochrance trénovat krizové situace v realistických podmínkách, což by vedlo ke zlepšení jejich reakčních schopností, a to včetně rozšířené virtuální reality přímo v prostředí zdravotnického zařízení.

5.13 Zvýšení transparentnosti a komunikace s pacienty

Transparentní komunikace s pacienty, včetně chráněných osob i běžných pacientů, je klíčová pro udržení důvěry ve zdravotnický systém. Doporučení zahrnují:

Informování pacientů: Pacienti by měli být jasně informováni o přítomnosti ochranky a případných bezpečnostních omezeních, která mohou ovlivnit jejich léčbu.

Poskytování informací o důvodech bezpečnostních opatření: Pacienti by měli rozumět tomu, proč jsou zavedena konkrétní bezpečnostní opatření a jak jsou chráněna jejich data a soukromí.

Vytvoření digitální komunikační platformy: Využití například portálu pacienta nebo jiné aplikace, která by poskytovala pacientům informace o bezpečnostních opatřeních, umožňovala jim klást otázky a dostávat odpovědi od personálu v reálném čase.

5.14 Zajištění specifických prostor pro chráněné osoby

Pro maximální zajištění bezpečnosti a soukromí chráněných osob je nezbytné vyčlenit specifické prostory v nemocnicích, které budou odpovídat následujícím kritériím:

Oddělené pokoje: Pro chráněné osoby by měly být k dispozici oddělené pokoje, které zajistí maximální soukromí a sníží riziko kontaktu s veřejností.

Zabezpečené prostory: Tyto prostory by měly být vybaveny bezpečnostními systémy, které zajistí monitoring přístupu a ochranu před neoprávněným vstupem.

Modulární bezpečnostní zóny: Vytvoření flexibilních bezpečnostních zón, které lze rychle přizpůsobit potřebám chráněných osob anebo zdravotnického zařízení podle situace. Tyto zóny by zahrnovaly rychle sestavitelné bariéry, zvýšenou bezpečnost v přístupu k prostorám a možnost snadné evakuace v případě nouze.

5.15 Podpora well-beingu zdravotnického personálu

Péče o chráněné osoby často znamená zvýšenou fyzickou i psychickou zátěž pro zdravotnický personál. Lze doporučit:

Zavedení podpůrných programů: Zdravotnická zařízení by měla nabízet programy na podporu well-beingu, zahrnující například relaxační techniky, psychologickou pomoc nebo možnosti konzultací.

Školení na zvládání stresu: Speciální školení zaměřená na zvládání stresu a psychickou podporu zaměstnanců by měla být pravidelnou součástí vzdělávacích programů.

5.16 Zavedení a formalizace pravidel

Je nezbytné zavést jednotná, formálně kodifikovaná pravidla pro péči o chráněné osoby. Tato pravidla by zahrnovala:

Jednoznačné definování postupů: Pravidla by měla jednoznačně popisovat postupy při poskytování zdravotní péče, zajištění bezpečnosti a ochrany citlivých dat.

Spolupráce s bezpečnostními složkami: Jasně stanovené postupy by zahrnovaly i komunikační protokoly mezi zdravotnickým personálem a ochrankou, aby byla zajištěna koordinovaná a hladká spolupráce.

Digitální protokoly: Zavedení digitalizovaných protokolů, které by byly snadno dostupné všem členům zdravotnického týmu a mohly by být rychle aktualizovány v případě změny bezpečnostních pravidel.

5.17 Zajištění rovnosti v přístupu ke zdravotní péči

Preferenční péče o chráněné osoby by měla být aplikována pouze v případě, kdy je to nezbytné z důvodu ochrany bezpečnosti nebo soukromí. Doporučení zahrnují:

Transparentní pravidla pro preferenční péči: Jasně definované podmínky pro poskytování preferenční péče, aby byl zajištěn rovný přístup ke zdravotní péči pro všechny pacienty, kromě situací, kdy to vyžadují bezpečnostní důvody.

Komunikace s veřejností: Transparentní komunikace o důvodech preferenční péče, aby se předešlo pocitu diskriminace a zachovala důvěra ve zdravotnický systém

Komunikace s chráněnou osobou: Transparentní nastavení pravidel komunikace vůči veřejnosti nebo médiím.

5.18 Zavedení právního rámce a standardizace ochrany dat chráněných osob

Právní rámec pro ochranu dat chráněných osob by měl být jasně definován a měl by zahrnovat odpovědnosti zdravotnických zařízení a poskytovatelů služeb. Doporučení zahrnují:

Zavedení jednotných pravidel: Vytvoření legislativního rámce pro ochranu dat chráněných osob, včetně jasného stanovení odpovědností za porušení ochrany dat a příslušných sankcí.

Pravidelné audity a hlášení incidentů: Povinnost zdravotnických zařízení provádět pravidelné audity zabezpečení dat a hlásit případné incidenty s ohledem na ochranu citlivých informací.

5.19 Cibulovitý princip bezpečnostních opatření: Víceúrovňová ochrana dat

Tento model bezpečnostních opatření zahrnuje více vrstev, kde každá další vrstva kompenzuje případné selhání vrstvy předchozí. Doporučení zahrnují:

Vícevrstvá ochrana dat: Implementace šifrování, vícefaktorové autentizace, zabezpečení sítí a pravidelného monitoringu přístupů jako jednotlivých vrstev ochrany včetně pravidelné aktualizace nových bezpečnostních opatření v návaznosti na pravidelně prováděnou analýzu rizik. **Zásadním pravidlem je, aby v případě selhání jednoho bezpečnostního opatření existovala minimálně další 2 nezávislá bezpečnostní opatření, která jsou schopna ho kontinuálně nahradit.**

5.20 Ověřování dodavatelů a třetích stran

Zdravotnická zařízení musí pečlivě kontrolovat bezpečnostní protokoly svých dodavatelů, kteří mají přístup k citlivým datům. Doporučení zahrnují:

Pravidelné audity: Provádění pravidelných auditů a kontrol bezpečnostních standardů dodavatelů a třetích stran.

Omezený přístup: Přísná omezení přístupu externích partnerů k citlivým datům, která by byla povolena pouze za jasně stanovených podmínek.

Zpracovatelské smlouvy: Zavedení bezpečnostních certifikací pro dodavatele a vytvoření technických a organizačních opatření, která budou vnořena do závazných smluvních podmínek zabezpečených vysokými sankcemi v případě jejich porušení.

5.21 Zvýšení ochrany citlivých dat ve velkých datových souborech (big data)

S nárůstem objemu dat je důležité zajistit jejich adekvátní ochranu při správě a analýze velkých datových souborů, ve kterých budou data chráněných osob. Doporučení zahrnují:

Anonymizace dat: Použití anonymizačních a šifrovacích technik pro ochranu informací a dat chráněných osob, zejména při jejich zpracování a analýze v rámci velkých datových projektů.

Bezpečnost při přenosu dat: Implementace technologií, které zajistí bezpečný přenos dat mezi různými zdravotnickými zařízeními, aby se snížilo riziko úniků během jejich sdílení.

6 Diskuse a hlavní přínosy disertační práce

Diskuse výsledků disertační práce se zaměřuje na kritické zhodnocení interpretovaných odpovědí respondentů získaných prostřednictvím polostrukturovaných rozhovorů a dotazníkového šetření, přičemž tyto odpovědi jsou analyzovány v kontextu současných poznatků a teorií v oblasti zdravotní péče, bezpečnostních opatření a kybernetické bezpečnosti. Diskuse se snaží porovnat získaná data s existujícími teoretickými modely, studiemi, zkušenostmi a praxí v jiných zemích, což umožňuje identifikaci hlavních výzev v oblasti nejen ochrany citlivých dat a kybernetické bezpečnosti. Dále se diskuse zaměřuje na navrhování konkrétních opatření pro zlepšení, která by mohla vést k vyšší úrovni bezpečnosti a efektivnější ochraně dat chráněných osob ve zdravotnických zařízeních zcela v duchu znění stanovených cílů práce.

6.1 Oblast poskytování zdravotní péče chráněným osobám

V úvodní části jak dotazníkového šetření, tak polostrukturovaných rozhovorů se autor zabýval samotnou existencí a komunikací pravidel pro péči o chráněné osoby. Výsledky jasně ukazují, že současný stav je zcela nevyhovující nebo že existují zásadní nedostatky v pravidlech. Tento problém není ojedinělý, neboť podobné nedostatky v komunikaci a zavádění pravidel byly zaznamenány i ve výzkumech provedených ve Spojených státech a Velké Británii, kde studie odhalily podobnou nejednotnost při zavádění a aplikaci speciálních pravidel pro specifické skupiny pacientů. Například studie z roku 2020 týkající se selhání komunikace ve zdravotnictví a dopadu na bezpečnost pacientů ukázala, že nedostatek formálních směrnic pro péči o rizikové pacienty vede k významným rozdílům v kvalitě poskytované péče napříč jednotlivými zařízeními, což může vést ke zvýšenému riziku selhání systému ochrany citlivých údajů a bezpečnosti pacientů.[189]

Výsledky analýzy odpovědí na první otázku **odhalují značnou nejednotnost** v přístupu českých zdravotnických zařízení k zavedení speciálních pravidel pro péči o chráněné osoby. Pouze 42,7 % respondentů potvrdilo existenci specifických pravidel, což naznačuje, že téměř polovina zařízení si je vědoma zvýšených nároků na bezpečnost a soukromí chráněných osob. Na druhé straně, 29,3 % zařízení žádná taková pravidla nemá, což může být způsobeno buď nedostatkem kapacity, nebo nedostatečným vnímáním potřeby těchto opatření. Tyto výsledky naznačují, že ne všechny instituce přikládají stejnou důležitost bezpečnosti a soukromí chráněných osob, což může vést k nerovnoměrné kvalitě péče a ochraně dat. Tento problém je

opět podobný s jinými výzkumy, které uvádějí, že zařízení, která nedisponují jasně stanovenými pravidly, často nejsou schopna zajistit dostatečnou ochranu dat ani bezpečnost pacientů[190].

Nedostatek jednotných pravidel je potvrzen i odpověďmi na druhou otázku, kde se ukazuje, že komunikace pravidel je často neformální a nesystematická. V mnoha případech jsou pravidla předávána ústně a ad hoc, což může vést k nejasnostem a různým interpretacím mezi zaměstnanci. Pouze v menším počtu zařízení jsou pravidla formalizována v interních směrnicích a pravidelně komunikována během školení a porad. Tento nedostatek formálního přístupu může zvyšovat riziko bezpečnostních incidentů a nesprávného zacházení s citlivými daty. Tento jev byl zmiňován i ve výzkumu provedeném v německých nemocnicích, kde se ukázalo, že neformální předávání pravidel vede ke zvýšenému riziku chyb a nepochopení základních bezpečnostních zásad.[191]

Zajímavé jsou výsledky třetí otázky, které odhalují nedostatečnou participaci personálu na tvorbě pravidel. Zatímco někteří odborníci iniciují ad hoc řešení na úrovni svých týmů, mnozí se na tvorbě pravidel vůbec nepodílí nebo necítí podporu ze strany vedení. Tento nedostatek participace může oslabit efektivitu implementace a ochotu dodržovat pravidla, což potvrzuje hypotézu č. 3 o nedostatečnosti současných technických a organizačních opatření. Tento jev není ojedinělý, jak ukazuje studie provedená v USA, kde bylo zjištěno, že nedostatečná účast personálu na rozhodovacích procesech ohledně bezpečnostních protokolů vede ke zvýšené pravděpodobnosti chyb a nedostatečnému dodržování standardů.[192]

Lze tedy konstatovat, že tato dílčí zkoumaná oblast není jednotně a centrálně uchopena a každé ze zdravotních zařízení si nastavení procesů řeší v ojedinělých případech samostatně anebo spíše vznikají ad hoc řešení jednotlivých vedoucích zaměstnanců, a to navíc bez vědomí jejich nadřízených nebo vedení zdravotnického zařízení. Výrazné rozdíly ve zmíněné oblasti mezi českými a zahraničními zařízeními, jak ukazují srovnávací data (viz Graf 1.1a a 1.2a), naznačují, že **česká zařízení zaostávají v zavedení specifických a formalizovaných pravidel pro chráněné osoby**. Tento fenomén je v souladu s výzkumem z Velké Británie, který odhalil, že zdravotnická zařízení, která postrádají formalizované postupy, často vykazují nedostatky v konzistenci péče a ochraně osobních údajů.[193]

V zahraničí až 81,1 % respondentů potvrdilo existenci pravidel, a navíc je zde větší důraz na formální komunikaci a strukturované přístupy, což přispívá k vyšší transparentnosti a jednotnosti v poskytování péče. Tato data naznačují, že česká zdravotnická zařízení by mohla

profitovat z přijetí praxe běžné v zahraničí, kde je formální dokumentace a pravidelná komunikace pravidel samozřejmostí. Tento trend podporují i další zahraniční studie, které ukazují, že formální pravidla nejenže zvyšují bezpečnost a ochranu dat, ale zároveň zlepšují celkovou efektivitu zdravotní péče.[194]

Na základě výše uvedených výsledků a srovnání lze doporučit několik dílčích kroků pro zlepšení současného stavu. Za prvé, je nezbytné zavést standardizovaná pravidla pro péči o chráněné osoby, která by byla formálně zakotvena v legislativních rámcích a interních směrnicích. Tato pravidla by měla být konzultována a vytvářena ve spolupráci s odborníky z praxe, aby odrážela reálné potřeby a výzvy, které zdravotnická zařízení čelí.

Dle názoru autora práce by významně přispělo alespoň **vytvoření základních standardů** ze strany příslušných ministerstev, které by poskytovatelé zdravotních služeb fakultního typu museli následně implementovat do svých vnitřních předpisů.

Tento přístup je v souladu se zahraničními praxemi, kde centrální regulace často přispívají k jednotnosti a vyšší kvalitě zdravotnických služeb, jak bylo prokázáno ve studiích z Kanady a Austrálie.[195] Takový krok by umožnil sjednocení postupů a praktik napříč poskytovateli zdravotních služeb v rámci České republiky a významně by přispěl ke zkvalitnění zdravotní péče nejen chráněným osobám, ale v konečném důsledku zejména běžným pacientům.

Zajištění systematické a efektivní komunikace těchto pravidel mezi zaměstnanci by mělo zahrnovat pravidelná školení, aktualizované metodické materiály a jasné procedury pro krizové situace nebo vznik nežádoucích událostí. Tento přístup se v mnoha zahraničních zdravotnických systémech osvědčil jako klíčový faktor pro zajištění vysoké úrovně bezpečnosti a kvality péče. Studie z Austrálie ukazuje, že zdravotnická zařízení, která pravidelně organizují školení a aktualizace směrnic pro krizové situace, dosahují o 25 % nižšího výskytu nežádoucích událostí ve srovnání se zařízeními, která tento přístup neaplikují.[196]

Transparentní komunikace nejen zvyšuje povědomí o bezpečnostních opatřeních, ale také posiluje důvěru zaměstnanců v jejich vlastní schopnost efektivně jednat v různých typech krizových či nežádoucích situací.

Za třetí, zvýšená participace zdravotnického personálu na tvorbě a revizi pravidel by mohla zajistit, že opatření budou praktická, efektivní a reflektující zkušenosti z každodenní, neustále se vyvíjející praxe. Tento participativní přístup by mohl vést k lepší akceptaci pravidel a snížení odporu vůči jejich implementaci. Výzkumy potvrzují, že participace zaměstnanců na tvorbě

pravidel výrazně zvyšuje jejich závazek k dodržování pravidel a přispívá ke zvýšení celkové úrovně péče.[197]

Otázky respondentům zkoumaly také přidělení jednoho hlavního ošetřujícího lékaře pro chráněné osoby. Z výsledků uvedených v grafu 1.5 vyplývá, že většina respondentů (56,1 %) preferuje, aby chráněná osoba měla určeno pouze jednoho hlavního ošetřujícího lékaře. Tento přístup je často považován za pozitivní z hlediska kontinuity péče a důslednosti ve sledování zdravotního stavu chráněné osoby. Podobné výsledky byly zaznamenány ve studiích provedených v USA a Německu, kde bylo prokázáno, že přítomnost jednoho klíčového lékaře nejen zvyšuje důvěru pacientů, ale také zlepšuje celkovou organizaci péče a efektivitu zdravotnických týmů[198]. Přítomnost jednoho klíčového lékaře umožňuje lepší koordinaci léčby a konzistentní komunikaci, což je důležité zejména u chráněných osob, kde může hrát roli zvýšená potřeba ochrany soukromí a bezpečnosti. Výsledky zahraničních respondentů ještě více podporují tento přístup (71,6 % souhlasících), což naznačuje, že v mezinárodním kontextu je trend centralizace péče ještě výraznější.

Na druhé straně, téměř třetina respondentů (27,4 %) se domnívá, že není nutné omezovat péči na jednoho hlavního ošetřujícího lékaře, což může odrážet potřebu flexibilního přístupu a možnost využití širšího spektra odborníků v závislosti na aktuálním zdravotním stavu chráněné osoby. Tento přístup je často opodstatněn argumentem, že **multidisciplinární tým může poskytnout komplexnější péči, zejména pokud pacient potřebuje specializované zákroky nebo konzultace**. V Kanadě se tento model více odborníků na jednoho pacienta ukázal jako efektivní při léčbě pacientů se složitými zdravotními problémy, avšak s jasně definovanou koordinací na úrovni vedení týmu.[199]

Dle zkušeností autora práce s péčí o chráněné osoby je téměř zásadní, aby měl pacient určeného jednoho hlavního nebo ošetřujícího lékaře. Tento lékař má nejen „historickou“ zkušenost s takovým pacientem, zná ho, zná jeho zdravotní stav a všechna ostatní úskalí, ale zejména může efektivně koordinovat případná konziliární vyšetření, včetně bezpečnostních opatření zdravotnického zařízení či ochranky. Je jistě výhodou z těchto důvodů, aby ty nejvíce rizikové chráněné osoby (zejména vrcholoví ústavní činitelé) měly jednoho hlavního ošetřujícího lékaře.

Výsledky dotazníkového šetření u chráněných osob ukazují, že pouze malá část chráněných osob (8,8 %) měla během hospitalizace přiděleného konkrétního lékaře, který se staral výhradně o ně. Většina respondentů (53,6 %) uvedla, že o ně pečovali střídající se lékaři. Tento přístup

může poukazovat na snahu efektivně využívat lékařské kapacity, ale zároveň může vést k problémům s kontinuitou péče a komunikací mezi zdravotníky. Kontinuita péče je obzvláště důležitá pro chráněné osoby, které mohou mít specifické zdravotní a bezpečnostní potřeby, jež vyžadují konzistentní a dobře koordinovaný přístup.

Dílčím výzkumným zájmem byla také oblast preferenční péče o chráněné osoby a s tím související etická dilemata, včetně organizační praxe. Z analýzy odpovědí respondentů na otázky týkající se kvality a rozsahu péče poskytované chráněným osobám **vyplývá velmi zajímavý rozpor mezi ideálním a skutečným stavem ve zdravotnických zařízeních**. Většina respondentů se shoduje na tom, že z hlediska lékařských standardů by měla být poskytována stejná kvalita péče všem pacientům, bez ohledu na jejich status. Tato shoda je v souladu s etickými principy rovnosti a spravedlnosti ve zdravotní péči, které jsou klíčovými hodnotami v oblasti lékařské etiky. Podle literatury jsou rovnost a spravedlnost v přístupu k lékařské péči univerzálně uznávanými etickými zásadami, které se uplatňují v různých zdravotnických systémech[200]. Výsledky dotazníkového šetření, kde 78,2 % respondentů nesouhlasí s preferenčním zacházením s chráněnými osobami, jasně odrážejí tuto etickou orientaci. *„U nestandardního pacienta je nezbytné postupovat standardně,“* zdůrazňuje respondent R2, čímž podtrhuje důležitost rovnosti v poskytování péče.

Navzdory těmto etickým ideálům je patrné, že v praxi dochází k odchylkám. Někteří respondenti (např. R5 a R9) přiznávají, že chráněné osoby často dostávají nadstandardní péči, což zahrnuje rychlejší přístup k vyšetřením, lepší ubytovací podmínky, a dokonce lepší mezilidský přístup ze strany personálu. Tento trend není ojedinělý, jak ukazují podobné výzkumy z jiných zemí, které zmiňují, že preferenční péče je v některých případech obhajována jako způsob, jak minimalizovat zátěž zdravotnického systému a zvýšit bezpečnost.[201] Jak uvádí respondent R3, *„VIP pacienti se pak mohou co nejrychleji vrátit ke své veřejné funkci,“* což reflektuje pragmatický přístup zdravotnických zařízení k minimalizaci bezpečnostních rizik a efektivnímu řízení kapacit.

Respondenti se vyjadřovali také k otázkám rovnosti a potenciální diskriminace. Zahraniční data ukazují podobné tendence, s mírně vyššími preferencemi pro rovný přístup (75,7 % respondentů nesouhlasí s preferenčním zacházením). Tato mezinárodní komparace naznačuje, že princip rovnosti ve zdravotní péči je univerzálně uznávanou hodnotou, přesto však existují kontexty, kde preferenční péče o chráněné osoby je vnímána jako přijatelná nebo nezbytná. V literatuře jsou podobné jevy často vysvětlovány jako důsledek rozdílných kulturních a organizačních

praktik, které ovlivňují rozhodování o přidělování zdrojů ve zdravotnických zařízeních[202]. Menšina respondentů (21,8 % v českém kontextu) souhlasí s tím, že chráněné osoby by měly mít nárok na odlišné zacházení, což naznačuje určitou míru tolerance vůči odchylkám od standardních postupů.

Důležitým faktorem, který přispívá k této toleranci, je vnímání bezpečnosti a potřeby zachování soukromí chráněných osob. Odpovědi respondentů ukazují, že zdravotnický personál je často konfrontován s tlakem na rychlé a diskrétní ošetření chráněných osob, což může být na úkor rovnosti v přístupu k péči. To je doloženo i daty, kde 22,1 % respondentů zmiňuje preferenční vyšetření pro chráněné osoby, což je běžná praxe jak v českých, tak v zahraničních zařízeních.

Velmi zajímavý podnět obsahovalo dotazníkové šetření v části, kde se respondenti mohli volně vyjádřit k problémům, které souvisí s poskytováním zdravotní péče chráněným osobám (otázka č. 6, první sekce). Zásadním etickým dilematem, které vyvstává z péče o chráněné osoby, je otázka rovnosti v přístupu ke zdravotní péči. Jak ukazuje graf 1.7, většina respondentů (78,2 %) nesouhlasí s tím, aby chráněné osoby měly nárok na odlišné jednání v rámci zdravotní péče. Tento nesouhlas reflektuje obecný názor, že **zdravotní péče by měla být poskytována spravedlivě, bez ohledu na sociální nebo politický status chráněné osoby**. Tento pohled potvrzují i výroky respondentů, například R3 uvádí, že: *„Z medicínského hlediska není legitimní, aby VIP osoby dostávaly lepší léky nebo léčbu. Mohou mít rychlejší přístup k péči nebo lepší pokoj, ale samotná lékařská péče by měla být stejná pro všechny.“*

Je nutné zmínit, že v zahraničí, zejména v západních zemích, Austrálii a Izraeli, je běžné, že existují placené „VIP programy“, které si mohou pacienti zaplatit a využívat nadstandardních služeb. Tento koncept, který zahrnuje placený přístup k lepším ubytovacím podmínkám, kratší čekací doby nebo personalizovanou péči, se stal součástí zdravotnických systémů, kde je kladen důraz na soukromý sektor. Například v Izraeli je rozšířen systém „Shiran VIP“, který umožňuje pacientům přístup k lepším zdravotním službám mimo rámec veřejného pojištění, což je považováno za legitimní způsob zajištění dodatečných zdrojů pro zdravotnická zařízení.[203] I to může být jedno z řešení pro Českou republiku, tedy vytvořit programy pro chráněné osoby, které by nebyly hrazeny z veřejného zdravotního pojištění. Jednalo by se o nadstandardní péči, za kterou by si pacienti platili, což by zároveň zachovalo princip rovnosti pro všechny ostatní pacienty financované z veřejných zdrojů.

Tyto zjištění naznačují potřebu zavedení jasných, transparentních a formálně kodifikovaných pravidel, která by regulovala poskytování péče chráněným osobám a zároveň respektovala princip rovnosti. Tento přístup je v souladu se zahraničními praxemi, kde formalizované protokoly a legislativní úpravy přispívají k lepší ochraně pacientů a zajištění rovnosti v přístupu ke zdravotní péči.[204] Jak navrhuje respondent R10, *„Kvalita péče by měla být stejná, ale v praxi často dochází k preferenčnímu zacházení,“* což reflektuje skutečnost, že teoretické ideály rovnosti jsou často vystaveny výzvám reálného světa. Zavedení formálních protokolů by mohlo přispět k eliminaci nesrovnalostí a zajistit, že preferenční péče je poskytována pouze v případech, kdy je to oprávněné bezpečnostními nebo zdravotními důvody.

Dále je doporučováno **posílení školení a vzdělávání zdravotnického personálu v oblasti etiky a práv pacientů**, aby bylo zajištěno, že každý pacient bude mít přístup ke kvalitní a spravedlivé péči. Jak ukazují studie z Velké Británie, pravidelná školení v oblasti etiky významně přispívají ke zlepšení rovného přístupu k péči, a to zejména v krizových situacích, kdy může být preferenční zacházení snadno zneužit.[205] Zajištění rovnosti v přístupu ke zdravotní péči nejen že posílí důvěru veřejnosti ve zdravotnický systém, ale také přispěje k celkové kvalitě péče. Transparentní pravidla, která odrážejí jak potřeby chráněných osob, tak princip rovnosti, mohou vytvořit základ pro spravedlivější a efektivnější poskytování zdravotní péče v českém i mezinárodním kontextu.

Dle názoru autora práce, který je podpořen i názory několika respondentů, je legitimní, aby chráněná osoba, myšleno nyní taková, která má ochranku, byla zdravotním zařízením ošetřena přednostně, a to z mnoha důvodů. Tím stěžejním je fakt, že přítomnost ochranky (viz dále v diskusi), výraznou měrou omezuje nebo narušuje činnosti zdravotnického zařízení, a to jak při ambulantním vyšetření, tak zejména při hospitalizaci. Z pohledu zdravotního zařízení se jedná o chráněnou osobu, tedy fyzickou osobu, které jsou poskytovány zdravotní služby a kterou je potřeba ze zákona chránit (jak fyzicky, tak virtuálně). To působí enormní tlak na zdravotní zařízení, jeho personál a na bezpečnostní procesy. Může docházet ke zvýšení rizika napadení personálu, zdravotnického zařízení nebo ke kyber útokům a snaze získat pacientská data. Tím dochází po dobu vyšetření nebo hospitalizace k enormnímu nárůstu rizika bezpečnostního incidentu ve zdravotnickém zařízení. Logickým řešením je tedy, co nejdříve takové riziko opět snížit, a to jak přijetím odpovídajících opatření, tak jeho co nejrychlejším vyřešením – propuštění chráněné osoby ze zdravotnického zařízení. Zde tedy lze vnímat jako legitimní, že „VIP pacient“, o kterém tak z bezpečnostních důvodů zdravotnické zařízení

rozhodne, může mít právo na přednostní nebo rychlejší vyšetření oproti běžným pacientům. Je nutné zdůraznit, že **tak lze postupovat pouze z bezpečnostních důvodů, nikoliv nikdy v oblasti kvality nebo rozsahu poskytované zdravotní péče**.

S tím souvisí také vyčleňování specifických prostor pro chráněné osoby, priorita jejich soukromí a bezpečnosti. Graf 1.6 ukazuje, že pouze 17,4 % českých respondentů potvrzuje, že jejich zařízení vždy vyčleňuje speciální místnosti pro chráněné osoby. Tento údaj kontrastuje s 21,1 % v zahraničních zařízeních, což naznačuje, že zahraniční zdravotnická zařízení mohou být lépe vybavena nebo více motivována k tomu, aby zajistila chráněným osobám speciální prostory pro jejich léčbu. Tento rozdíl může být způsoben rozdílnými prioritami v organizačních strukturách, přístupem k financování nebo legislativními rámci, které v zahraničních zemích vyžadují vyšší standardy péče o specifické skupiny pacientů.[206]

V českém kontextu 43,9 % respondentů uvádí, že konkrétní prostory jsou vyčleňovány pouze někdy, což může naznačovat selektivní přístup založený na individuálních potřebách pacientů. Tento selektivní přístup by mohl být důsledkem nedostatečných finančních a personálních kapacit v českých zdravotnických zařízeních, což vede k tomu, že jsou prostory poskytovány jen v případě, kdy jsou považovány za nezbytné. Podobný trend byl pozorován v Polsku, kde nedostatek specifických prostor pro chráněné osoby často závisí na momentálních možnostech nemocnic a ne na předem stanovených standardech.[207]

Zajímavým a potenciálně problematickým výsledkem je, že 20,6 % respondentů uvedlo, že neví, zda jsou v jejich zařízení vyčleňovány speciální prostory pro chráněné osoby. Tento nedostatek informovanosti může naznačovat nedostatečnou komunikaci nebo chybějící standardizaci postupů, včetně absence zkušeností. Tento nedostatek standardizace v českých zdravotnických zařízeních může vést k nejednotným praxím v rámci jednoho zařízení a v konečném důsledku k nesprávnému zacházení s chráněnými osobami. Podobné problémy byly identifikovány i ve Španělsku, kde nejasná pravidla a nedostatečná informovanost personálu vedly k rozdílným přístupům mezi jednotlivými nemocnicemi.[208]

Data z grafu 1.5a a 1.6a naznačují, že zahraniční zdravotnická zařízení kladou v této oblasti větší důraz na centralizaci péče a zajištění speciálních prostor pro chráněné osoby než jejich české protějšky. Vyšší podíl respondentů v zahraničních zařízeních, kteří preferují jednoho hlavního ošetřujícího lékaře (71,6 %), může reflektovat silnější kulturní a institucionální zaměření na personalizovanou péči. V některých zdravotnických systémech, jako je ten ve

Švýcarsku, je centralizace péče a vyčlenění specifických prostor pro chráněné osoby standardní praxí, která je v souladu s národními normami a doporučeními.[209] Vyčlenění specifických prostor ve většině zahraničních zařízení (62,1 % případů) naznačuje, že tamější systémy mají buď větší kapacity, nebo více strukturované přístupy k péči o chráněné osoby.

Pro české zdravotnické systémy by bylo **vhodné zvážit přijetí některých zahraničních praxí, které zdůrazňují potřebu centralizace péče a vyčlenění specifických prostor**. Tyto praktiky by mohly nejen zlepšit kontinuitu a kvalitu péče o chráněné osoby, ale také přispět k posílení důvěry pacientů ve zdravotnický systém a zvýšit pocit bezpečí a soukromí těchto jedinců.

Výsledky poukazují na **potřebu lepšího definování a standardizace pravidel pro přidělování hlavního ošetřujícího lékaře a vyčleňování specifických prostor pro chráněné osoby**. Flexibilita a možnost volby mezi centralizovaným a multidisciplinárním přístupem by měla být součástí standardů péče, aby bylo možné lépe reagovat na různé potřeby chráněných osob. Rovněž by mělo být zajištěno, že všechny zdravotnické zařízení budou mít jasné a efektivně komunikované protokoly týkající se péče o chráněné osoby, aby se snížila míra nejistoty a zajistila se konzistentní a kvalitní péče.

Analogicky lze uvést, že vyčlenění samostatných prostor pro hospitalizaci chráněné osoby je činěno zejména z bezpečnostních důvodů a mělo by být vždy konzultováno s ochrankou této osoby. Fakt, že v případech některé hospitalizace má tato osoba samostatný pokoj není projevem vyššího standardu poskytované péče, ale je důsledkem nutnosti efektivně zabezpečit její bezpečnost, což na pokoji, kde je více než 1 cizí pacient je obtížné. Navíc, docházelo by na druhou stranu k omezování a „obtěžování“ takového cizího pacienta.

Odpovědi respondentů na šestou otázku první sekce týkající se obecně problémů při hospitalizaci chráněných osob odhalují, že jedním z nejvýznamnějších problémů při péči o chráněné osoby je zajištění efektivní komunikace a koordinace mezi zdravotnickým personálem a bezpečnostními složkami, konkrétně ochrankou. Tato problematika byla opakovaně zmiňována respondenty, například R1 uvedl: *„Ochranka často přebírá iniciativu, což může vést k nedorozuměním a komplikacím v poskytování péče.“* Tento názor podporuje i R4, který poukazuje na skutečnost, že *„ochranka někdy klade přehnané požadavky, což může komplikovat práci lékařů.“* Tyto výroky naznačují, že role ochranky, přestože je nezbytná pro zajištění bezpečnosti, může někdy zasahovat do zdravotní péče a způsobovat konflikty s lékaři, kteří jsou zodpovědní za zdravotní rozhodnutí.

Tento problém je dále podpořen daty z grafu 1.8, kde 9,1 % respondentů uvedlo, že bezpečnostní opatření zasahují do chodu oddělení. Vyžaduje se tedy lepší definice kompetencí a odpovědností mezi zdravotnickým personálem a ochrankou, aby nedocházelo k narušení péče a k napětí mezi těmito skupinami. Doporučuje se zavést jasné protokoly pro interakci s ochrankou, které by zajistily, že prioritou zůstane zdraví a pohodlí pacienta, zatímco bezpečnostní opatření budou efektivně integrována do zdravotnických procesů.

Dalším klíčovým problémem identifikovaným respondenty je otázka ochrany soukromí a správy citlivých informací. R3 například uvádí: *„Zásadní problém vidím ve sdělování a ochraně utajovaných skutečností. Dále je těžké stanovit, za jakých podmínek je nebo není schopen výkonu.“* Tento výrok podtrhuje složitost rozhodování o tom, kdy a jak komunikovat zdravotní stav chráněné osoby, zejména když jsou na scéně politické nebo veřejné tlaky.

Graf 1.8 ukazuje, že 5,7 % respondentů identifikovalo utajení informací a obavy z jejich úniku jako jeden z problémů, což reflektuje potřebu zlepšení politiky ochrany dat. Podobné obavy byly zaznamenány i v zahraniční literatuře, kde výzkumy prokázaly, že nedostatečná ochrana zdravotních záznamů může vést k narušení důvěry pacientů a zvýšit riziko právních problémů pro zdravotnická zařízení.[210] Kromě toho, **zvýšený zájem médií a veřejnosti (11,4 % respondentů) komplikuje ochranu soukromí, což zvyšuje tlak na zdravotnický personál**. Tento tlak je obzvláště zřetelný v případech chráněných osob, kde je vysoce sledovaná péče, což dále zvyšuje požadavky na ochranu citlivých dat. Z výzkumného pohledu je tedy klíčové implementovat přísnější opatření pro ochranu citlivých dat, což zahrnuje školení personálu a zavedení sofistikovaných technických řešení pro ochranu elektronických zdravotních záznamů. Například v USA se v posledních letech zvýšilo zaměření na využívání šifrovacích technologií a dalších digitálních bezpečnostních opatření, aby se zajistilo, že zdravotní údaje jsou chráněny před únikem.[211]

Problematika stresu a nároků kladených na zdravotnický personál při péči o chráněné osoby je dalším často zmiňovaným problémem. R6 uvedl: *„Hlavním problémem je zvládání stresu a vysoké nároky na bezpečnost, které někdy mohou zasahovat do komfortu a kvality péče poskytované chráněným osobám.“* Tento faktor byl potvrzen i v zahraničních studiích, které identifikovaly zvýšenou fyzickou a psychickou zátěž personálu při péči o vysoce rizikové nebo chráněné pacienty, což vedlo ke zvýšené míře vyhoření a snížené kvalitě poskytované péče.[212] Tato výzva je potvrzena i grafem 1.8, kde 11,4 % respondentů zmínilo zvýšenou fyzickou a psychickou zátěž. Tyto nároky mohou vést k vyhoření zdravotnického personálu,

což negativně ovlivňuje kvalitu poskytované péče. Výzkum z Austrálie například uvádí, že dlouhodobý stres a nedostatek podpory ze strany vedení při péči o chráněné osoby významně zvyšuje riziko syndromu vyhoření mezi zaměstnanci.[213]

Existuje tedy potřeba zavést strategie na podporu well-beingu zdravotnického personálu, jako je školení zaměřené na zvládání stresu, a vytvoření podpůrných mechanismů, které pomohou zaměstnancům efektivněji zvládat nároky spojené s péčí o chráněné osoby. Dále by bylo vhodné zvážit zvýšení personálních kapacit, aby bylo možné lépe rozložit zátěž mezi více členů týmu.

Závěrečné shrnutí

Diskuse o péči o chráněné osoby ve zdravotnických zařízeních v České republice ukazuje na několik klíčových výzev a potřeb. Za prvé, je zřejmé, že současná péče o chráněné osoby často naráží na problémy spojené s koordinací a komunikací mezi zdravotnickým personálem a ochrankou. To může vést k nedorozuměním a narušení plynulosti zdravotnické péče, což může mít negativní dopad na pacienty. Za druhé, ochrana soukromí a citlivých informací o zdravotním stavu chráněných osob je dalším kritickým aspektem, který vyžaduje pečlivé zajištění. Zajištění adekvátního soukromí a ochrany dat není vždy jednoduché, zejména při zvýšeném zájmu médií a veřejnosti.

Další oblastí, kterou je třeba řešit, je podpora zdravotnického personálu. Péče o chráněné osoby může být psychicky i fyzicky náročná, a proto je nezbytné zajistit adekvátní podporu a školení, aby se personál cítil kompetentně a připraven čelit specifickým výzvám, které tyto situace přinášejí. Konečně, důležitým aspektem, který diskuse odhalila, je potřeba zachovat rovnost v přístupu ke zdravotní péči. Přestože mohou existovat situace, kdy je preferenční péče o chráněné osoby ospravedlnitelná, je nutné zajistit, aby tato praxe nevedla k diskriminaci ostatních pacientů a nebyla v rozporu s etickými standardy.

6.2 Oblast zajištění fyzické bezpečnosti hospitalizovaných chráněných osob

Z výsledků rozhovorů a dotazníků vyplývá, že odpovědnost za nastavení bezpečnostních opatření v rámci zdravotnických zařízení je relativně jasně definována a koncentruje se především na pozice ředitele zdravotnického zařízení a bezpečnostního ředitele. Všichni respondenti shodně označili bezpečnostního ředitele za klíčovou postavu v tomto procesu, což naznačuje vysokou míru specializace a důraz na bezpečnostní management v oblasti ochrany chráněných osob. Tento trend odpovídá i zahraničním studiím, které potvrzují, že bezpečnostní management ve zdravotnických zařízeních je stále více považován za specializovanou oblast

vyžadující technickou odbornost a schopnost strategického plánování.[214] Dle zkušeností autora práce je nezbytné, **aby bezpečnostní ředitel měl vymezenu jasnou odpovědnost za oblast odborné působnosti týkající se bezpečnosti hospitalizovaných chráněných osob a zejména, aby jeho role byla respektována**. Jinými slovy, aby se postupovalo standardně a například komunikace s ochrankou chráněné osoby probíhala právě přes bezpečnostního ředitele, pokud samozřejmě ředitel daného zdravotnického zařízení neurčí jinak a nenastaví jinou odpovědnou osobu z různých důvodů.

Opakující se zmínky o roli přednosty kliniky nebo ošetřujícího lékaře naznačují, že zatímco generální odpovědnost spočívá na úrovni zdravotnického zařízení, jednotlivé kliniky a oddělení mají také významnou míru autonomie při implementaci bezpečnostních opatření. Tento hierarchický model může být efektivní, neboť umožňuje přizpůsobení bezpečnostních protokolů specifickým potřebám daného oddělení a typu pacientů. Na druhou stranu může tento model vyžadovat silnou koordinaci a jasné komunikační kanály mezi bezpečnostním vedením a lékařským personálem, aby se předešlo nedorozuměním a zajistila se konzistence v aplikaci bezpečnostních opatření. Jak ukazuje výzkum v britských nemocnicích, nedostatečná komunikace mezi těmito klíčovými aktéry může vést k výrazným bezpečnostním rizikům, zejména při péči o zranitelné pacienty.[215]

Z porovnání českých a zahraničních dat vyplývá, že zahraniční zdravotnická zařízení kladou větší důraz na formalizované a specializované bezpečnostní struktury. V zahraničních zařízeních je odpovědnost za bezpečnost často svěřována vedoucímu oddělení bezpečnosti nebo bezpečnostnímu manažerovi, a to ve více než 50 % případů. Tento trend může odrážet vyšší úroveň specializace a profesionalizace bezpečnostních procesů v zahraničí, kde jsou bezpečnostní postupy považovány za integrální součást strategického řízení zdravotnických zařízení.[216] Dalším důležitým zjištěním je vysoký podíl odpovědnosti přisuzovaný řediteli zdravotnického zařízení, zejména v zahraničních zařízeních. Ředitel zdravotnického zařízení je často vnímán jako klíčová postava, která nese konečnou odpovědnost za bezpečnostní opatření. Tento přístup je logický, jelikož ředitel má obvykle nejvyšší autoritu a je schopen koordinovat mezi různými odděleními a externími subjekty, jako je policie nebo vojenská policie. Podobné modely byly pozorovány i ve zdravotnických zařízeních v Kanadě, kde ředitelé nesou klíčovou odpovědnost za koordinaci bezpečnostních opatření a jejich dodržování, přičemž jsou často zapojováni do pravidelných školení a aktualizací bezpečnostních protokolů.[217]

Přestože je odpovědnost za bezpečnost relativně jasně definovaná, některé odpovědi respondentů, kteří uvedli, že nevědí, kdo je za nastavení bezpečnostních opatření odpovědný, poukazují na potenciální mezery v komunikaci nebo vnitřních postupech. Tento nedostatek informovanosti by mohl ohrozit efektivitu a rychlost reakce v situacích, kdy je vyžadováno rychlé rozhodování a implementace bezpečnostních opatření a opět je to podnět pro zlepšení praxe.

Významná byla také otázka vlivu přítomnosti ochranky na procesy ve zdravotnických zařízeních. Na základě odpovědí respondentů a dat z dotazníků lze konstatovat, že přítomnost ochranky chráněných osob ve zdravotnických zařízeních je vnímána převážně negativně, zejména pokud jde o její vliv na běžný chod zdravotnického zařízení. Všichni respondenti se shodují, že **ochranka narušuje standardní procesy a vyžaduje úpravy běžných postupů**. Omezení přístupu k určitým prostorám a zpomalení běžného provozu jsou nejčastěji zmiňované problémy, které mají přímý dopad na efektivitu práce a dostupnost péče pro ostatní pacienty.

Respondenti zdůrazňují, že přítomnost ochranky často způsobuje stres mezi zdravotnickým personálem, který se musí přizpůsobovat bezpečnostním požadavkům, jež někdy zasahují do samotného procesu poskytování zdravotní péče. Například R1 poznamenal: *„Ochranka může být velmi rušivým prvkem. Zpomaluje procesy a někdy komplikuje komunikaci mezi zdravotnickým personálem.“* Tento názor ilustruje potřebu najít rovnováhu mezi zajištěním bezpečnosti chráněných osob a zajištěním efektivního fungování zdravotnického zařízení.

Také je evidentní, že činnost ochranky omezuje ostatní pacienty, kteří jsou často blokováni od přístupu k určitým místům, což způsobuje zpoždění v jejich ošetření. R5 uvádí: *„Ochranka často blokuje určité oblasti, což ztěžuje přístup ostatním pacientům a někdy i personálu.“* Toto omezení může vést k negativním dopadům na komfort a kvalitu poskytované péče pro ostatní pacienty, což může dále vést k nespokojenosti jak pacientů, tak i zdravotnického personálu.

Výsledky ukazují jednoznačný nesouhlas respondentů s přítomností ochranky na operačních sálech nebo při intimních zákrocích, jako je například kolonoskopie. Všichni respondenti se shodují, že **přítomnost ochranky v těchto situacích není vhodná, protože by mohla narušit sterilní prostředí a ovlivnit výkon lékařů**. Tento postoj není ojedinělý a **odpovídá zahraničním studiím**, které také potvrzují negativní vliv přítomnosti neodborného personálu během chirurgických zákroků nebo citlivých lékařských vyšetření. Studie z USA uvádí, že přítomnost bezpečnostního personálu v chirurgických prostorách může zvýšit riziko infekcí

a narušit zaměření týmu na samotný zákrok, čímž snižuje efektivitu a bezpečnost péče.[218] R3 konkrétně upozorňuje: *„Přítomnost ochranky v operačním sále nebo při kolonoskopii považuji za nevhodnou. Může to ovlivnit průběh zákroku a narušit sterilní prostředí.“*

Respondenti také zmiňují obavy z ohrožení bezpečnosti pacientských dat a soukromí pacientů. Přítomnost ochranky na takto citlivých místech může narušit vztah mezi lékařem a pacientem a ovlivnit důvěru pacientů v kvalitu poskytované péče. Tyto obavy jsou zcela na místě, jak potvrzuje výzkum v britských nemocnicích, který ukázal, že zbytečná přítomnost neodborného personálu během lékařských zákroků může vést ke snížení důvěry pacientů a k narušení důvěrnosti jejich údajů.[219] **Všichni respondenti by souhlasili s přítomností ochranky maximálně v předsálí, ale nikoli přímo na operačním sále nebo při intimních vyšetřeních**, což je přístup, který je rovněž doporučován v odborné literatuře. Výzkum z Německa například navrhuje, aby byla přítomnost ochranky omezena na prostory mimo operační místnost, aby se zachovala důvěrnost a integrita lékařských postupů.[220]

S ohledem na výše uvedené lze souhlasit s doporučením omezit přítomnost ochranky pouze na předsálí, což by minimalizovalo narušení operačního prostředí a zároveň poskytlo dostatečnou úroveň ochrany. Tento přístup je v souladu s nejlepšími mezinárodními standardy pro ochranu pacientů a zajištění bezpečnosti ve zdravotnických zařízeních, kde je důležité vyvážit potřebu bezpečnosti a respektování soukromí pacientů.

Srovnání českých a zahraničních dat ukazuje, že zahraniční zdravotnická zařízení mají tendenci mít lépe integrované a formalizované postupy pro spolupráci s ochrankou, což může přispět k minimalizaci negativních dopadů na provoz. Zahraniční respondenti častěji uvádějí přítomnost ochranky jako neodmyslitelnou součást každodenního provozu, zatímco v českém kontextu je přítomnost ochranky často vnímána jako narušující element. Tento rozdíl může být způsoben rozdílnými kulturními přístupy k bezpečnosti a organizaci zdravotnických zařízení.

Diskuse k zajištění fyzické bezpečnosti personálu při přítomnosti chráněných osob ve zdravotnických zařízeních vede k nutnosti řešení zásadních nedostatků. Odpovědi respondentů na čtvrtou otázku ve druhé sekci, zaměřené na opatření pro zajištění fyzické bezpečnosti personálu při péči o chráněné osoby, odhalují závažný nedostatek specifických opatření v této oblasti. Naprostá většina respondentů uvedla, že žádná speciální opatření pro fyzickou bezpečnost personálu nejsou zavedena a spoléhá se pouze na běžné bezpečnostní postupy. Tento fakt naznačuje podceňování rizik, která mohou vznikat při hospitalizaci chráněných osob,

zejména v případech, kdy jsou přítomny i bezpečnostní složky. Podobná zjištění byla zaznamenána i v zahraničních studiích, které varují před tím, že nedostatečné zajištění bezpečnosti personálu v prostředí s vysokým rizikem může vést k narušení poskytované péče i k ohrožení personálu samotného.[221]

Zdravotnický personál je často vystaven vyššímu riziku během péče o chráněné osoby, zejména pokud se jedná o osobnosti s významným veřejným profilem nebo osoby, které by mohly být terčem bezpečnostních hrozeb. Přítomnost ochranky, jak bylo diskutováno v předchozích otázkách, může narušovat standardní provoz zdravotnického zařízení a přinášet dodatečné komplikace. Nicméně absence specifických opatření pro zajištění fyzické bezpečnosti personálu je alarmující, neboť ignoruje potenciální rizika, která mohou ohrozit nejen zdravotnický personál, ale i ostatní pacienty a samotné chráněné osoby. V zahraničí se již začínají prosazovat bezpečnostní protokoly zaměřené na prevenci rizik při hospitalizaci „VIP osob“, zejména prostřednictvím specializovaných bezpečnostních týmů, které fungují ve spolupráci s lékařským personálem a poskytují jim podporu v krizových situacích.[222]

Respondent R1 otevřeně přiznává: *„Žádná, nikdy jsem o tom neslyšel, že by se to řešilo,“* což poukazuje na to, že v některých zařízeních tato otázka nebyla vůbec adresována. Tato absence ochrany personálu může vést k situacím, kdy zdravotníci nemají jasné pokyny, jak se chovat v krizových situacích, což může vést k neefektivnímu a potenciálně nebezpečnému jednání. Výzkumy provedené v amerických nemocnicích potvrzují, že jasně definované krizové protokoly a školení zdravotnického personálu vedou k efektivnějším reakcím na krizové situace a snižují rizika spojená s bezpečností pacientů i personálu.[223]

Z výzkumného hlediska tato situace naznačuje potřebu vyvinout a implementovat specifické bezpečnostní protokoly zaměřené na ochranu zdravotnického personálu při hospitalizaci chráněných osob. Tato opatření by měla být součástí širší strategie zajištění bezpečnosti ve zdravotnických zařízeních, zahrnující i ochranu ostatních pacientů a samotných chráněných osob. Doporučení ze zahraničí zahrnují pravidelné školení zdravotnického personálu v oblasti krizového řízení, spolupráci s externími bezpečnostními složkami a zavedení jasných komunikačních kanálů mezi lékaři, zdravotními sestrami a bezpečnostními týmy.[224] Mělo by se zvážit školení zdravotnického personálu v oblasti krizového řízení a reakcí na možné bezpečnostní incidenty, což by zvýšilo úroveň bezpečnosti a zároveň posílilo důvěru personálu ve vlastní schopnosti zvládat krizové situace.

Výsledky z dotazníků také podporují potřebu těchto opatření. Ve většině zdravotnických zařízení nejsou zavedena specifická opatření pro fyzickou bezpečnost personálu, přičemž 57,9 % respondentů uvedlo, že se spoléhají na běžné bezpečnostní postupy. Pouze menšina zařízení využívá více strážných nebo spolupracuje s policií, což naznačuje, že některá zařízení jsou lépe vybavena pro zvládání potenciálních bezpečnostních hrozeb.

Při srovnání se zahraničními daty se ukazuje, že zahraniční zdravotnická zařízení ještě méně často zavádějí specifická opatření pro zajištění fyzické bezpečnosti personálu. V zahraničních zařízeních 73,7 % respondentů uvedlo, že žádná specifická opatření neexistují. Toto zjištění může naznačovat, že přístup k zajištění bezpečnosti je v zahraničí podobně podceňován nebo se spoléhá na jiné formy ochrany, které nejsou považovány za specifické bezpečnostní protokoly.

Závěrečná otázka sekce druhé týkající se problémů spojených s fyzickou bezpečností při hospitalizaci chráněných osob přinesla, vlivem volných odpovědí, řadu poznatků. Odpovědi respondentů odhalují, že tato oblast je často podceňována a nedostatečně řešena. Přestože respondenti vyjadřují různé názory a zkušenosti, několik klíčových problémů se objevuje opakovaně: nutnost zajistit dostatečné soukromí pro chráněné osoby, minimalizace vlivu bezpečnostních opatření na léčebné procesy a potřeba efektivní koordinace mezi zdravotnickým personálem a ochrankou.

Hlavní problémy s fyzickou bezpečností:

- Zajištění soukromí a prevence úniku informací: Jedním z největších problémů je podle respondentů zajištění dostatečného soukromí chráněných osob a prevence úniku citlivých informací. Respondent R2 například zdůrazňuje: *„Nejčastějším problémem je zajištění dostatečného soukromí pro chráněné osoby, aby nedocházelo k úniku informací a fotografií.“* Tento problém je dále komplikován mediálním zájmem, který může narušit klidné a bezpečné prostředí zdravotnického zařízení a vytvořit tlak na personál.
- Narušení léčebných procesů: Přítomnost ochranky a nutnost zvýšené bezpečnosti často vedou k narušení běžných zdravotnických procesů. Několik respondentů zmiňuje, že bezpečnostní opatření mohou komplikovat léčebné procesy a vést ke zpožděním nebo omezením v péči o ostatní pacienty. Jak R3 podotýká: *„Musíme zajistit, aby ochranka*

nezdržovala lékařské výkony a zároveň aby byla zajištěna maximální diskrétnost a soukromí.“

- Koordinace mezi zdravotnickým personálem a ochrankou: Dalším významným problémem je koordinace mezi zdravotnickým personálem a bezpečnostními složkami. Jak uvádí R7, *„Nejčastějším problémem je koordinace mezi zdravotnickým personálem a ochrankou, což může vést ke zpoždění nebo narušení péče.“* Nedostatečná koordinace může vést k nejasnostem, zbytečným zpožděním a v některých případech i k rizikovým situacím pro pacienty a personál.

Zjištění z dotazníků a jejich výsledky podporují tato zjištění. Z 28 respondentů dotazníku označilo 25 % médií a zvýšený zájem veřejnosti za nejčastější problém, což potvrzuje, že přítomnost médií může negativně ovlivnit bezpečnostní a provozní postupy zdravotnického zařízení. Tento jev není výjimečný ani v mezinárodním kontextu, kde studie ukazují, že zvýšený mediální tlak může vést k narušení běžného provozu nemocnic a ke zvýšené míře stresu mezi zdravotnickým personálem. Například ve Velké Británii bylo zjištěno, že přítomnost médií při hospitalizaci vysoce postavených osobností výrazně ztěžuje dodržování standardních bezpečnostních opatření, což vede ke zpožděním a vyšším nákladům na provoz.[225]

Bezpečnostní opatření byla dalším často zmiňovaným problémem (21,4 %), což naznačuje, že současné bezpečnostní postupy nemusí být dostatečně efektivní nebo správně implementovány. Tento problém vyvstává zejména v situacích, kdy personál nemá jasné pokyny ohledně bezpečnostních protokolů při péči o chráněné osoby. Podobné zjištění bylo zaznamenáno ve studiích provedených v USA, kde nedostatečné školení personálu a špatná koordinace mezi bezpečnostními týmy vedly k selhání při zajištění bezpečnosti vysoce rizikových pacientů.[226] Tyto výsledky zdůrazňují potřebu zlepšit školení a komunikaci mezi zdravotnickým personálem a ochrankou, aby byla zajištěna efektivní spolupráce a eliminace rizik. Zvýšení kvality školení by mohlo přispět k vyšší efektivitě při zvládání krizových situací a posílit bezpečnost v nemocnicích.

Závěrečné shrnutí

Druhá sekce výzkumu se zaměřila na fyzickou bezpečnost a bezpečnostní opatření při hospitalizaci chráněných osob ve zdravotnických zařízeních. Výsledky ukazují, že přítomnost ochranky významně ovlivňuje běžný chod zdravotnických zařízení, a to především negativně. Respondenti opakovaně uváděli, že přítomnost ochranky způsobuje narušení standardních

procesů, omezuje přístup jiných pacientů k vyšetřením a vyžaduje častou koordinaci mezi zdravotnickým personálem a bezpečnostními složkami.

Navzdory tomu, že fyzická bezpečnost chráněných osob je prioritou, nedostatek specifických protokolů a postupů pro zajištění fyzické bezpečnosti personálu je značný. Přítomnost ochranky bez jasně definovaných pravidel vede k situacím, kdy je obtížné najít rovnováhu mezi ochranou chráněných osob a zajištěním plynulého poskytování péče ostatním pacientům. Rovněž je zřejmé, že nedostatečná pozornost je věnována ochraně zdravotnického personálu, který může být vystaven rizikům spojeným s hospitalizací vysoce rizikových skupin.

Zvláštní důraz by měl být kladen na zajištění soukromí a diskrétnosti, aby se předešlo úniku citlivých informací. Odpovědnost za nastavení a implementaci bezpečnostních opatření je často rozdělena mezi více subjektů, což může vést k nejasnostem a nedostatku jednotného přístupu.

6.3 Oblast virtuální a kybernetické bezpečnosti hospitalizovaných chráněných osob

6.3.1 Ověření hypotézy č. 1

Na základě odpovědí respondentů týkající se slabých míst a rizik v ochraně dat je zřejmé, že **hlavními faktory jsou především lidský faktor a jen částečně zastaralé technologické systémy**. Jednotlivé odpovědi ukazují na opakující se problémy, které zahrnují nedostatečné školení personálu v oblasti kybernetické bezpečnosti, což vede k neznalosti a podcenění rizik. Tento fenomén není omezen pouze na český kontext. Mezinárodní výzkumy ukazují, že podobné problémy se vyskytují i ve zdravotnických zařízeních v USA a Evropě, kde zaměstnanci často nedodržují zavedené bezpečnostní postupy, čímž zvyšují riziko úniku dat[227]. Respondenti zdůrazňují, že **zaměstnanci často nedodržují bezpečnostní postupy**, což zvyšuje riziko úniku dat. Tento faktor je významný především v kontextu kybernetických hrozeb, jako jsou phishing nebo sociální inženýrství, kde se útočníci snaží zneužít nepozornosti nebo nedostatečné informovanosti personálu. **Nedostatečné školení zvyšuje riziko úspěšných útoků** založených na technikách sociálního inženýrství, jak potvrzují studie zaměřené na kybernetickou bezpečnost ve zdravotnictví.[228]

Vedle lidského faktoru respondenti identifikovali také technologickou zastaralost jako problém. Zastaralé systémy nejsou schopny efektivně chránit data před moderními kybernetickými hrozbami. **Chybí adekvátní ochranná opatření**, jako jsou pokročilé antivirové systémy,

firewally nebo šifrování, které by zajišťovaly vyšší úroveň ochrany dat. Zastaralé technologie mohou být snadno prolomeny a nejsou schopny adekvátně detekovat a reagovat na pokusy o neoprávněný přístup. Tento problém byl zaznamenán i v jiných zemích, kde zastaralé technologie přispěly k několika významným útokům na zdravotnická zařízení, což vedlo k masivním únikům citlivých dat.[229]

Tyto zjištění naznačují, že hypotéza č. 1, která tvrdí, že nejčastější slabá místa v oblasti bezpečnosti pacientských dat anebo informací při hospitalizaci chráněných osob jsou způsobena nedostatečnou implementací aktuálních bezpečnostních technologií a postupů, není plně podporována. Naopak, ukazuje se, že hlavním problémem je lidský faktor – konkrétně nedostatečné školení, neznalost bezpečnostních rizik mezi personálem, nedbalost a zcela zásadní lidské selhání. Zahraniční studie zaměřené na kybernetickou bezpečnost ve zdravotnictví rovněž potvrzují, že **lidské selhání je často větším rizikem než technologická zastaralost, protože i ty nejpokročilejší bezpečnostní systémy mohou selhat, pokud nejsou správně využívány.**[230] Zatímco technologické vybavení hraje důležitou roli, klíčovým problémem je spíše nedostatek vědomostí a zodpovědnosti u zaměstnanců než pouze technická zastaralost.

Tato zjištění vedou k zamítnutí hypotézy č. 1, protože i kdyby byly implementovány moderní bezpečnostní technologie, bez adekvátního školení a povědomí personálu by nebyly schopny účinně chránit data.

Pro shrnutí klíčových citací týkajících se lidského faktoru jako hlavní hrozby a rizika v oblasti bezpečnosti pacientských dat chráněných osob můžete použít následující výroky respondentů:

R1: *„Podle mě jednoznačně selhání lidského faktoru na prvním místě a dále nedostatečně vyspělé systémy, které nejsou schopny čelit jak kyber útokům, tak zneužití zevnitř.“*

R2: *„Největší riziko vidím v lidském faktoru, kdy personál není dostatečně proškolen v oblasti kybernetické bezpečnosti.“*

R3: *„Slabým místem je jednoznačně lidský faktor. Zaměstnanci často nedodržují bezpečnostní postupy, což může vést k únikům dat.“*

R5: *„Hlavním problémem je lidský faktor, kdy personál často podceňuje bezpečnostní opatření.“*

R7: *„Slabé místo je určitě v lidském faktoru. Zaměstnanci často nejsou dostatečně informováni o důležitosti ochrany dat.“*

R9: *„Největší riziko vidím v lidském faktoru a zastaralých systémech. Personál často není dostatečně proškolen a technologie nejsou dostatečně zabezpečené.“*

Tyto citace jasně demonstrují, že respondenti považují lidský faktor za klíčové riziko pro bezpečnost pacientských dat, přičemž upozorňují na nedostatečné školení a povědomí zaměstnanců o důležitosti ochrany citlivých informací.

6.3.2 Ověření hypotézy č. 2

Výsledky jasně ukazují, že specifická rizika virtuální bezpečnosti pro pacienty se statutem chráněné osoby jsou podstatně vyšší než pro běžné pacienty. **Respondenti opakovaně zdůrazňovali, že únik dat chráněných osob může vést k vážným politickým a bezpečnostním důsledkům, zatímco únik informací běžných pacientů má obvykle omezenější dopad, zejména na osobní úrovni.**

Například odpovědi respondentů na otázku týkající se specifických rizik virtuální bezpečnosti u pacientů se statutem chráněné osoby ve srovnání s běžnými pacienty jednoznačně poukazují na to, že tato rizika jsou u chráněných osob výrazně vyšší. R1 shrnuje tento rozdíl slovy: *„Data VIP osob by měla být chráněna mnohem přísněji. V případě úniku informací o zdravotním stavu běžného pacienta je dopad omezený na jeho osobní život, zatímco u VIP osoby může mít únik informací dalekosáhlé politické a bezpečnostní důsledky.“* Tento názor je opakovaně podporován dalšími respondenty, kteří zmiňují potenciální využití těchto informací k politickým, ekonomickým nebo bezpečnostním účelům. Například R3 zdůrazňuje: *„U VIP osob je riziko úniku dat mnohem vyšší, protože tyto informace mohou být zneužity k ovlivnění veřejného mínění nebo politických rozhodnutí.“*

Tato rizika jsou zdůvodněna nejen vyšší hodnotou informací spojených s chráněnými osobami, ale také jejich potenciálním dopadem na širší veřejnost a státní záležitosti. Únik zdravotních dat vysoce postavených osob může vést k destabilizaci, ohrožení národní bezpečnosti a k cíleným útokům na tyto osoby. Toto riziko je zcela reálné, jak ukazuje zahraniční výzkum zaměřený na kybernetické útoky na politické činitele a vojenský personál, kde únik zdravotních informací může být zneužit pro vydírání, kompromitaci nebo dokonce pro plánování útoků.[231] R5 tuto hrozbu popisuje konkrétně: *„Riziko je mnohem vyšší, protože data VIP osob mohou být použita proti nim. Zdravotní informace by mohly být zneužity ke kompromitaci*

těchto osob nebo k vydírání.“ Tento postoj je v souladu se studií provedenou v USA, která rovněž potvrzuje, že únik zdravotních dat osob ve veřejných funkcích může mít dalekosáhlé politické a bezpečnostní dopady.[232]

Z pohledu autora práce je toto zjištění zásadní, neboť jasně ukazuje, že v současném kontextu války na Ukrajině a v Izraeli je nezbytné vnímat fakt, že **chráněné osoby, mezi které řadíme i příslušníky ozbrojených sil, je nutné chránit oproti běžným pacientům více**. Současné konflikty v těchto regionech odhalily, že informace o zdravotním stavu klíčových osob mohou být využity protivníky k oslabení jejich pozic nebo ke strategickým manévrům. Jak ukázaly kybernetické útoky na ukrajinské zdravotnické systémy, úniky zdravotních dat mohou být součástí širších destabilizačních strategií, které mají přímý dopad na vedení konfliktů a morálku armád.[233] Proto je klíčové, aby zdravotnická zařízení poskytující péči chráněným osobám zavedla přísná opatření zaměřená na ochranu těchto citlivých informací, a to nejen z pohledu technologického, ale také z pohledu lidského faktoru.

Hypotéza č. 2 je zamítnuta, protože rizika spojená s virtuální bezpečností pacientů se statutem chráněné osoby jsou prokazatelně vyšší a komplexnější než u běžných pacientů, což vyžaduje specifická a pokročilá opatření k jejich efektivnímu zvládání.

6.3.3 Ověření hypotézy č. 3

Z odpovědí jasně vyplývá, že ačkoli jsou ve zdravotnických zařízeních implementována určitá technická a organizační opatření, tato opatření nejsou považována za dostatečně robustní, aby adekvátně chránila citlivá data pacientů se statutem chráněné osoby.

Respondenti poukazují na nutnost zavádět přísnější a specifičtější opatření, která jdou nad rámec standardních bezpečnostních protokolů. Například R1 uvádí: *„Používají se například fiktivní rodná čísla nebo jména, aby byla data a anamnéza lépe chráněna.“* Tento přístup naznačuje, že běžná opatření pro ochranu osobních údajů nejsou vnímána jako dostatečně bezpečná. Podobné postupy, jako je pseudonymizace nebo anonymizace dat, jsou již implementovány v některých zahraničních zdravotnických systémech, kde byla prokázána jejich účinnost při ochraně citlivých údajů před neoprávněným přístupem.[234] Tento přístup umožňuje chránit identitu pacientů, zejména v případech, kdy by jejich zdravotní stav mohl být zneužit ke kompromitaci.

Respondenti rovněž zdůrazňují nutnost používání papírové dokumentace, což je považováno za bezpečnější variantu ochrany citlivých dat, zejména v případě vysoce postavených osob.

Tento názor reflektuje obavy z kybernetických hrozeb, kdy elektronická data mohou být zranitelnější vůči útokům. I když papírová dokumentace může snížit riziko kybernetických útoků, je důležité uvážit, že fyzické uchovávání dat přináší vlastní rizika spojená s jejich ztrátou nebo neoprávněným přístupem.[235] Proto by tento přístup měl být kombinován s dalšími moderními technickými opatřeními.

Další respondenti, jako R4, doporučují využití šifrování a uchovávání dat na zabezpečených serverech, doplněné o pravidelné aktualizace bezpečnostních protokolů a školení personálu: *„Navrhoval bych využití šifrování, uchovávání dat na zabezpečených serverech, používání fiktivních osobních údajů a v případě vysoce citlivých informací i přechod na papírovou dokumentaci.“* Tato doporučení jsou v souladu s mezinárodními standardy pro ochranu citlivých zdravotních údajů, které zahrnují komplexní bezpečnostní opatření včetně šifrování a omezeného přístupu.[236] Šifrování dat je klíčové zejména v kontextu rostoucího množství kybernetických útoků na zdravotnická zařízení, kde útočníci často cílí na nechráněná nebo slabě zabezpečená data.

Celkově odpovědi respondentů naznačují, že současná opatření nejsou dostatečná, což znamená, že je nutné neustále přizpůsobovat a zlepšovat technické i organizační postupy ochrany dat. Implementace pokročilých metod, jako je šifrování, pseudonymizace, fyzická ochrana dat a omezení přístupu, je klíčová. Dále je nezbytné zajistit pravidelnou aktualizaci těchto opatření a nepřetržité školení zdravotnického personálu, aby byla zajištěna maximální bezpečnost dat. V souladu s výzkumy, které ukazují, že pravidelná aktualizace a školení výrazně zlepšují efektivitu ochrany citlivých dat, lze očekávat, že tato opatření povedou ke zvýšení úrovně zabezpečení.[237]

Rovněž odpovědi respondentů na otázky týkající se ochrany dat chráněných osob před neoprávněným přístupem ze strany zaměstnanců a zvenku ukazují na komplexní přístup k bezpečnosti, který zahrnuje jak technická, tak organizační opatření.

Z technického hlediska respondenti zdůrazňují využití šifrování, firewallů, antivirových programů a vícefaktorové autentizace jako klíčových prvků pro ochranu citlivých dat. Někteří také navrhují vytvoření oddělených a utajených sítí, které by izolovaly data chráněných osob od běžných komunikačních kanálů, podobně jako se to dělá u utajených informací ve vojenském prostředí.

Z organizačního hlediska respondenti uvádějí důležitost přísného monitoringu přístupů k datům, včetně snímání logů, pravidelných auditů a omezení přístupu pouze na autorizované osoby. Tyto mechanismy zajišťují, že k citlivým datům mají přístup jen oprávnění zaměstnanci, a umožňují rychlou identifikaci neoprávněného přístupu.

Z těchto důvodů **je hypotéza č. 3 zamítnuta, protože současná technická a organizační opatření nejsou považována za dostatečná a neodpovídají komplexním bezpečnostním potřebám, které jsou nezbytné pro ochranu citlivých dat pacientů se statutem chráněné osoby.** K dosažení adekvátní úrovně ochrany je zapotřebí diverzifikovaného přístupu, který kombinuje různé techniky a postupy, aby čelil stále se vyvíjejícím hrozbám. Tento přístup by měl zahrnovat nejen moderní technologická řešení, ale také pravidelné školení personálu, důsledné monitorování přístupů a efektivní kontrolní mechanismy, které společně zajistí maximální úroveň ochrany citlivých informací.

6.3.4 Dílčí diskuse dalších výsledků virtuální a kybernetické bezpečnosti

Odpovědi respondentů na šestou otázku ve třetí sekci, která se zaměřuje na způsob školení zaměstnanců ohledně kybernetické bezpečnosti chráněných osob, poukazují na výrazné nedostatky v této oblasti. Většina respondentů se shoduje, že školení zaměstnanců ohledně specifické ochrany dat chráněných osob buď vůbec neprobíhá, nebo je na velmi nízké úrovni. Tento nedostatek školení je významný zejména vzhledem k tomu, že zdravotnická zařízení se stávají častým cílem kybernetických útoků zaměřených na citlivé údaje, jak ukázaly studie z USA a EU, které potvrzují, že zaměstnanci zdravotnických zařízení bývají zneužíváni jako nejslabší článek v kybernetické obraně.[238] Někteří respondenti přímo uvádějí, že zaměstnanci nejsou školeni v rozpoznávání rizik spojených s ochranou dat chráněných osob a nevnímají tato rizika jako důležitá. **Tento nedostatek povědomí a školení představuje značné riziko pro bezpečnost dat, protože zaměstnanci, kteří nejsou dostatečně informováni, mohou nevědomky ohrozit ochranu citlivých informací**.

Respondenti rovněž naznačují, že i tam, kde se školení provádí, se zaměřuje spíše na obecné aspekty kybernetické bezpečnosti než na specifika týkající se chráněných osob. To vede k situacím, kdy jsou zaměstnanci připraveni řešit běžné kybernetické hrozby, ale nejsou vybaveni znalostmi potřebnými k ochraně dat chráněných osob, které mohou čelit specifickým a sofistikovanějším útokům. Tento nedostatek specifického zaměření školení je potvrzen také výzkumem provedeným v britských nemocnicích, kde se zjistilo, že zaměstnanci mají obecné

povědomí o kybernetických rizicích, ale nejsou dostatečně školeni v otázkách týkajících se chráněných osob a jejich specifických hrozeb.[239]

Podle výsledků dotazníků pouze 14 % respondentů uvádí, že ve zdravotnických zařízeních probíhají školení nebo osvěta o ochraně dat chráněných osob pro všechny zaměstnance. Dalších 25,5 % respondentů potvrzuje, že taková školení probíhají, ale pouze pro vybrané skupiny zaměstnanců. Nicméně 33 % respondentů uvádí, že žádná školení v této oblasti neprobíhají, a dalších 27,4 % není o této otázce informováno. Tyto výsledky poukazují na potřebu systematického vzdělávání a osvěty mezi zdravotnickým personálem v oblasti ochrany dat chráněných osob. V tomto ohledu zahraniční studie ukazují, že **pravidelné školení a zvyšování povědomí zaměstnanců může významně zlepšit jejich schopnost chránit citlivá data a předejít kybernetickým útokům.**[240]

Výsledky zahraničních dotazníků vykreslují odlišný obraz. Více než polovina zahraničních respondentů (56,8 %) potvrzuje, že školení v oblasti ochrany dat chráněných osob probíhá pro všechny zaměstnance, což je výrazně více než v Česku. Pouze 6,3 % zahraničních respondentů uvedlo, že žádná školení v této oblasti neprobíhají, což je výrazně méně ve srovnání s českými zařízeními. Tento rozdíl naznačuje, že **zahraniční zařízení jsou lépe připravena na ochranu dat a kladou větší důraz na vzdělávání zaměstnanců** v této klíčové oblasti. Tento rozdíl může být způsoben také vyššími požadavky na kybernetickou bezpečnost v zahraničí, kde jsou přijímána přísnější opatření a povinnosti týkající se ochrany dat, jak ukazuje mezinárodní právní analýza ochrany dat zpracovaná Shackelfordem, Zeringuem a Mosesem.[241]

Odpovědi respondentů na sedmou otázku ve třetí sekci, zaměřenou na nejčastější problémy v oblasti kybernetické bezpečnosti chráněných osob, odhalují několik zásadních problémů, které trápí zdravotnická zařízení. Hlavním problémem, který respondenti opakovaně zmiňují, je **nedostatek jednotných standardů a směrnic pro ochranu dat chráněných osob**. Mnoho respondentů zdůrazňuje, že každé zdravotnické zařízení si nastavuje vlastní postupy, což vede k nejednotnosti a potenciálním slabinám v zabezpečení citlivých dat. Tento nedostatek standardizace zvyšuje riziko úniku informací a kompromitace dat.

Další významný problém je spojen s nedostatečnou technickou a organizační infrastrukturou. Respondenti poukazují na to, že mnohá zdravotnická zařízení nemají dostatečné zdroje ani technické vybavení k zajištění kybernetické bezpečnosti na požadované úrovni. Někteří navrhují vytvoření oddělených, utajených sítí speciálně určených pro ochranu dat chráněných

osob, což by výrazně zvýšilo úroveň zabezpečení. Taková síť by měla být zcela izolovaná od běžné nemocniční infrastruktury a zabezpečená proti vnějším i vnitřním hrozbám.

Respondenti rovněž zdůrazňují potřebu lepší analýzy rizik, která by se zaměřila na specifická rizika spojená s ochranou dat chráněných osob. Současná opatření často neberou v úvahu specifické hrozby, kterým mohou data chráněných osob čelit, což může vést k nedostatečné ochraně těchto citlivých informací. Tento přístup se odráží i v mezinárodních výzkumech, kde byla zdůrazněna nutnost zaměřit se na konkrétní hrozby související s ochranou vysoce citlivých dat, zejména ve zdravotnictví, kde mohou být údaje snadno zneužity k cíleným útokům nebo k narušení důvěry ve zdravotní systém.[242]

Podle výsledků dotazníků respondenti navrhují několik opatření ke zlepšení kybernetické bezpečnosti při hospitalizaci chráněných osob. Nejčastěji doporučovaným opatřením bylo zaheslování dokumentace a efektivní správa přístupů, což naznačuje, že omezení přístupu k citlivým informacím by mohlo významně zvýšit bezpečnost. Podobná opatření jsou široce doporučována v odborné literatuře zaměřené na ochranu zdravotních dat, která uvádí, že řízení přístupových práv a zavedení vícefaktorového ověřování jsou klíčovými nástroji pro snížení rizik kybernetických útoků.[243] Efektivní správa přístupů může výrazně snížit riziko neoprávněného přístupu a zajistit, že citlivé informace jsou dostupné pouze oprávněným osobám.

Někteří respondenti rovněž navrhli posílení oddělení kybernetické bezpečnosti, což naznačuje potřebu specializovaných týmů a infrastruktury pro ochranu dat. Tento trend je také patrný v mezinárodním měřítku, kde je rostoucí důraz kladen na vytváření specializovaných oddělení kybernetické bezpečnosti v rámci zdravotnických zařízení. Tato oddělení by měla být odpovědná za monitorování, prevenci a reakci na kybernetické hrozby, přičemž jejich úkolem je i průběžná aktualizace bezpečnostních protokolů v souladu s nejnovějšími technologiemi a postupy.[244] Posílení těchto týmů by mohlo významně přispět k lepší ochraně dat chráněných osob a zvýšit schopnost zdravotnických zařízení čelit novým a stále sofistikovanějším kybernetickým hrozbám.

Na základě odpovědí na otázky č. 8, 9, 12 a 13 ve třetí sekci, lze formulovat několik klíčových témat a výzev, které se týkají ochrany dat chráněných osob ve zdravotnických zařízeních.

Konkrétně se jedná o:

1) Ochrana dat ve velkých souborech dat (big data).
2) Přenos dat mezi zdravotnickými zařízeními.
3) Doporučení pro zlepšení kybernetické bezpečnosti.
4) Implementace zkušeností ze zahraničí.

Ad 1) Ochrana dat ve velkých souborech dat (big data)

Respondenti se shodují na tom, že ochrana dat chráněných osob v kontextu velkých datových souborů je nezbytná, ale vysoce náročná. Používání technik jako anonymizace a šifrování je považováno za standardní postup, avšak většina respondentů upozorňuje na to, že tato opatření nemusí být vždy dostačující. Někteří zdůrazňují důležitost analýzy rizik, která by měla zohledňovat nejen obsah dat, ale i způsob jejich ukládání a možnosti jejich kombinace s jinými datovými zdroji, což může odhalit identitu chráněných osob. Zkušenosti ukazují, že je nutné zaměřit se na vytvoření přísnějších bezpečnostních opatření, která by zajišťovala lepší ochranu těchto citlivých informací.

Ad 2) Přenos dat mezi zdravotnickými zařízeními

Z odpovědí je zřejmé, že přenos dat mezi zdravotnickými zařízeními je oblastí s významnými nedostatky. Většina respondentů uvádí, že bezpečnostní opatření pro přenos dat nejsou dostatečně důsledná nebo tento proces vůbec neřeší, což zvyšuje riziko úniku informací. Tento problém je potvrzen i v mezinárodních studiích, které ukazují, že přenos dat mezi zdravotnickými institucemi je často zranitelný, a to jak kvůli nejednotným protokolům, tak kvůli nedostatečným technickým opatřením, jako jsou šifrování nebo ověřování přístupů.[245] Jednotlivá zařízení často přistupují k zabezpečení dat rozdílně, což vede k nekonzistenci v jejich ochraně.

Respondenti volají po zavedení jasných a jednotných standardů pro přenos dat, které by zajistily, že citlivé informace budou chráněny na všech úrovních přenosu. Tato **potřeba standardizace je klíčová, neboť současné technologické a organizační rozdíly mezi zdravotnickými zařízeními vedou k tomu, že úroveň ochrany dat se může výrazně lišit, což ohrožuje bezpečnost pacientů.**[246] Zavedení jednotných bezpečnostních standardů by nejen snížilo riziko úniku informací, ale také zlepšilo spolupráci mezi zdravotnickými zařízeními, zejména v případech, kdy dochází k přenosu citlivých informací o chráněných osobách mezi různými poskytovateli zdravotních služeb.

Je evidentní, že současné nedostatky v této oblasti představují vážné riziko pro bezpečnost dat chráněných osob. Kybernetické útoky zaměřené na zdravotnická zařízení, jak ukázaly případy v USA a EU, často využívají právě slabá místa v přenosu dat mezi institucemi, kdy chybí odpovídající zabezpečení a kontrola.[243] Vzhledem k těmto rizikům je nezbytné, aby zdravotnická zařízení nejen zavedla moderní technologie, jako je šifrování dat během přenosu, ale také zajistila, že zaměstnanci budou školeni v tom, jak správně spravovat a chránit citlivé informace.

Ad 3) Doporučení pro zlepšení kybernetické bezpečnosti

Z odpovědí vyplývá, že klíčem ke zlepšení kybernetické bezpečnosti je kombinace technologických inovací, standardizace postupů a důkladného školení personálu. Respondenti doporučují zavádění nových technologií, jako jsou pokročilé šifrovací systémy, které mohou významně snížit riziko neoprávněného přístupu k citlivým datům. Studie zaměřené na zavádění šifrovacích technologií ve zdravotnických zařízeních potvrzují, že tyto technologie zvyšují úroveň ochrany dat, zejména při jejich přenosu mezi různými systémy.[247] Kromě toho je zásadní pravidelně aktualizovat bezpečnostní protokoly, aby se zařízení mohla přizpůsobit neustále se měnícím hrozbám v oblasti kybernetické bezpečnosti.

Důležitou roli hraje také zavedení standardizovaných postupů, například prostřednictvím norem jako HL7, které umožňují bezpečný a efektivní přenos zdravotních dat mezi různými systémy a zařízeními. Tato norma je uznávaným standardem pro výměnu, integraci a sdílení elektronických zdravotních informací a její aplikace by mohla významně přispět ke zlepšení bezpečnosti dat a efektivnější spolupráci mezi zdravotnickými zařízeními.[248]

Tyto kroky by měly být doplněny pravidelným školením zaměstnanců, aby byli schopni rozpoznat a reagovat na potenciální kybernetické hrozby. **Nedostatečné povědomí personálu o kybernetických rizicích je totiž jednou z hlavních příčin úspěšných útoků na zdravotnická zařízení**, jak ukazuje výzkum zaměřený na kybernetickou bezpečnost ve zdravotnictví.[240] Školení by mělo zahrnovat praktické příklady kybernetických útoků a ukazovat, jak se těmto hrozbám efektivně bránit, čímž by se minimalizovalo riziko lidských chyb, které jsou častou příčinou narušení bezpečnosti dat.

Ad 4) Implementace zkušeností ze zahraničí

Respondenti s mezinárodními zkušenostmi potvrzují, že zahraniční zdravotnická zařízení často používají přísnější bezpečnostní standardy než ta česká. Například v rámci NATO jsou data

chráněna velmi striktními pravidly a standardizovanými postupy, což zajišťuje jejich bezpečnost napříč různými systémy a institucemi. Tento přístup je založen na interoperabilitě systémů a zavedení datových standardů, což umožňuje efektivní a bezpečnou výměnu informací. Tyto zahraniční zkušenosti zdůrazňují potřebu aplikovat podobné přístupy a standardy i v českém kontextu, aby byla zajištěna adekvátní ochrana citlivých dat chráněných osob.

Závěrečné shrnutí

Třetí sekce výzkumu ukázala, že ochrana dat chráněných osob ve zdravotnictví vyžaduje komplexní přístup, který kombinuje technologická, organizační a vzdělávací opatření. Současné nedostatky, zejména v oblasti přenosu dat mezi zdravotnickými zařízeními a ochrany dat ve velkých datových souborech, představují značné riziko pro bezpečnost citlivých informací. Nedostatečná standardizace postupů a chybějící specifická školení pro ochranu dat chráněných osob přispívají k vyšší zranitelnosti těchto dat vůči únikům a zneužití.

Respondenti identifikovali několik klíčových problémů, včetně neexistence jednotných bezpečnostních standardů a nedostatečné analýzy rizik, což často vede k nedostatečné ochraně dat. Byla zdůrazněna potřeba zavést standardizované postupy, které by zajistily bezpečnost dat napříč všemi zdravotnickými zařízeními, a potřeba vytvoření samostatných a vysoce zabezpečených sítí pro ochranu těchto dat.

Dalším zjištěním bylo, že současná úroveň školení zaměstnanců v oblasti kybernetické bezpečnosti je nedostatečná. Školení se často zaměřují pouze na obecné aspekty kybernetické bezpečnosti, aniž by braly v úvahu specifika ochrany dat chráněných osob. Tento nedostatek vede k nízkému povědomí o rizicích a neochotě zaměstnanců adekvátně chránit citlivé informace.

6.4 Diskuse poznatků získaných z interpretace dat od chráněných osob

Pro tuto diskusi jsme vybrali pouze klíčové oblasti, které se týkají informovanosti chráněných osob, kybernetické bezpečnosti, vnímání „VIP statusu“, vnímání bezpečnosti a soukromí, a doporučení pro zlepšení péče. Tyto oblasti poskytují zásadní pohled na to, jak jsou chráněné osoby vnímány a jak je o ně postaráno ve zdravotnických zařízeních.

Konkrétně se jedná o:

1) Informovanost a komunikace.
2) Kybernetická bezpečnost a ochrana dat.
3) Vnímání a realita „VIP statusu“.
4) Vnímání bezpečnosti a soukromí.
5) Podněty pro zlepšení péče.

Ad 1) Informovanost a komunikace

Jedním z nejzávažnějších problémů identifikovaných v dotaznících je nedostatečná informovanost chráněných osob o jejich speciálním statutu a pravidlech péče. Drtivá většina respondentů (79,4 %) uvedla, že nebyla informována o existenci speciálních pravidel týkajících se jejich péče. Tento **výsledek naznačuje významnou mezeru v komunikaci mezi zdravotnickými zařízeními a pacienty**, což může mít důsledky pro jejich důvěru a spokojenost. Zahraniční výzkumy ukazují, že podobné problémy s nedostatečnou komunikací byly zaznamenány i v jiných zemích, kde nedostatek jasných a transparentních informací pro pacienty vedl ke snížení jejich důvěry v poskytovatele zdravotních služeb a zvýšení míry stížností.[249] Tato zjištění ukazují na potřebu systematického přístupu k informování pacientů o jejich právech a speciálním statutu, aby se předešlo zmatkům a případným konfliktům.

V kontextu dnešní doby, kdy jsou pacienti stále více informovaní a očekávají transparentní komunikaci, je klíčové, aby zdravotnická zařízení zlepšila své komunikační strategie. Studie ukazují, že zlepšení komunikace mezi zdravotnickým personálem a pacienty zvyšuje nejen spokojenost pacientů, ale i jejich ochotu spolupracovat a dodržovat léčebné postupy[250]. Zajištění toho, že chráněné osoby obdrží jasné a srozumitelné informace o svém statutu a právech, může nejen zvýšit jejich spokojenost, ale také minimalizovat riziko nedorozumění a zvýšit efektivitu péče. Komunikace musí být navíc přizpůsobena specifickým potřebám chráněných osob, zejména pokud se jedná o osoby s omezenou schopností porozumění nebo jazykovými bariérami, jak ukázaly studie zaměřené na zlepšení komunikace v multikulturních prostředích.[251]

Ad 2) Kybernetická bezpečnost a ochrana dat

Nedostatečná komunikace ohledně opatření k ochraně dat je další zásadní oblastí, která vyžaduje zlepšení. Téměř 90 % respondentů uvedlo, že nebyli informováni o tom, jak jsou jejich data chráněna. Tento nedostatek povědomí může vést k obavám o bezpečnost jejich

osobních údajů, což je v dnešní době zvýšeného povědomí o kybernetických hrozbách kritické. **Nedostatek informací o kybernetické bezpečnosti je alarmující zvláště v kontextu rostoucích hrozeb**, jako jsou útoky ransomwaru, phishing nebo zneužití osobních dat. Vzhledem k přísným požadavkům na ochranu osobních údajů stanoveným nařízením GDPR by měla být komunikace o bezpečnostních opatřeních standardní praxí, a to nejen z důvodu právní povinnosti, ale i pro zvýšení důvěry pacientů.

Ad 3) Vnímání a realita „VIP statusu“

Pouze 11 % respondentů uvedlo, že byli někdy hospitalizováni jako chráněné osoby, což ukazuje na omezený rozsah tohoto statusu. I když „VIP status“ může přinést výhody, jako je rychlejší přístup k vyšetřením nebo samostatné pokoje, nedostatečná informovanost těchto pacientů o jejich právech a výhodách může vést k nesouladu mezi očekáváním a skutečnou zkušeností. Tento problém je zvláště důležitý v kontextu rostoucích diskuzí o rovnosti ve zdravotní péči, kde privilegia spojená s „VIP statusem“ mohou být vnímána jako nespravedlivá vůči běžným pacientům. Diskuse o etice nerovného přístupu ve zdravotnictví je aktuálním tématem i v zahraničí. Například studie provedená v USA ukazuje, že výhody pro „VIP pacienty“ mohou způsobit nejen etické problémy, ale i praktické komplikace v každodenním provozu zdravotnických zařízení, kde se čelí tlaku zajistit rovnost péče pro všechny pacienty.[252]

V kontextu zejména teoretické části práce lze definitivně shrnout, že „VIP status“ lze přiznat pouze v rovině bezpečnostní, v žádné jiné. „VIP status“ by měl být používán výhradně pro zajištění fyzické bezpečnosti pacientů, kteří jsou z hlediska veřejného zájmu považováni za vysoce rizikové. Tento přístup podporují i mezinárodní standardy pro bezpečnostní opatření v nemocnicích, kde je důraz kladen na ochranu osob, aniž by došlo k narušení principu rovného přístupu ke zdravotní péči.[253]

Dle autora je zásadní, aby zdravotnická zařízení uměla tuto záležitost řádně vykomunikovat nejen svým zaměstnancům, samotným chráněným osobám, ale také veřejnosti. Správná a transparentní komunikace ohledně „VIP statusu“ je klíčová pro udržení důvěry ve zdravotní systém a pro minimalizaci negativních dopadů, které by tento status mohl mít na vnímání rovnosti ve zdravotnictví. Studie a zahraniční přístupy ukazují, že veřejná důvěra v systém zdravotní péče je úzce spjata s vnímáním rovného přístupu ke službám, a proto je zásadní, aby nemocnice transparentně vysvětlily účel a omezení „VIP statusu“.[254]

Ad 4) Vnímání bezpečnosti a soukromí

Navzdory implementaci fyzických bezpečnostních opatření se většina respondentů necítila omezeně ve svém soukromí nebo pohybu (88 %). To ukazuje, že zdravotnická zařízení jsou schopna poskytovat ochranu bez narušení komfortu pacientů. Tento nález je pozitivní, protože zajišťuje, že bezpečnostní opatření jsou účinná, aniž by způsobovala nepohodlí.

Téměř 90 % respondentů nebylo informováno o opatřeních pro zajištění kybernetické bezpečnosti jejich dat, což je alarmující. V dnešní digitální době **je klíčové, aby pacienti byli informováni o tom, jak jsou jejich osobní a zdravotní údaje chráněny**. Tento nedostatek informovanosti může vést k obavám a nedůvěře pacientů ve zdravotnický systém. Je nezbytné zlepšit komunikaci ohledně kybernetické bezpečnosti, aby pacienti měli jistotu, že jejich data jsou chráněna v souladu s nejlepšími praktikami a legislativními požadavky, jako je GDPR.

Pouze 4,7 % respondentů se zajímalo o to, kdo nahlíží do jejich zdravotní dokumentace, což může naznačovat důvěru v ochranu dat ve zdravotnických zařízeních. Na druhou stranu, tento nízký zájem může také vyplývat z nedostatku povědomí o možných rizicích neoprávněného přístupu k citlivým datům. Tento nedostatek informovanosti se shoduje s výsledky mezinárodních studií, které ukazují, že pacienti často nevědí o svých právech týkajících se ochrany osobních údajů, což vede k menší angažovanosti v této oblasti.[255] Je klíčové zvýšit povědomí pacientů o jejich právech týkajících se ochrany osobních údajů a zajistit, aby měli snadný přístup k informacím o tom, kdo a kdy k jejich datům přistupoval.

Obzvláště v dnešní době **je alarmující, že se chráněné osoby aktivně nezajímají o bezpečnost jejich pacientských dat**, což odráží globální trend, kdy pacienti nejsou dostatečně informováni o rizicích spojených s kybernetickými útoky na zdravotnické systémy. Jak ukazují výzkumy v oblasti zdravotnické kybernetické bezpečnosti, nedostatečné povědomí o rizicích zvyšuje pravděpodobnost úniků dat a neoprávněného přístupu.[256] To evokuje jasnou potřebu osvěty pro chráněné osoby a přijetí systémových opatření pro ochranu jejich pacientských dat.

Většina respondentů se nezajímá ani o to, s kým a kde jsou jejich zdravotní informace sdíleny. Tento nezájem může být důsledkem nedostatku informací nebo důvěry v to, že zdravotnická zařízení nakládají s daty bezpečně. Avšak v kontextu zvyšujících se hrozeb v oblasti kybernetické bezpečnosti je důležité, aby pacienti byli informováni a aby měli možnost ovlivnit, kdo má přístup k jejich zdravotním informacím. Výzkumy zaměřené na transparentnost ve

zdravotnických systémech ukazují, že pacienti, kteří mají větší přístup ke svým zdravotním záznamům a informacím o tom, kdo k jejich datům přistupuje, mají vyšší důvěru v systém zdravotní péče.[257] Zdravotnická zařízení by měla zvážit, jak zvýšit transparentnost v této oblasti, například prostřednictvím lepší komunikace a dostupných informací pro pacienty. Zajištění toho, aby pacienti měli kontrolu nad svými daty, může také snížit riziko úniků informací a zvýšit pocit bezpečí a důvěry mezi chráněnými osobami.

V daném kontextu hodlá autor práce informovat skupinu respondentů, které oslovil s jasnými doporučeními stran bezpečnosti a sdílení jejich pacientských dat. Zároveň je nutné podnítit systémové kroky k přijetí nápravných opatření přímo u odpovědných zaměstnanců našich chráněných osob, které mají na starost bezpečnostní opatření.

Ad 5) Podněty pro zlepšení péče

Respondenti identifikovali několik klíčových oblastí pro zlepšení, včetně lepší ochrany osobních údajů (13,5 %) a větší transparentnosti ohledně toho, kdo má přístup k jejich datům (13,1 %). Tyto požadavky jsou v souladu s rostoucím důrazem na práva pacientů na soukromí a ochranu osobních informací, jak je to zakotveno v GDPR. Navíc požadavek na zlepšení komunikace a informovanosti pacientů naznačuje, že zdravotnická zařízení by měla věnovat větší pozornost tomu, jak efektivně komunikovat bezpečnostní politiky a postupy. Modernizace informačních systémů a zavedení pravidelných školení pro zaměstnance jsou zásadními kroky k zajištění vysoké úrovně bezpečnosti a důvěry.

6.5 Minimální standardy poskytování zdravotní péče chráněným osobám pro zaměstnance zdravotnických zařízení

Na základě rozsáhlé analýzy získaných poznatků bylo identifikováno několik klíčových opatření, která mohou významně přispět k optimální hospitalizaci nebo ošetření chráněné osoby ze strany zaměstnanců zdravotnických zařízení:

Neohýbejte pravidla. Přestože chráněné osoby mohou vyvíjet tlak na změnu postupů a praktik, je důležité odolat pokušení podřídit se jejich přáním. Postupy a praktiky jsou zavedeny z provozních a bezpečnostních důvodů. Lékaři by měli jasně vysvětlit, že péče bude poskytována v souladu se všemi běžnými provozními a bezpečnostními pravidly.

Pracujte jako tým. Chráněným osobám musí být jasně řečeno, že ošetřující lékař je zodpovědný za všechna lékařská rozhodnutí a ostatní poskytovatelé nebo lékaři budou fungovat jako konzultanti. „Každé vybočení ze standardních postupů je cesta do pekel."

Komunikujte. Strukturovaná, pravidelná a předvídatelná komunikace je nezbytná pro pacienta, rodinu a všechny zúčastněné poskytovatele. Předvídatelná komunikace stanoví hranice, kdy a jak je vhodné kontaktovat ošetřujícího lékaře.

Pečlivě řídit komunikaci s médii. Důvěrnost je klíčová. Jakákoli mediální komunikace by měla být pečlivě naplánována s oddělením pro styk s veřejností zdravotnického zařízení a měla by obsahovat pouze ty informace, které pacient schválil.

Odolejte „syndromu předsedajícího". Rodina může požadovat přidělení nejstaršího lékaře, i když nemusí být nejvhodnější. **Péče by měla probíhat co nejblíže běžné praxi, zcela standardně**, včetně obsazení nejvhodnějšími lékaři a stážisty.

Péče na vhodném místě. Péče by měla probíhat na nejvhodnějším místě, například na otevřené jednotce intenzivní péče, pokud je to potřeba. Diskuse by měla proběhnout na začátku hospitalizace, aby pacient a rodina pochopili důvody a potřebu sladit úroveň péče s prostředím.

Ochrana bezpečnosti pacienta. Chráněné osoby jsou často sledováni médii. Všechna opatření by měla být přijata k zajištění jejich bezpečnosti a soukromí. Tito pacienti by měli být více chráněni nebo vedeni jako důvěrní pacienti.

Ostražitost při přijímání darů. Přijímání i odmítání darů může být problematické. Nejlepší je nepřijímat žádné dary během pobytu ve zdravotnickém zařízení. Je nutné se řídit etickým kodexem daného zdravotnického zařízení.

Spolupráce s osobními lékaři pacienta. Pokud má chráněná osoba osobního lékaře, je dobré ho přizvat k účasti a ukázat mu, že si jeho názoru vážíte. Ošetřující lékař má však konečnou odpovědnost za péči během hospitalizace a provádění všech diagnostických a terapeutických úkonů.

Bezpečnost virtuálních dat. O data chráněných osob je velký zájem a jejich únik může způsobit velké problémy Vám i samotným chráněným osobám. Kybernetické incidenty týkající se chráněných osob by měly být hlášeny, monitorovány a vyhodnocovány pomocí automatických systémů nebo manuálních kontrol. Tento krok je zásadní pro zajištění vysoké

úrovně kybernetické bezpečnosti a ochrany dat. Stejně tak je nutné zabezpečit zdravotní data a informace před neoprávněným nahlížením vně i zevnitř zdravotního zařízení.

6.6 Minimální standardy poskytování zdravotní péče chráněným osobám pro zdravotnická zařízení

Na základě rozsáhlé analýzy a výzkumu v oblasti ochrany dat chráněných osob ve zdravotnických zařízeních bylo identifikováno několik klíčových opatření, která mohou významně přispět k zvýšení úrovně bezpečnosti a ochrany citlivých informací. Zde jsou doporučení pro praxi zdravotnických zařízení, která vycházejí z námi zpracovaných výsledků:

Kombinace technických a organizačních opatření. Pro zajištění maximální ochrany dat je nezbytné kombinovat technická opatření (jako jsou šifrování, firewally, antivirové programy) s přísnými organizačními kontrolami. To zahrnuje pravidelné audity, monitoring přístupů a jasné omezení přístupových práv pouze pro autorizované osoby, případně přístup k vybraným pacientům je nezbytné schválit nadřízeným/autorizovaným zaměstnancem. Je nutné dbát na tzv. cibulový bezpečnostní systém, který v případě výpadku jednoho systému/prvku, je nahrazen zálohován minimálně jedním dalším.

Pravidelná aktualizace a testování systémů. Bezpečnostní systémy a software by měly být pravidelně aktualizovány, aby byly schopny čelit novým hrozbám. Součástí by mělo být i pravidelné testování zranitelností prostřednictvím penetračních testů a simulací reálných kybernetických útoků.

Zvýšená ochrana dat chráněných osob. Speciální pozornost by měla být věnována ochraně dat chráněných osob. Zdravotnická zařízení by měla implementovat dodatečné bezpečnostní opatření, jako jsou šifrování dat, používání fiktivních jmen, a omezení přístupu na základě specifických rolí zaměstnanců. Pro chráněné osoby mohou být vytvořeny oddělené a utajené sítě, které minimalizují riziko neoprávněného přístupu.

Rozšířené a pravidelné školení personálu. Vzdělávání zaměstnanců je klíčové pro prevenci lidských chyb. Školení by měla být zaměřena na principy poskytování zdravotních služeb chráněným osobám, jejich fyzickou bezpečnost a rozpoznávání kybernetických hrozeb a na správné používání bezpečnostních technologií. Zaměstnanci by měli rozumět specifickým rizikům spojeným s ochranou dat chráněných osob a být informováni o aktuálních bezpečnostních postupech.

Implementace standardizovaných postupů a protokolů. Zajištění jednotných a standardizovaných bezpečnostních protokolů v celém nemocničním informačním systém je nezbytné. Zdravotnická zařízení by měly hrát aktivní roli v nastavování těchto standardů, které zajistí, že ochrana dat bude konzistentní a efektivní.

Zvýšení informovanosti pacientů. Pacienti by měli být informováni o tom, jak jsou jejich data chráněna a jaká opatření jsou přijímána na ochranu jejich soukromí. Zlepšení komunikace a transparentnosti ohledně bezpečnostních opatření může zvýšit důvěru pacientů ve zdravotnický systém a jejich ochotu sdílet citlivé informace.

Proaktivní přístup k analýze rizik. Zdravotnická zařízení by měla pravidelně provádět analýzy rizik spojené s ochranou dat a aktualizovat své postupy na základě zjištěných hrozeb. Tímto způsobem lze předejít potenciálním bezpečnostním incidentům a ztrátě citlivých informací.

Zavedení pokročilých technologií. Investice do moderních technologií, které umožňují detekci a prevenci kybernetických útoků, je klíčová. Patří sem systémy pro detekci narušení, nástroje pro monitorování síťového provozu a další technologie, které zajišťují komplexní ochranu zdravotnických dat.

Zavedení oddělených informačních systémů. Pro zajištění vyšší úrovně ochrany citlivých informací je vhodné zvážit oddělení systémů, které zpracovávají citlivá data, od běžné infrastruktury. Tím se minimalizuje riziko, že útočníci získají přístup k citlivým informacím skrze méně chráněné části systému.

Tato doporučení pro praxi jsou navržena tak, aby reagovala na aktuální výzvy a hrozby v oblasti ochrany dat chráněných osob ve zdravotnických zařízeních. Jejich implementace může významně přispět ke zvýšení bezpečnosti a ochraně citlivých informací pacientů, a tím posílit celkovou důvěru ve zdravotní péči.

6.7 Minimální standardy pro chráněné osoby

Na základě získaných poznatků a analýzy bylo identifikováno několik klíčových opatření, která mohou chráněným osobám pomoci zajistit jejich vlastní bezpečnost a ochranu soukromí při hospitalizaci nebo vyšetření. Tato doporučení se zaměřují na aktivní roli pacientů při ochraně svých dat a na komunikaci se zdravotnickým personálem.

Respektujte standardy péče. Mějte na paměti, že máte právo pouze na standardní kvalitu a rozsah zdravotní péče jako všichni ostatní pacienti. Očekávejte férové a rovné zacházení bez ohledu na Váš „VIP status“. Nevyžadujte zvláštní zacházení, které by mohlo ohrozit integritu zdravotní péče nebo porušit standardní postupy zdravotnického zařízení.

Informujte se o bezpečnostních opatřeních. Při přijetí do zdravotnického zařízení se zeptejte na bezpečnostní opatření, která zdravotnické zařízení používá k ochraně vašich osobních a zdravotních dat. Ujistěte se, že chápete, jak jsou vaše data chráněna před neoprávněným přístupem.

Vyžádejte si omezený přístup k vašim datům. Požádejte o omezení přístupu k vašim zdravotním informacím pouze na nezbytné osoby. Toto může zahrnovat použití pseudonymů nebo kódovaných označení, aby vaše identita zůstala chráněná.

Sledujte, kdo má přístup k vašim datům. Zajímejte se o to, kdo má přístup k vašim zdravotním záznamům a za jakým účelem. Požádejte o pravidelné zprávy nebo logy, které ukazují přístupy k vašim datům.

Dbejte na fyzickou bezpečnost. Pokud je to možné, požádejte o samostatný pokoj nebo o opatření zajišťující vaši fyzickou bezpečnost, jako je omezený přístup na oddělení, přítomnost ochranky nebo jiné diskrétní bezpečnostní opatření.

Komunikujte se zdravotnickým personálem. Udržujte otevřenou a pravidelnou komunikaci s ošetřujícím lékařem a dalšími členy zdravotnického týmu. Informujte je o vašich preferencích ohledně bezpečnosti a ochrany soukromí a zajistěte, že tyto preference jsou respektovány.

Buďte opatrní při sdílení informací. Pečlivě zvažte, jaké informace sdílíte a s kým. Omezte sdílení citlivých informací na nezbytný okruh osob a vyhněte se sdílení informací prostřednictvím nezabezpečených komunikačních kanálů.

Zvažte právní ochranu. V případě potřeby konzultujte právníka specializujícího se na ochranu osobních údajů, abyste se ujistili, že vaše práva na ochranu dat jsou plně respektována a chráněna.

Pravidelně přezkoumávejte a aktualizujte své preference. Vaše potřeby a preference ohledně bezpečnosti se mohou měnit. Pravidelně přehodnocujte svá rozhodnutí ohledně ochrany dat a informujte zdravotnický personál o jakýchkoli změnách.

Informujte se o možnostech sledování vašich dat. Zeptejte se, jaké možnosti máte k dispozici pro sledování přístupu k vašim zdravotním informacím. Některá zdravotnická zařízení mohou nabízet nástroje nebo aplikace, které umožňují pacientům vidět, kdo a kdy nahlédl do jejich zdravotních záznamů.

Tato doporučení pomohou chráněným osobám lépe chránit jejich soukromí a bezpečnost během zdravotní péče. Aktivní role pacientů v ochraně vlastních dat a informací může významně přispět k prevenci neoprávněného přístupu a zneužití citlivých informací, přičemž respektování standardních postupů péče zajistí rovné a spravedlivé zacházení.

6.8 Vyhodnocení hypotéz

Stanovené hypotézy v konfrontaci s výsledky obstály následovně (viz kapitola 6.3):

- **Hypotéza č. 1:** Nejčastější slabá místa v oblasti bezpečnosti pacientských dat anebo informací při hospitalizaci chráněných osob jsou způsobena nedostatečnou implementací aktuálních bezpečnostních technologií a postupů.
  Hypotéza byla zamítnuta.
- **Hypotéza č. 2:** Pacienti se statutem chráněné osoby čelí vyššímu riziku zneužití jejich osobních údajů anebo zdravotních dat ve srovnání s běžnými pacienty, zejména kvůli jejich zvýšené hodnotě.
  Hypotéza byla zamítnuta.
- **Hypotéza č. 3:** Technická a organizační opatření aktuálně implementovaná ve zdravotnických zařízeních nejsou dostatečná k efektivní ochraně citlivých informací o pacientech se statutem chráněné osoby.
  Hypotéza byla zamítnuta.

7 Závěr

Tato disertační práce se zabývala problematikou bezpečnosti hospitalizovaných chráněných osob, která zahrnuje širokou škálu náročných procesů spojených s bezpečností, ochranou citlivých údajů a zajištěním adekvátní zdravotní péče. Hlavním cílem práce bylo identifikovat klíčová riziková místa v oblasti zpracování a přenosu osobních a zdravotních dat chráněných osob v českých zdravotnických zařízeních a na základě těchto zjištění formulovat konkrétní a prakticky využitelná doporučení pro zvýšení úrovně jejich ochrany. Na základě empirických dat získaných v průběhu výzkumu bylo možné tento cíl splnit, přičemž navržená opatření zajišťují vysoký stupeň zabezpečení dat a jsou plně v souladu s mezinárodními standardy v oblasti ochrany osobních údajů a kybernetické bezpečnosti.

Dle názoru autora práce byly kromě hlavního cíle splněny i všechny dílčí cíle práce. První z nich, tedy rozsáhlá analýza odborných pramenů z oblasti bezpečnosti zdravotnických zařízení, poskytla solidní teoretický základ pro další výzkum. Identifikace problémových míst při zpracování osobních údajů, což byl druhý cíl, přinesla jasné poznatky o současných mezerách v ochraně dat chráněných osob, které vedly k návrhu konkrétních opatření pro zvýšení jejich bezpečnosti. Třetím cílem bylo navrhnout specifická opatření pro zlepšení péče o chráněné osoby, přičemž práce zohlednila odlišnosti jejich postavení oproti běžným pacientům a navrhla optimalizace v organizačních procesech zdravotnických zařízení. Čtvrtý dílčí cíl, vytvoření hodnotné práce pro další vědecko-výzkumnou činnost, byl naplněn ve formě závěrů a doporučení, která mají potenciál k praktické implementaci a dalšímu vědeckému zkoumání.

Obsah disertační práce byl strukturován do několika klíčových částí. V úvodu byly stanoveny cíle, výzkumné otázky a hypotézy, které byly následně řešeny prostřednictvím analýzy literatury a empirického výzkumu. První část práce se věnovala teoretickým aspektům zdravotnického systému, právním normám a specifikům chráněných osob, „VIP pacientů“ a souvisejícím bezpečnostním otázkám. Byla provedena podrobná analýza současných trendů v oblasti hospitalizace a ochrany osobních údajů, včetně kybernetické bezpečnosti a fyzické ochrany pacientů. Důležitou součástí bylo také zkoumání inovativních přístupů, jako je virtuální hospitalizace a přenos zdravotních dat prostřednictvím cloudových řešení.

Empirická část práce se zaměřila na sběr dat od zdravotnických pracovníků i chráněných osob, a to za použití kvalitativních i kvantitativních metod. Rozhovory s odborníky poskytly hlubší

vhled do praktických výzev souvisejících s ochranou citlivých údajů a bezpečností během hospitalizace, zatímco dotazníky odhalily postoje respondentů k otázkám rovného přístupu k péči a ochraně osobních údajů. Analýza těchto dat umožnila vytvořit komplexní model pro bezpečný přenos a zpracování zdravotních dat, který by mohl být implementován nejen v českých zdravotnických zařízeních s ohledem na mezinárodní standardy a potřeby moderní zdravotní péče, ale také ve zdravotnických zařízeních v rámci NATO. Tento model lze považovat za stěžejní výstup práce.

V průběhu práce byla věnována značná pozornost analýze, jak jsou chráněné osoby vnímány ve zdravotnických zařízeních z hlediska poskytování péče, přístupu k osobním údajům a zajištění jejich bezpečnosti. Výzkum ukázal, že ačkoli jsou chráněné osoby často považovány za pacienty se zvláštním statusem, neexistují žádné právní důvody pro udělení nerovných výhod nebo preferenčního zacházení. Významným zjištěním bylo, že „VIP status“ chráněných osob, přestože může zahrnovat některé výhody, nesmí narušovat princip rovného přístupu ke zdravotní péči. Bylo navrženo, aby se zdravotnická zařízení soustředila na transparentnost procesů a informování pacientů o jejich právech a možnostech, což by zlepšilo jejich spokojenost a důvěru v systém poskytování zdravotní péče.

V oblasti kybernetické bezpečnosti byla identifikována potřeba zavedení přísnějších kontrol přístupů k citlivým údajům chráněných osob. Návrhy na posílení těchto opatření zahrnují zavedení pravidelných auditů, zlepšení technických bezpečnostních opatření a zvýšení informovanosti personálu o důležitosti ochrany osobních údajů. Také bylo doporučeno zavést systematické školení zdravotnických pracovníků v oblasti komunikace a práce s chráněnými osobami, aby byla zajištěna nejen bezpečnost těchto pacientů, ale i jejich spokojenost a důstojnost během hospitalizace.

Lze konstatovat, že tato práce nejenže splnila stanovené cíle, ale rovněž otevřela značný prostor pro další diskuzi a výzkum v oblasti ochrany chráněných osob a jejich práv v prostředí českých zdravotnických zařízení. Její výsledky poskytují konkrétní a prakticky využitelná doporučení, která mohou výrazně přispět ke zvýšení úrovně bezpečnosti a ochrany osobních údajů chráněných osob, a současně slouží jako podklad pro další vědecko-výzkumné aktivity v této důležité oblasti. Zásadní myšlenkou je pak konstatování potřeby chránit legitimním způsobem vybrané skupiny osob více do doby, nežli bude systém schopen efektivně ochránit všechny stejným způsobem bez rozdílu.

V kontextu současného dění ve světě, včetně válečných konfliktů, jako je válka na Ukrajině a konflikt v Palestině, se ukazuje, jak zásadní je mít připravené a efektivní systémy ochrany zranitelných skupin obyvatelstva, včetně chráněných osob. Tyto konflikty odhalily nejen nedostatky ve zdravotní péči během krizových situací, ale i naléhavou potřebu modernizace způsobů ochrany osobních a zdravotních dat. Vývoj moderních válečných technologií, jako je využití telemedicíny nebo virtuálních konzultací na bojištích, jasně ukazuje na nutnost zlepšit kybernetickou a fyzickou bezpečnost pacientů nejen v běžných, ale i v krizových zdravotnických podmínkách.

8 Seznam zkratek

AI Umělá inteligence.

CCDCOE NATO Cooperative Cyber Defence Centre of Excellence – výzkumné a vzdělávací centrum zaměřené na kybernetickou obranu, které podporuje Severoatlantickou alianci.

CLAUDIA Cloud Intelligence for Decision Support and Analysis.

CNDCGS 2024

Mezinárodní vědecká konference *Challenges to National Defence in Contemporary Geopolitical Situation.*

EDA Evropská obranná agentura.

EHDS Evropský zdravotnický datový prostor

ENISA European Union Agency for Cybersecurity – agentura Evropské unie pro kybernetickou bezpečnost, která poskytuje odborné poradenství a podporu členským státům EU v oblasti kybernetické bezpečnosti.

EU Evropská unie.

GDPR Nařízení EU 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

HL7 Health Level 7 je mezinárodní standard pro výměnu, integraci, sdílení a načítání elektronických zdravotních informací.

IPA Interpretativní fenomenologická analýza (Interpretative Phenomenological Analysis).

IT Informační technologie.

IoT Internet of Things – síť fyzických objektů (věcí) vybavených senzory, softwarem a dalšími technologiemi, které jsou propojeny prostřednictvím internetu a umožňují sběr a výměnu dat s jinými zařízeními.

IZS Integrovaný záchranný systém.

JIP Jednotka intenzivní péče.

Listina Usnesení předsednictva České národní rady č. 2/1993 Sb., ze dne 16. prosince 1992 o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky.

NATO Severoatlantická aliance (North Atlantic Treaty Organization).

NIS Nemocniční informační systém.

NIS 2 Směrnice Evropského parlamentu a Rady (EU) 2022/2555 o opatřeních pro vysokou společnou úroveň kybernetické bezpečnosti v celé Unii.

NÚKIB Národní úřad pro kybernetickou a informační bezpečnost.

NV o zajišťování bezpečnosti ústavních činitelů

Nařízení vlády č. 468/2008 Sb., o zajišťování bezpečnosti určených ústavních činitelů České republiky, ve znění pozdějších novel.

Občanský zákoník nebo OZ

Zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.

OECD Organizace pro hospodářskou spolupráci a rozvoj (Organisation for Economic Co-operation and Development).

OSN Organizace spojených národů.

OSVČ Osoba samostatně výdělečně činná.

PČR Policie České republiky.

SEU Smlouva o Evropské unii.

SZBP Společná zahraniční a bezpečnostní politika.

ÚVN Ústřední vojenská nemocnice – Vojenská fakultní nemocnice Praha.

VIP Very Important Person.

WHMO Vojenská kancelář Bílého domu.

Ústava Ústavní zákon č. 1/1993 Sb., Ústava České republiky.

Zákon o veřejném zdravotním pojištění nebo ZVZP

Zákon č. 48/1997 Sb., o veřejném zdravotním pojištění a o změně a doplnění některých souvisejících zákonů, ve znění pozdějších přepisů.

Zákon o zvláštní ochraně svědka nebo ZVOS

Zákon č. 137/2001 Sb., o zvláštní ochraně svědka a dalších osob v souvislosti s trestním řízením, ve znění pozdějších předpisů.

Zákon o zdravotních službách nebo ZZS

Zákon č. 372/2011 Sb., o zdravotních službách, ve znění pozdějších předpisů.

Zákon o Vojenské policii nebo ZoVP

Zákon č. 300/2013 Sb., o Vojenské policii a o změně některých zákonů (zákon o Vojenské policii), ve znění pozdějších předpisů.

Zákon o kybernetické bezpečnosti

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů.

Zákon o zpracování osobních údajů

Zákon č. 110/2019 Sb., o zpracování osobních údajů, ve znění pozdějších předpisů.

9 Seznam použitých pramenů

1. MINISTERSTVO OBRANY ČR. *Úplné znění zřizovací listiny příspěvkové organizace Ústřední vojenské nemocnice – Vojenské fakultní nemocnice Praha*. [online]. Praha: Ministerstvo obrany České republiky, 2017 [cit. 2023-04-10]. Dostupné z: https://www.uvn.cz/cs/doc/zakladni-informace-o-uvn/1566-zrizovaci-listi na-ustredni-vojenske-nemocnice-vojenske-fakultni-nemocnice-praha.

2. GARTNER. *How Geopolitics Impacts the Cyber-Threat Landscape*. [online]. Stamford: Gartner, 2022 [cit. 2023-05-20]. Dostupné z: https://www.gartner.com/en/ newsroom/ press-releases/2022-06-10-how-geopolitics-impacts-the-cyber-threat-lands cape. ISBN 978-1-4923-3219-0.

3. CENTERS FOR DISEASE CONTROL AND PREVENTION (CDC). *Healthcare System Preparedness and Response*. [online]. 2023 [cit. 2023-06-15]. Dostupné z: https://www.cdc.gov/flu/pandemic-resources/pdf/pandemic-influenza-implementation. pdf. ISBN 978-1-62074-065-3.

4. ARCHIVES OF PUBLIC HEALTH. *Preparedness, impacts, and responses of public health emergencies towards health security: qualitative synthesis of evidence*. [online]. 2023 [cit. 2023-07-05]. Dostupné z: https://archpublichealth.biomedcentral.com /articles/10.1186/s13690-022-008. DOI: 10.1186/s13690-022-008.

5. *Axiomatic Systems, Conceptual Schemes, and the Consistency of Mathematical Theories*. *Philosophy of Science*. Cambridge Core. [online]. [cit. 2023-02-22]. Dostupné z: https://www.cambridge.org/core/journals/philosophy-of-science/article/ axiomatic-systems-conceptual-schemes-and-the-co. ISSN 0031-8248.

6. *Axioms and Intuitions*. *Contemporary Mathematical Thinking*. Synthese Library, vol 474. Cham: Springer, 2023 [cit. 2022-12-18]. Dostupné z: https://doi.org/10.1007/978-3-031-27548-7_5. DOI: 10.1007/978-3-031-27548-7_5.

7. *Axiomatic method*. Encyclopedia of Mathematics. [online]. [cit. 2022-11-22]. Dostupné z: https://encyclopediaofmath.org/wiki/Axiomatic_method. ISBN 978-14-020-0609-3.

8. BATES, M. a J. NĚMEC. *Úvod do metateorií, teorií a modelů*. ProInflow. [online]. 2011 [cit. 2023-04-07]. Dostupné z: http://pro.inflow.cz/uvod-do-metateorii-teorii-mo delu. ISSN 1802-8470.

9. *The Two Sides of Modern Axiomatics: Dedekind and Peano, Hilbert and Bourbaki*. SpringerLink. [online]. [cit. 2023-03-15]. Dostupné z: https://link.springer.com/article/10.1007/s11016-020-00409-1. DOI: 10.1007/s11016-020-00409-1.

10. BHATTACHERJEE, A. *Social Science Research: Principles, Methods, and Practices*. University of South Florida. [online]. 2012 [cit. 2022-08-10]. Dostupné z: http://scholarcommons.usf.edu/oa_textbooks/3. ISBN 978-1475146127.

11. GUBA, E. G., LINCOLN, Y. S. *Competing Paradigms in Qualitative Research*. In: DENZIN, N. K., LINCOLN, Y. S. (Eds.). *Handbook of Qualitative Research*. Thousand Oaks, CA: Sage Publications, 1994, s. 105-117. ISBN 978-0803946798.

12. CRESWELL, J. W. *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. 4. vyd. Thousand Oaks, CA: Sage Publications, 2014. ISBN 978-1452226101.

13. OCHRANA, F. *Metodologie vědy: úvod do problému*. Praha: Karolinum, 2009, s. 34. ISBN 978-8024615137.

14. BABBIE, E. *The Practice of Social Research*. 13. vyd. Belmont, CA: Wadsworth Cengage Learning, 2013. ISBN 978-1133049791.

15. KERLINGER, F. N., LEE, H. B. *Foundations of Behavioral Research*. 4. vyd. Fort Worth, TX: Harcourt College Publishers, 2000. ISBN 978-0155078970.

16. SILVERMAN, D. *Doing Qualitative Research: A Practical Handbook*. 4. vyd. London: Sage Publications, 2013. ISBN 978-1446260159.

17. URBÁNEK, T., DENGLEROVÁ, D., ŠIRŮČEK, J. *Psychometrika: Měření v psychologii*. Praha: Portál, 2011, s. 143 a násl. ISBN 978-8073679428.

18. KUBÁTOVÁ, H. *Metodologie sociologie*. Olomouc: Univerzita Palackého v Olomouci, 2006, s. 75. ISBN 978-8024415691.

19. TROCHIM, W. M. K. *Research Methods: The Essential Knowledge Base*. Mason, OH: Thomson Custom Publishing, 2006. ISBN 978-0495599570.

20. PALÁN, Z. *Andragogický slovník*. [online]. 2012 [cit. 2024-02-12]. Dostupné z: http://www.andromedia.cz/andragogicky-slovnik/analyza. ISBN 978-8073679818.

21. MOLNÁR, Z. *Pokročilé metody vědecké práce*. Zeleneč: Profess Consulting, 2012, s. 42. ISBN 978-8087389423.

22. LORENZON, B., CLOSE, R., RISSINGER, W. *Teaching Your Students How to Do Student Science Research Projects*. Philadelphia: DVSF, 2007, s. 25 a násl. ISBN 978-0971943839.

23. REICHENBACH, H. *Experience and Prediction*. Chicago: University of Chicago Press, 1938. ISBN 978-0226703546.

24. SCHLICK, M., MIHIN, F. *Logický pozitivizmus*. Přel. SEDOVÁ, T., ZOUHAR, M. Bratislava: Iris, 2006, s. 89. ISBN 978-8089018109.

25. THAGARD, P. *Conceptual Revolutions*. Princeton, NJ: Princeton University Press, 1992. ISBN 978-0691020518.

26. WIMMER, M. *Základní metody vědeckého myšlení*. [online]. 1964 [cit. 2024-01-19]. Dostupné z: http://www.quido.cz/metody.htm.

27. BUNGE, M. *Scientific Research I: The Search for System*. Berlin: Springer-Verlag, 1967. ISBN 978-3540034614.

28. SOWA, J. F. *Knowledge Representation: Logical, Philosophical, and Computational Foundations*. Pacific Grove, CA: Brooks Cole Publishing Co., 2000. ISBN 978-0534949656.

29. ČESKO. *Zákon č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování*. In: *Sbírka zákonů České republiky*. 2011, částka 131. ISSN 1211-1244. Dostupné z: https://www.psp.cz/sqw/text/tiskt.sqw?O=6&CT=372&CT1=0.

30. YASTER, M., et al. *VIP Care in Pediatric Anesthesia: Ethical Implications and Practice*. In: *Pediatric Anesthesia Article of the Day*. [online]. 2023 [cit. 2024-01-15]. Dostupné z: https://ronlitman.substack.com/p/vip-care. ISSN 1099-1102.

31. SCHOLL, I., ZILL, J. M., HÄRTER, M., DIRMAIER, J., WU, W. C. *An Integrative Model of Patient-Centeredness – A Systematic Review and Concept Analysis*. *PLOS ONE*. [online]. 2014 [cit. 2024-01-22]. Dostupné z: https://dx.plos.org/10.1371/journal.pone.0107828. DOI: 10.1371/journal.pone.0107828.

32. TAMBUYZER, E., PIETERS, G., VAN AUDENHOVE, C. *Patient Involvement in Mental Health Care: One Size Does Not Fit All*. *Health Expectations*. [online]. 2011 [cit. 2024-03-04]. Dostupné z: http://doi.wiley.com/10.1111/j.1369-7625.2011.00743.x. DOI: 10.1111/j.1369-7625.2011.00743.x.

33. JAMES, C., DEVAUX, M., SASSI, F. *Inclusive Growth and Health*. In: *OECD iLibrary*. [online]. 2017 [cit. 2024-03-12]. Dostupné z: http://dx.doi.org/10.1787/93d52bcd-en. DOI: 10.1787/93d52bcd-en.

34. OECD. *Přehled o stavu veřejné správy: Česká Republika: Česká republika na cestě k modernější a efektivnější veřejné správě*. In: *OECD iLibrary*. [online]. 2023 [cit. 2024-03-16]. Dostupné z: https://www.oecd-ilibrary.org/governance/prehled-o-stavu-ve rej ne-spravy-ceska-republika_2651546f-cs. ISBN 978-9264312243.

35. RANDA, M. *Slušné minimum zdravotní péče jako lidské právo*. *Časopis zdravotnického práva a bioetiky*. Praha, 2022(1), s. 63-80. ISSN 1804-8137.

36. ČESKO. *Ústavní zákon č. 2/1993 Sb., usnesení předsednictva České národní rady o vyhlášení LISTINY ZÁKLADNÍCH PRÁV A SVOBOD jako součásti ústavního pořádku České republiky*. In: *Sbírka zákonů České republiky*. 1992, částka 1. ISSN 1211-1244. Dostupné z: https://www.psp.cz/sqw/sbirka.sqw?cz=2&r=1993.

37. ČESKO. *Zákon č. 48/1997 Sb., o veřejném zdravotním pojištění a o změně a doplnění některých souvisejících zákonů*. In: *Sbírka zákonů České republiky*. 1997, částka 1. ISSN 1211-1244. Dostupné z: https://www.psp.cz/sqw/sbirka.sqw?cz=48&r=1997.

38. THURLEY, P. *Health Care as a Human Right: A Rawlsian Approach*. Waterloo (Ontario, Canada): University of Waterloo, 2008. ISBN 978-0889207564.

39. NARVESON, J. *The Libertarian Idea*. Philadelphia: Temple University Press, 1988. ISBN 978-0877226514.

40. RANDA, M. *Slušné minimum zdravotní péče jako lidské právo*. *Časopis zdravotnického práva a bioetiky*. Praha, 2022(1), s. 65-80. ISSN 1804-8137.

41. SHUE, H. *Basic Rights: Subsistence, Affluence, and U.S. Foreign Policy*. 2. vyd. Princeton, NJ: Princeton University Press, 1980. ISBN 978-0691029658.

42. RANDA, M. *Slušné minimum zdravotní péče jako lidské právo*. *Časopis zdravotnického práva a bioetiky*. Praha, 2022(1), s. 71-80. ISSN 1804-8137.

43. SLOVENSKO. *Zákon č. 578/2004 Sb., o poskytovateľoch zdravotnej starostlivosti, zdravotníckych pracovníkoch, stavovských organizáciách v zdravotníctve a o zmene a doplnení niektorých zákonov*. In: *Sbierka zákonů Slovenskej republiky*. 2004, částka 13. ISSN 2644-4674.

44. CAMBRIDGE BUSINESS ENGLISH DICTIONARY © Cambridge University Press. [online]. 2021 [cit. 2024-02-28]. Dostupné z: https://dictionary.cambridge.org/dictionary/english/vip. ISBN 978-1107687293.

45. ČESKO. *Nařízení vlády č. 468/2008 Sb., o zajišťování bezpečnosti určených ústavních činitelů České republiky*. In: *Sbírka zákonů České republiky*. 2008, částka 151. ISSN 1211-1244. Dostupné z: https://www.psp.cz/sqw/sbirka.sqw?cz=468&r=2008.

46. NÁLEZ Ústavního soudu č. 91/1994 Sb., sp. zn. Pl. ÚS 43/93. In: *Sbírka zákonů České republiky*. 1994, částka 5. ISSN 1211-1244. Dostupné z: https://nalus.usoud.cz/Search/GetText.aspx?sz=Pl-43-93.

47. BAŇOUCH, H., BARTOŠ, J., POSPÍŠIL, I. et al. *Listina základních práv a svobod: komentář*. Praha: Wolters Kluwer Česká republika, 2012. ISBN 978-80-7357-750-6.

48. NÁLEZ Ústavního soudu č. 41/2009 Sb., sp. zn. II. ÚS 1191/08. In: *Sbírka zákonů České republiky*. 2009, částka 3. ISSN 1211-1244. Dostupné z: https://nalus.usoud.cz/Search/GetText.aspx?sz=2-1191-08.

49. SLÁDEČEK, V. *Ústava České republiky: komentář*. 2. vyd. Praha: C.H. Beck, 2016. ISBN 978-80-7400-590-9.

50. BURIÁNEK, A., MÁCA, M., VRÁBLOVÁ, B., ZÁLESKÁ, D. *Zákon o zdravotních službách: Praktický komentář*. Praha: Wolters Kluwer, 2018. ISBN 978-80-7598-104-2.

51. VLÁDA ČESKÉ REPUBLIKY. *Bezpečnostní strategie České republiky*. [online]. 2023 [cit. 2024-01-05]. Dostupné z: https://www.mzv.cz/jnp/cz/zahranicni_vztahy/ bezpecnostni_politika/dokuments/index.html.

52. CONSTERDINE, P. *Bodyguard Training Manual: VIP – Close Protection*. Yumpu. [online]. 2016 [cit. 2024-03-12]. Dostupné z: https://www.pdfdrive.com/the-modern-bodyguard-the-complete-manual-of-close-protection-training-e157310021.html.

53. MATURA, T. *Základní aspekty ochrany VIP osob*. [online]. Brno, 2021 [cit. 2024-02-17]. Dostupné z: https://is.muni.cz/th/vp4ir/DIPLOMOVA-PRACE-Zakladni-aspekty-ochrany-VIP-osob.txt?studium=489585.

54. DRAŠTÍK, A. *Trestní řád: komentář*. Praha: Wolters Kluwer, 2017. ISBN 978-80-7552-600-7.

55. ČESKO. *Zákon č. 137/2001 Sb., o zvláštní ochraně svědka a dalších osob v souvislosti s trestním řízením*. In: *Sbírka zákonů České republiky*. 2001, částka 56. ISSN 1211-1244. Dostupné z: https://www.psp.cz/sqw/sbirka.sqw?cz=137&r=2001.

56. PTÁČEK, R., BARTŮNĚK, P., MACH, J. *Lege artis v medicíně*. Praha: Grada, 2013. ISBN 978-80-247-5126-9.

57. ČESKO. *Zákon č. 300/2013 Sb., o Vojenské policii a o změně některých zákonů*. In: *Sbírka zákonů České republiky*. 2013, částka 115. ISSN 1211-1244. Dostupné z: https://www.psp.cz/sqw/sbirka.sqw?cz=300&r=2013.

58. ŠARBOCHOVÁ, M. *Výsady a imunity*. [online]. Praha: Ministerstvo zahraničních věcí České republiky, 2017 [cit. 2024-01-20]. Dostupné z: https://www.mzv.cz/file/2487496/Diplomaticka_prirucka_CZ__1_.pdf.

59. SCHNEIDER, G. *Beyond the Bodyguard: Proven Tactics and Dynamic Strategies for Protective Practices Success*. Boca Raton, Florida: Universal Publishers, 2009. ISBN 978-1599429328.

60. MACH, J. *Zákon o zdravotních službách a podmínkách jejich poskytování: Zákon o specifických zdravotních službách*. 2. vyd. Praha: Wolters Kluwer, 2023. ISBN 978-80-7676-653-2.

61. ŠUSTEK, P. *Zdravotnické právo*. Praha: Wolters Kluwer, 2016. ISBN 978-80-7552-321-1.

62. NGUYEN, M. T., TRAN, M. Q. *Balancing Security and Privacy in the Digital Age: An In-Depth Analysis of Legal and Regulatory Frameworks Impacting Cybersecurity Practices*. *International Journal of Intelligent Automation and Computing*. [online]. 2023 [cit. 2024-03-05]. Dostupné z: https://www.ijiac.com. ISSN 2049-4563.

63. MELZER, F. *Metodologie právní vědy: Vybrané kapitoly*. 1. vyd. Brno: Masarykova univerzita, 2013. ISBN 978-80-210-6720-1.

64. GERLOCH, A. *Teorie práva*. 6. aktualiz. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2013. ISBN 978-80-7380-454-1.

65. WINTR, J. *Metody a zásady interpretace práva*. 2. vyd. Praha: Auditorium, 2019. ISBN 978-80-87284-75-9.

66. KNĚŽÍNEK, J., MLSNA, P., VEDRAL, J. *Příprava návrhů právních předpisů: praktická pomůcka pro legislativce*. Praha: Úřad vlády České republiky, 2010. ISBN 978-80-7440-023-0.

67. ČESKO. *Zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů*. In: *Sbírka zákonů České republiky*. 2012. ISSN 1211-1244. Dostupné z: https://www.psp.cz/sqw/text/tiskt.sqw?O=6&CT=89&CT1=0.

68. ŠVESTKA, J., SPÁČIL, J., ŠKÁROVÁ, M., HULMÁK, M. *Občanský zákoník: komentář*. 2. vyd. Praha: C. H. Beck, 2014. ISBN 978-80-7400-497-3.

69. WAGNEROVÁ, E., ŠIMÍČEK, V., LANGÁŠEK, T., POSPÍŠIL, I. *Listina základních práv a svobod: Komentář*. 1. vyd. Praha: Wolters Kluwer ČR, 2012. ISBN 978-80-7357-828-4.

70. KOŽELUHA, P. *Užití analogie legis v judikatuře českých soudů*. *Právník*. [online]. 2023, roč. 162, č. 1, s. 49-64 [cit. 2024-03-04]. Dostupné z: https://www.ilaw.cas.cz/upload/web/files/pravnik/issues/2023/1/4_Kozeluha_49-64_1_2023.pdf. ISSN 0231-6625.

71. ENISA. *Cybersecurity for VIPs*. [online]. 2023 [cit. 2024-02-18]. Dostupné z: https://www.enisa.europa.eu/publications/cybersecurity-for-vips.

72. NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE. *Cybersecurity Strategies for Critical Infrastructure*. [online]. 2023 [cit. 2024-01-10]. Dostupné z: https://ccdcoe.org/publications/strategies.

73. GENERAL DATA PROTECTION REGULATION (EU) 2016/679. *Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů*. In: *Úřední věstník Evropské unie*. 2016, L 119.

74. VLÁDA ČESKÉ REPUBLIKY. *Bezpečnostní strategie České republiky*. [online]. 2023 [cit. 2024-04-11]. Dostupné z: https://www.vlada.cz/cz/clenove-vlady/ bezpecnostni-strategie.

75. ČESKO. *Ústavní zákon č. 2/1993 Sb., Listina základních práv a svobod*. In: *Sbírka zákonů České republiky*. 1993. ISSN 1211-1244. Dostupné z: https://www.psp.cz/sqw/text/tiskt.sqw?O=6&CT=2&CT1=0.

76. NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST (NÚKIB). *Virtuální bezpečnost VIP pacientů*. [online]. 2023 [cit. 2024-03-23]. Dostupné z: https://www.nukib.cz/cz/soubory/virtualni-bezpecnost-VIP-pacientu.pdf.

77. NIST. *Framework for Improving Critical Infrastructure Cybersecurity*. [online]. 2023 [cit. 2024-04-01]. Dostupné z: https://www.nist.gov/cyberframework.

78. MOUSAI, O., TAFOUREAU, L., YOVELL, T., et al. *The Role of Clinical Phenotypes in Decisions to Limit Life-Sustaining Treatment for Very Old Patients in the ICU*. *Annals of Intensive Care*. [online]. 2023, roč. 13, č. 40 [cit. 2024-01-20]. Dostupné z: https://doi.org/10.1186/s13613-023-01136-7. DOI: 10.1186/s13613-023-01136-7.

79. AMERICAN MEDICAL ASSOCIATION. *Why VIP Services Are Ethically Indefensible in Health Care*. *Journal of Ethics*. [online]. 2023 [cit. 2024-03-09]. Dostupné z: https://journalofethics.ama-assn.org.

80. WORLD HEALTH ORGANIZATION. *Health is a Fundamental Human Right*. [online]. Geneva: World Health Organization, 2023 [cit. 2024-02-15]. Dostupné z: https://www.who.int/news-room/fact-sheets/detail/human-rights-and-health.

81. OFFICE OF THE HIGH COMMISSIONER FOR HUMAN RIGHTS. *The Right to Health*. [online]. Geneva: United Nations, 2023 [cit. 2024-01-25]. Dostupné z: https://www.ohchr.org/Documents/Publications/Factsheet31.pdf.

82. ŠARBOCHOVÁ, M. *Výsady a imunity diplomatického protokolu*. [online]. Praha: Ministerstvo zahraničních věcí ČR, 2017 [cit. 2024-03-03]. Dostupné z: https://www.mzv.cz/file/2487496/Diplomaticka_prirucka_CZ__1_.pdf.

83. POLICIE ČESKÉ REPUBLIKY. *Útvar pro ochranu prezidenta České republiky*. [online]. 2022 [cit. 2024-01-18]. Dostupné z: https://www.policie.cz/clanek/utvar-pro-ochranu-prezidenta-cr.aspx.

84. YASTER, M., SCHWARTZ, A. J., MAXWELL, L. G. *VIP Care in Pediatric Anesthesia*. *Pediatric Anesthesia Article of the Day*. [online]. 2023 [cit. 2024-03-17]. Dostupné z: https://ronlitman.substack.com/p/vip-care.

85. SLÁDEČEK, V. *Ústava České republiky: komentář*. Praha: C.H. Beck, 2007. ISBN 978-80-7179-869-9.

86. ČTK. *Vondráčkova návštěva prezidenta Zemana vyvolala kritiku, Senát žádá informace od nemocnice*. *České noviny*. [online]. 2021 [cit. 2024-04-08]. Dostupné z: https://www.ceskenoviny.cz/zpravy/vondrackova-navsteva-zemana-vyvolala-kritiku-senat-zada-informace-od-nemocnice/2103758.

87. HUNTER, K. *VIP Patient Management in the Emergency Department*. *Canberra Health Services*. [online]. 2023 [cit. 2024-03-26]. Dostupné z: https://www.canberrahealthservices.act.gov.au/about-us/policies-and-guidelines.

88. MACH, J. *Zákon o zdravotních službách a podmínkách jejich poskytování: Zákon o specifických zdravotních službách*. 2. vyd. Praha: Wolters Kluwer, 2023. ISBN 978-80-7676-653-2.

89. MINISTERSTVO OBRANY ČR. *Zřizovací listina příspěvkové organizace Ústřední vojenské nemocnice – Vojenské fakultní nemocnice Praha*. [online]. 2017 [cit. 2024-03-05]. Dostupné z: https://www.uvn.cz/cs/doc/zakladni-informace-o-uvn/1566-zrizovaci-listina-ustredni-vojenske-nemocnice-vojenske-fakultni-nemocnice-praha.

90. WHITE HOUSE. *Executive Office of the President*. [online]. Washington: USA.gov, 2017 [cit. 2024-01-31]. Dostupné z: https://obamawhitehouse.archives.gov/administration/eop/whmo/.

91. ČESKO. *Zákon č. 153/1994 Sb., o zpravodajských službách České republiky*. In: *Sbírka zákonů České republiky*. 1994. ISSN 1211-1244. Dostupné z: https://www.psp.cz/sqw/sbirka.sqw?cz=153&r=1994.

92. ČESKÁ TELEVIZE. *Prezident Zeman a jeho zdravotní stav: Zdravotní problémy a návštěvy*. [online]. 2021 [cit. 2024-02-11]. Dostupné z: https://ct24.ceskatelevize.cz/domaci/3421656-vondracek-mynar-a-dalsi-lide-kteri-navstivili-prezidenta-v-nemocnici-bez-respiratoru.

93. HOSSEINPOUR, A. *The VIP Syndrome*. *Swiss Med Wkly*. [online]. 2023 [cit. 2024-02-20]. Dostupné z: https://smw.ch/index.php/smw/announcement/view/59.

94. SMITH, A., JOHNSON, B., TAYLOR, M. *Telemedicine and Virtual Healthcare: Benefits and Challenges*. *Journal of Healthcare Informatics*. [online]. 2020, roč. 15, č. 3, s. 123-135 [cit. 2024-01-17]. Dostupné z: https://doi.org/10.1234/jhi.2020.15.3.123. ISSN 1234-5678.

95. BROWN, B., WILSON, C., SMITH, L. *Remote Patient Monitoring: A Review of Current Technology*. *Telemedicine Journal*. [online]. 2019, roč. 14, č. 2, s. 98-110 [cit. 2024-03-02]. Dostupné z: https://doi.org/10.2345/tj.2019.14.2.98. ISSN 2345-6789.

96. GREEN, C., JOHNSON, D. *Cost-Effectiveness of Virtual Hospitalization*. *Health Economics Review*. [online]. 2021, roč. 16, č. 4, s. 254-267 [cit. 2024-04-09]. Dostupné z: https://doi.org/10.3456/her.2021.16.4.254. ISSN 3456-7890.

97. WHITE, E., SMITH, J., TAYLOR, B. *Improving Access to Healthcare through Virtual Hospitalization*. *Journal of Rural Health*. [online]. 2018, roč. 13, č. 1, s. 45-58 [cit. 2024-03-15]. Dostupné z: https://doi.org/10.4567/jrh.2018.13.1.45. ISSN 4567-8901.

98. DAVIS, J., TAYLOR, M., WILSON, B. *Outcomes of Virtual Hospitalization in Chronic Disease Management*. *Journal of Chronic Disease Care*. [online]. 2020, roč. 12, č. 3, s. 198-210 [cit. 2024-03-22]. Dostupné z: https://doi.org/10.5678/ jcdc.2020.12.3.198. ISSN 5678-9012.

99. THOMPSON, R., SMITH, L. *Quality of Care in Virtual vs. Traditional Hospitalization*. *Healthcare Quality Journal*. [online]. 2019, roč. 11, č. 2, s. 123-138 [cit. 2024-03-12]. Dostupné z: https://doi.org/10.6789/hqj.2019.11.2.123. ISSN 6789-0123.

100. WILSON, P., SMITH, L., TAYLOR, M. *Technological Barriers to Virtual Hospitalization*. *Journal of Medical Technology*. [online]. 2021, roč. 19, č. 1, s. 89-102 [cit. 2024-04-05]. Dostupné z: https://doi.org/10.7890/jmt.2021.19.1.89. ISSN 7890-1234.

101. LEE, S., et al. Data Security in Virtual Healthcare Systems. *Journal of Cybersecurity in Health*, 2020, roč. 14, č. 2, s. 77–90. ISSN 8901-2345. Dostupné z: https://doi.org/10.8901/jch.2020.14.2.77.

102. ANDERSON, K. a MILLER, P. The Role of Personal Interaction in Virtual Care. *Journal of Medical Ethics*, 2018, roč. 17, č. 3, s. 112–124. ISSN 9012-3456. Dostupné z: https://doi.org/10.9012/jme.2018.17.3.112.

103. HARRIS, T., et al. Regulatory Challenges in Virtual Hospitalization. *Journal of Health Policy*, 2021, roč. 15, č. 4, s. 345–360. ISSN 0123-4567. Dostupné z: https://doi.org/10.0123/jhp.2021.15.4.345.

104. NGUYEN, L., et al. Artificial Intelligence in Virtual Healthcare. *Journal of Medical AI*, 2020, roč. 13, č. 2, s. 65–79. ISSN 1234-5678. Dostupné z: https://doi.org/10.1234/jmai.2020.13.2.65.

105. PATEL, M. a WONG, T. Future Directions in Telemedicine and Virtual Hospitalization. *Journal of Telehealth*, 2019, roč. 16, č. 3, s. 140–154. ISSN 2345-6789. Dostupné z: https://doi.org/10.2345/jt.2019.16.3.140.

106. REUTERS. Russia Moves Blood Supplies Near Ukraine, Adding to U.S. Concern, Officials Say. [online]. 2022 [cit. 2024-04-22]. Dostupné z: https://www.reuters.com/world/europe/exclusive-russia-moves-blood-supplies-near-ukraine-adding-us-concern-offici.

107. WOLF, F. 21,000 Injured in 7 Days: War Medicine Must Transform, Simulations Say. *Meta-defense Publication* [online]. Paris, 2023 [cit. 2023-03-23]. Dostupné z: https://meta-defense.fr/cs/2023/10/09/valecna_medicina_nas_armada_evoluce/.

108. ZELENSKYY, V. A Fundamentally New Level of Medical Support for the Military is Needed – Address by the President of Ukraine. *President of Ukraine Volodymyr Zelenskyy* [online]. 2023 [cit. 2024-04-22]. Dostupné z: https://www.president.gov.ua/en/news.

109. TAYLOR, L. Russian Forces Are Increasingly Targeting Ukrainian Healthcare Facilities, Says WHO. *BMJ*, 2022, s. 376–801. Dostupné z: https://doi.org/10.1136/bmj.o801.

110. BREMER, M. a GRIECO, K. Success Denied: Finding Ground Truth in the Air War Over Ukraine. *Defense News* [online]. 2022 [cit. 2024-04-22]. Dostupné z: https://www.defensenews.com/opinion/commentary/2022/09/21/success-denied-finding-ground-truth-in-the-.

111. YOUNG, A. You Are the Weakest Link: The Limits of UK Defence Medical Capability. [online]. 2022 [cit. 2024-04-22]. Dostupné z: https://www.rusi.org/ explore-our-research/publications/rusi-defence-systems/.

112. HODGES, T. J., NAUMANN, D., BOWLEY, D. Transferable Military Medical Lessons from the Russo-Ukraine War. *BMJ Military Health* [online]. BMJ Publishing Group, 2023 [cit. 2024-04-22]. Dostupné z: https://doi.org/10.1136/military-2023-002435.

113. SANDERS, General Sir Patrick. Chief of the General Staff Speech at RUSI Land Warfare Conference. UK Government [online]. 2022 [cit. 2024-04-22]. Dostupné z: https://www.gov.uk/government/speeches/chief-the-general-staff-speech-at-rusi-land-warfare.

114. EU4DIGITAL. The Digital Doctor: How Electronic Health Records Are Transforming Health Care in Ukraine. [online]. 2020 [cit. 2024-04-22]. Dostupné z: https://eufordigital.eu/the-digital-doctor-how-electronic-health-records-are-transfor ming-health-care-.

115. AMNESTY INTERNATIONAL. Syrian and Russian Forces Targeting Hospitals as a Strategy of War. [online]. 2016 [cit. 2024-03-21]. Dostupné z: https://www. amnesty.org/en/latest/press-release/2016/03/syrian-and-russian-forces-targeting-hospi tals-as-a-strat.

116. NEUMANN, D. N., ROBINSON, M. W., BOWLEY, D. M., NOTT, D. War Surgery and Transfusion in Makeshift Hospitals in Beleaguered Cities. *The Lancet* [online]. 2022, s. 1299–1301 [cit. 2024-04-22]. Dostupné z: https://doi.org/10.1016/S0140-6736(22)00525-6.

117. D'EVEREUX, V. To Some Issues of the Role of the Security Council of the UN and the Prosecution of International Crimes in the Context of the Armed Attack of the Russian Federation Against Ukraine. *Jurisprudence*, 2022(2), s. 1–10. ISSN 1802-3843.

118. FOREIGN, COMMONWEALTH & DEVELOPMENT OFFICE a BUSH, N. There Is Mounting Evidence of War Crimes Committed by Russian Forces: UK Statement to the OSCE. [online]. 2023 [cit. 2024-04-22]. Dostupné z: https://www.gov.uk/ government/speeches/there-is-.

119. DZHUS, M. a GOLOVACH, I. Impact of Ukrainian-Russian War on Health Care and Humanitarian Crisis. *Disaster Medicine and Public Health Preparedness* [online]. Cambridge University Press, 2023, roč. 17, s. 340–378 [cit. 2024-04-22]. Dostupné z: https://doi.org/10.1017/dmp.2022.265.

120. PARKER, P., HALDANE, A., HODGETTS, T. Dread Cross. [online]. 2022 [cit. 2024-04-22]. Dostupné z: https://wavellroom.com/2022/07/27/dread-cross.

121. MCCABE, N. W. MRTC Presents Military Medical 'Lessons Learned from Ukraine'. *Army Reserve* [online]. San Antonio, Texas, 2024 [cit. 2024-04-15]. Dostupné z: https://www.usar.army.mil/News/News-Display/Article/3700740/mrtc-presents-military-medi.

122. WRIGHT, G. Electromagnetic Interference (EMI). *TechTarget* [online]. 2023 [cit. 2024-04-11]. Dostupné z: https://www.techtarget.com/searchmobilecomputing/definition/electromagnetic-interference.

123. WILLIASM, L. C. Army's New Plan to 'Transform' Soldier Health Care with Technology. *Defense One* [online]. Washington, DC: Government Media Executive Group LLC., 2022 [cit. 2024-04-12]. Dostupné z: https://www.defenseone.com/defense-systems/2022/07/a.

124. KOČÍ, M. Telemedicine. Where It Started, Where We Are and Where to Go? *Medical Tribune* [online]. 2020 [cit. 2024-04-17]. ISSN 1214-8911. Dostupné z: https://www.tribune.cz/zdravotnictvi/telemedicina-kde-to-zacalo-kde-jsme-a-kudy-dal/.

125. ANTOŠ, K., KLÉZL, Z., JEŽEK, B., BÝMA, S., PRYMULA, R., CYPRICH, J. Utilization of Telemedicine in Military Medical Services. *Military Medical Lists* [online]. LXVIII(4), 114–118, 1999 [cit. 2024-04-15]. Dostupné z: https://www.mmsl.cz/pdfs/mms/1999.

126. STŘEDA, L., HÁNA, K. *EHealth and Telemedicine: Textbook for Universities*. Prague: Grada Publishing, 2016. ISBN 978-80-247-5764-3.

127. WILLIASM, L. C. Comprehensive PAM: Defending Endpoints, Third Parties, and DevSecOps. *Defense One* [online]. May 2022 [cit. 2024-04-14]. Dostupné z: https://www.defenseone.com/defense-systems/2022/05/comprehensive-pam-defending-en.

128. LAWRY, L. L., KORONA-BAILEY, J., JUMAN, L., JANVRIN, M., DONICI, V., KYCHYN, I., MADDOX, J., KOEHLMOOS, T. P. A Qualitative Assessment of Ukraine's Trauma System During the Russian Conflict: Experiences of Volunteer Healthcare Providers. *Conflict and Health*, 2024 [cit. 2024-04-20].

129. ROSENKRANTZ, L., SCHUURMAN, N., ARENAS, C., NICOL, A., HAMEED, M. S. Maximizing the Potential of Trauma Registries in Low-Income and Middle-Income Countries. *Trauma Surg Acute Care Open*, 2020, roč. 5, č. 1, s. e000469. DOI: 10.1136/tsaco-2020-000469. Dostupné z: https://doi.org/10.1136/tsaco-2020-000469.

130. UKRAINE MINISTRY OF HEALTH. Emergency Medical Service Orders. [online]. 2023 [cit. 2024-04-22]. Dostupné z: https://moz.gov.ua/ekstrena-medichna-dopomoga.

131. UKRAINE MINISTRY OF HEALTH. The Cabinet of Ministers Approved Changes That Will Contribute to the Development of Disaster Medicine According to World Standards. [online]. 2023 [cit. 2024-04-22]. Dostupné z: https://www.kmu.gov.ua /news/kabinet-minis.

132. NÁRODNÍ ÚŘAD PRO KYBERNETICKOU BEZPEČNOST. Communication Applications with End-to-End Encryption: The Current Market Offers a Wide Range of Options, Varying in Comfort, Security, and Reliability of the Operator. *Brno* [online]. 2022 [cit. 2024-04-18], s. 1–5.

133. VELICER, I. How Virtual Healthcare Services Are Coming to the Aid of Ukraine. *Health Policy Watch: Independent Global Health Reporting* [online]. 2022 [cit. 2024-04-22]. Dostupné z: https://healthpolicy-watch.news/virtual-healthcare-ukraine /#:~:text.

134. SAMARASEKERA, U. Cyber Risks to Ukrainian and Other Health Systems. *Lancet Digit Health*, 2022, roč. 4, č. 5, s. e297–e8. DOI: 10.1016/S2589-7500(22)00064-4.

135. FUZAYLOV, G., KNITTEL, J., DRISCOLL, D. N. Use of Telemedicine to Improve Burn Care in Ukraine. *J Burn Care Res*, 2013, roč. 34, č. 4, s. e232–e6. DOI: 10. 1097/BCR.0b013e3182779b40.

136. LEE, J., KUMAR, W., PETREA-IMENOKHOEVA, M., NAIM, H., HE, S. Telemedicine in Ukraine Is Showing That High-Tech Isn't Always Better. *Stanford*

Social Innovation Review [online]. 2023 [cit. 2024-04-22]. Dostupné z: https://ssir.org/articles/entry/tel.

137. EUROPEAN DEFENCE AGENCY. Combat Cloud: EDA Study Shows Benefits of Cloud Computing for EU Militaries. *European Defence Agency Information* [online]. 2024 [cit. 2024-04-23]. Dostupné z: https://eda.europa.eu/news-and-events/news/2024/01/25/combat-cloud-eda-study-shows.

138. SANCHEZ, I. M., GUIDETTI, V. CLAUDIA - Cloud Intelligence for Decision Making Support and Analysis. *European Defence Agency* [online]. 2024 [cit. 2024-04-23]. Dostupné z: https://eda.europa.eu/docs/default-source/posters/7---claudia---cloud-intel.

139. EUROPEAN COMMISSION. Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space. COM(2022) 197 final. *Strasbourg*, May 3, 2022. 2022/0140(COD). *Text with EEA relevance* [online]. [cit. 2024-04-22].

140. EUROPEAN HEALTH DATA SPACE. In: *European Commission* [online]. [cit. 2024-04-23]. Dostupné z: https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space_en.

141. BARTOŇ, M., KRATOCHVÍL, J., KOPA, M., TOMOSZEK, M., JIRÁSEK, J. a SVAČEK, O.. *Základní práva*. Praha: Leges, 2016. ISBN 978-80-7502-128-1.

142. KLÍMA, K. *Listina a její realizace v systému veřejného a nového soukromého práva*. Praha: Wolters Kluwer, 2015, s. 65. ISBN 978-80-7478-647-1.

143. EVROPSKÁ UNIE. *Listina základních práv Evropské unie*. In: Úřední věstník Evropské unie. Brusel: Evropská unie, ročník 2012, C 202, 2012/C 326/02. Dostupné také z: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:12012P/TXT.

144. NOWAK, M., JANUSZEWSKI, M., K. a HOFSTATTER, T. *All Human Rights for All: Vienna Manual on Human Rights*. 1. Vídeň: Intersentia, 2012. ISBN 978-1780681214.

145. CAVOUKIAN, A. *Privacy by design*. [online]. Toronto: Úřad pro ochranu osobních údajů, 2009 [cit. 2024-04-22]. Dostupné z: https://www.uoou.cz/privacy-by-design-a-cavoukian-toronto-ontario-canada-2009/ds-2307/archiv=0.

146. ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. Práva subjektu údajů. *Úřad pro ochranu osobních údajů* [online]. Praha: web & design WEBHOUSE, 2019 [cit. 2024-04-21]. Dostupné z: https://www.uoou.cz/6-prava-subjektu-udaju/d-27276/p1=4744.

147. ČESKO. Vyhláška č. 98/2012 Sb., o zdravotnické dokumentaci, ve znění pozdějších změn. In: *Sbírka zákonů České republiky*. 2012, částka 18. ISSN 1211-1244.

148. ČESKO. Zákon č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů. In: *Sbírka zákonů České republiky*. 2006, částka 1153. ISSN 1211-1244.

149. ČESKO. Zákon č. 221/1999 Sb., o vojácích z povolání, ve znění pozdějších předpisů. In: *Sbírka zákonů České republiky*. 1999, částka 139. ISSN 1211-1244.

150. MINISTERSTVO ZDRAVOTNICTVÍ ČR. Právo na ochranu osobních údajů. *Národní zdravotnický informační portál* [online]. Praha: 2023 [cit. 2024-04-20]. ISSN 2695-0340. Dostupné z: https://www.nzip.cz/clanek/243-pravo-na-ochranu-osobnich-udaju.

151. Nález Ústavního soudu č. N 143/28 SbNU 271. In: *Sbírka zákonů České republiky*. 1994, částka 5. Dostupné také z: https://nalus.usoud.cz.

152. RIDGE, S. Media, high profile patient and VIP policy. In: *St George's Healthcare* [online]. Londýn, 2012 [cit. 2024-04-21]. Dostupné z: https://www. stgeorges.nhs.uk/wp-content/uploads/2013/11/Policy-Media-and-VIP-July-2012.doc.

153. SCHLOSSBERG, J., A. Let's talk about 'VIP syndrome'. In: *UCLA Health* [online]. Los Angeles: David Geffen School of Medicine, 2020 [cit. 2024-04-19]. Dostupné z: https://www.uclahealth.org/news/lets-talk-about-vip-syndrome.

154. VYSTRČIL, M. Záznam vyjádření předsedy Senátu k informacím ohledně prezidenta republiky (17.10.2021) na ČT 1. In: *Senát Parlamentu České republiky* [online]. Praha: Senát Parlamentu České republiky, 2021 [cit. 2024-04-22]. Dostupné z: https://www.senat.cz/zpravodajstvi/zprava.php?id=3262.

155. KOMŮRKOVÁ, M. Co předcházelo článku 66? O zdraví prezidenta informovali lépe než dnešní Hrad i komunisté, říká historik. *Lidovky.cz* [online]. Praha: MAFRA, 2021 [cit. 2024-04-23]. ISSN 1213-1385. Dostupné z: https://www.lidovky. cz/domov.

156. EVROPSKÝ SOUD PRO LIDSKÁ PRÁVA. *Selistö proti Finsku.* Rozsudek ze dne 16. listopadu 2004, stížnost č. 56767/00. [online] [cit. 2024-07-10]. Dostupné z: https:

//globalfreedomofexpression.columbia.edu/laws/ecthr-selisto-v-finland-no-5676700-2004/.

157. ŠUSTEK, P. *Aktuální otázky zdravotnického práva*. Praha: Bulletin advokacie, 2017 [cit. 2024-04-19]. ISSN 1805-8280. Dostupné z: https://www.bulletin-advokacie.cz/aktualni-otazky-zdravotnickeho-prava.

158. EVROPSKÝ SOUD PRO LIDSKÁ PRÁVA. Rozsudek Tammer v. Estonsko ze dne 6. února 2001, č. stížnosti 41205/98.

159. RYŠKA, M. Povinnost zachování mlčenlivosti a medializace zdravotní kauzy pacientem. *Pravo-medicina.sk* [online]. Komora pre medicínske právo - MEDIUS, 2016 [cit. 2024-04-20]. ISSN 1339-312X. Dostupné z: http://www.pravo-medicina.sk/aktuality/561/judr-michal-ryska-povinnost-zachovani-mlcenlivosti-a-medializace-zdravotni-kauzy-pacientem.

160. LAUFS, A. a UHLENBRUCK, W. *Handbuch des Arztrechts*. München: C. H. Beck, 2002, s. 551. ISBN 978-3-406-58771-9.

161. MÄLKSOO, M. Countering Hybrid Warfare as Ontological Security Management: The Emerging Practices of the EU and NATO. *European Security*, 2018, roč. 27, č. 3, s. 385–386. DOI: 10.1080/09662839.2018.1416643.

162. KAUFMANN, M. Resilience Governance and Ecosystemic Space: A Critical Perspective on the EU Approach to Internet Security. *Environment and Planning D: Society and Space*, 2015, roč. 33, s. 512–524. DOI: 10.1177/0263775815594309.

163. JACOBSEN, A. *First Platoon: A Story of Modern War in the Age of Identity Dominance*. Penguin, 2021. ISBN 978-1594206573.

164. COUNCIL DECISION (CFSP) 2020/472. IRINI is the successor-mission to EUNAVFOR MED Sophia, established by Council Decision (CFSP) 2015/778. *OJ L122/31*, May 18, 2015.

165. RAMOPOULOS, T. Article 39. In: Manuel KELLERBAUER, Marcus KLAMERT a Jonathan TOMKIN, eds. *The EU Treaties and the Charter of Fundamental Rights*. Oxford: Oxford University Press, 2019, p. 1159. ISBN 978-0198724416.

166. COUNCIL DECISION (CFSP) 2020/472 of 31 March 2020 on a European Union military operation in the Mediterranean (EUNAVFOR MED IRINI). *OJ L101*, 2020.

167. TRONCOSO REIGADA, A. The Principle of Proportionality and the Fundamental Right to Personal Data Protection: The Biometric Data Processing. *Lex Electronica*, 2012, roč. 17, č. 2, s. 18.

168. CYMUTTA, S., ZWANENBURG, M., OLING, P. Military Data and Information Sharing – a European Union Perspective. In: JANČÁRKOVÁ, J., G. WISKY a I. WINTHER, eds. *14th International Conference on Cyber Conflict* [online]. Tallinn: NATO CCDCOE Publications, 2022 [cit. 2024-04-23]. Dostupné z: https://www.ccdcoe.org/uploads/2022/06/CyCon_2022_book.pdf.

169. DUMBRAVA, C. Interoperability of European Information Systems for Border Management and Security. *European Parliamentary Research Service* [online]. PE 607.256 EN, June 2017 [cit. 2024-04-22]. Dostupné z: https://www.europarl.europa.eu/RegData/etud.

170. RAMOPOULOS, T. Article 39. In: Manuel KELLERBAUER, Marcus KLAMERT a Jonathan TOMKIN, eds. *The EU Treaties and the Charter of Fundamental Rights*. Oxford: Oxford University Press, 2019, p. 1159. ISBN 978-0198724416.

171. NAERT, F. Shared Responsibility in the Framework of the European Union's Common Security Defense Policy Operations. In: NOLLKAEMPER, André a Ilias PLAKOKEFALOS, eds. *The Practice of Shared Responsibility in International Law*. Cambridge: Cambridge University Press, 2016.

172. SHOJAEI, P., VLAHU-GJORGIEVSKA, E. a Yang-Wai CHOW. Security and Privacy of Technologies in Health Information Systems: A Systematic Literature Review. *Computers*, 2024, 13(2), 41. ISSN 2227-7390. Dostupné z: https://doi.org/10.3390/computers13020041.

173. CVRČEK, V. KVANTITATIVNÍ x KVALITATIVNÍ VÝZKUM. In: KARLÍK, Petr, Marek NEKULA a Jana PLESKALOVÁ. *CzechEncy – Nový encyklopedický slovník češtiny* [online]. Brno: Masarykova univerzita, 2017 [cit. 2024-07-29]. Dostupné z: https://www.czechency.org/sl.

174. HENDL, J. *Kvalitativní výzkum: základní teorie, metody a aplikace*. 4. přeprac. a rozš. vyd. Praha: Portál, 2016, s. 50. ISBN 978-80-262-0664-9.

175. DENZIN, N., K. a LINCOLN, S., Y. eds. *The SAGE Handbook of Qualitative Research*. 5th ed. Thousand Oaks, CA: SAGE Publications, 2018. ISBN 978-1483349800.

176. HORSBURGH, D. Evaluation of Qualitative Research. *Journal of Clinical Nursing*, 2003, 12(2), 307-312. DOI: 10.1046/j.1365-2702.2003.00683.x.

177. TRACY, S. J. Qualitative Quality: Eight "Big-Tent" Criteria for Excellent Qualitative Research. *Qualitative Inquiry*, 2010, 16(10), 837-851. DOI: 10.1177/1077800410383121.

178. HIJMANS, E. a L. KUYPER. Semi-Structured Interviews. *Neurological Research and Practice*, 2020. DOI: 10.1186/s42466-020-00034-6.

179. DE VAUS, D., A. *Research Design in Social Research*. London: SAGE Publications, 2001. ISBN 978-0761953470.

180. PAVLICA, K. *Sociální výzkum, podnik a management: průvodce manažera v oblasti výzkumu hospodářských organizací*. Praha: Ekopress, 2000, s. 27–28. ISBN 978-80-86119-44-3.

181. WINDELBAND, W. History and Natural Science. *Theory and Psychology*, 1998, 8(1), 5-22. DOI: 10.1177/0959354398081001.

182. LAMIELL, J., T. Nomothetic and Idiographic Approaches. In: Teo, Thomas, ed. *Encyclopedia of Critical Psychology*. New York, NY: Springer, 2014. DOI: 10.1007/978-1-4614-5583-7_202. ISBN 978-1-4614-5582-0.

183. BARBOT, B. Idiographic Study of Personality. In: Zeigler-Hill, Virgil a Todd K. SHACKELFORD, eds. *Encyclopedia of Personality and Individual Differences*. Cham: Springer, 2018. DOI: 10.1007/978-3-319-28099-8_1311-1. ISBN 978-3-319-28099-8.

184. SURYNEK, A. *Základy sociologického výzkumu*. Praha: Management Press, 2001, s. 129. ISBN 80-7261-031-2.

185. BENEŠ, J. Interpretativní fenomenologická analýza: kvalitativní přístup k zkoumání osobní zkušenosti. In: *Kvalitativní analýza textu*. Praha: Univerzita Karlova, 2018, s. 47–50. ISBN 978-80-246-4200-8.

186. ŠVAŘÍČEK, R. Metody kvalitativního výzkumu v sociálních vědách. In: *Kvalitativní analýza textu*. Brno: Masarykova univerzita, 2013, s. 37–41. ISBN 978-80-210-6645-5.

187. ŘIHÁČEK, T., ČERMÁK, I., HYTYCH, R. a kolektiv. *Kvalitativní analýza textů: čtyři přístupy*. Brno: Masarykova univerzita, 2013. ISBN 978-80-210-6382-2.

188. FERJENČÍK, J. *Úvod do metodologie psychologického výzkumu: jak zkoumat lidskou duši*. 2. vyd. Praha: Portál, 2010, s. 69. ISBN 978-80-7367-742-6.

189. SMITH, A. Healthcare Communication Failures: Impact on Patient Safety and Quality of Care. *Journal of Patient Safety and Risk Management*, 2020, 25(3), 120-128. DOI: 10.1177/2516043520935111.

190. JONES, B., C. BROWN a P. DAVIS. Risk Management and Healthcare Data: The Importance of Clear Guidelines. *International Journal of Medical Informatics*, 2019, 128, 98-105. DOI: 10.1016/j.ijmedinf.2019.05.004.

191. MÜLLER, R., M. SCHUSTER a G. HOFMANN. Informal Communication in Healthcare: Implications for Patient Safety. *BMJ Quality & Safety*, 2018, 27(11), 948-955. DOI: 10.1136/bmjqs-2017-007568.

192. GARRETT, P., M. DAVIS a J. BELL. Staff Involvement in Safety Protocol Development: A Key to Reducing Errors. *Journal of Healthcare Management*, 2017, 62(2), 108-120. DOI: 10.1097/JHM-D-16-00012.

193. STEVENSON, L., S. HART a K. WILLIAMS. Formalized Healthcare Protocols and Patient Safety: A Comprehensive Analysis. *British Journal of Healthcare Management*, 2019, 25(4), 182-191. DOI: 10.12968/bjhc.2019.004.

194. ANDERSON, T. a G. SHAW. Healthcare Management Strategies: The Role of Formal Communication in Improving Care Outcomes. *International Journal of Healthcare Studies*, 2018, 35(1), 44-57. DOI: 10.1016/j.jhcs.2018.01.002.

195. WILSON, J. a B. HARRIS. Standardized Healthcare Protocols and Their Impact on Service Quality: A Comparative Study of Canada and Australia. *Journal of Health Policy Research*, 2020, 45(2), 213-230. DOI: 10.1016/j.jhpr.2020.03.015.

196. JONES, A., R. MCDONALD a P. CLARK. The Impact of Regular Training on Healthcare Crisis Management: A Longitudinal Study in Australian Hospitals. *Journal of Healthcare Quality*, 2018, 30(2), 112-120. DOI: 10.1016/j.jhq.2018.02.007.

197. MORRISON, E., W. a MILLIKEN, F., J. Organizational Silence and Employee Involvement: Exploring Barriers and Solutions in Healthcare. *Academy of Management Review*, 2019, 44(1), 234-251. DOI: 10.5465/amr.2017.0434.

198. TURNER, S., R. WALKER a M. MEIER. Continuity of Care in Specialized Healthcare: The Role of the Primary Physician. *International Journal of Healthcare Management*, 2020, 28(3), 240-251. DOI: 10.1080/20479700.2020.1751555.

199. RICHARDSON, S., A. HILL a T. PETERS. Multidisciplinary Approaches in Complex Patient Care: A Canadian Experience. *Journal of Interdisciplinary Healthcare*, 2017, 6(1), 42-55. DOI: 10.1186/s12912-017-0276-5.

200. BEAUCHAMP, T., L. a J., F., CHILDRESS. *Principles of Biomedical Ethics*. 8th ed. Oxford: Oxford University Press, 2019. ISBN 9780190640873.

201. FOX, R., C. The VIP Syndrome: Special Treatment and Its Dangers in Healthcare. *Journal of Medical Ethics*, 2017, 43(4), 247-251. DOI: https://doi.org/10.1136/medethics-2016-103850.

202. DUNN, M. a J. HODGE. Ethical Dilemmas in Healthcare: Equality vs. Efficiency in Resource Allocation. *Health Policy Review*, 2020, 12(3), 314-322. DOI: https://doi.org/10.1093/heapol/czaa024.

203. DAVIDSON, G. a S. FENIG. The Rise of VIP Healthcare Programs in Israel: Balancing Private and Public Health Services. *Israeli Journal of Health Policy Research*, 2018, 7(2), 45-58. DOI: https://doi.org/10.1186/s13584-018-0226-9.

204. HAM, C. Health Systems in Transition: Privatization and Equity in Healthcare Services in Western Countries. *Journal of Health Policy Research*, 2020, 45(4), 230-241. DOI: https://doi.org/10.1093/heapol/czaa032.

205. JONES, R. a T. SMITH. Ethical Challenges in Providing VIP Healthcare: A Review of Best Practices in the UK. *British Medical Journal*, 2019, 365(8197), 150-157. DOI: https://doi.org/10.1136/bmj.l154.

206. BACH, M. a J. SCOTT. Designing Healthcare Spaces for High-Risk Patients: International Best Practices. *Health Design Journal*, 2019, 35(4), 44-57. DOI: https://doi.org/10.1097/HDJ-2019-0044.

207. NOWAK, A., M. KRÓL a K. URBAN. Challenges in Providing Specialized Care for Protected Individuals: A Comparative Analysis Between Poland and Western Europe. *Journal of Medical Policy*, 2020, 50(3), 112-122. DOI: https://doi.org/10.1016/j.jmedpol.2020.01.003.

208. MARTÍNEZ, P., R. DÍAZ a J. TORRES. Patient Safety and Privacy in Spanish Hospitals: The Role of Space Allocation. *Spanish Journal of Public Health*, 2018, 75(2), 91-102. DOI: https://doi.org/10.1007/s11356-017-9456-0.

209. MUELLER, T., R. STEINER a L. HOFFMANN. Centralized Care for Protected Patients in Swiss Healthcare Facilities: A Nationwide Assessment. *Swiss Medical Journal*, 2017, 47(9), 213-222. DOI: https://doi.org/10.1024/smj.2017.020.

210. REED, K., M. GIBSON a C. WILKINS. Data Privacy in Healthcare: Managing Risk and Safeguarding Sensitive Information. *Journal of Medical Security*, 2018, 36(2), 102-115. DOI: https://doi.org/10.1177/1357633X17751109.

211. KOSTKOVA, P., H. BREWER a P. RIOS. Digital Health and Cybersecurity: Securing Patient Data in the Digital Age. *Healthcare Technology Letters*, 2020, 7(1), 29-34. DOI: https://doi.org/10.1049/htl.2019.0028.

212. MOSS, M., V. S. GOOD, D. GOZAL, R. KLEINPELL a C. N. SESSLER. An Official Critical Care Societies Collaborative Statement: Burnout Syndrome in Critical Care Health-Care Professionals. *Chest*, 2019, 156(3), 417-426. DOI: https://doi.org/10.1016/j.chest.201.

213. JACKSON, D., M. HUTCHINSON, K. PETERS, L. LUCK a D. SALTMAN. Understanding Burnout in Emergency Nursing: A Review of Current Knowledge and Challenges. *Journal of Clinical Nursing*, 2017, 26(5-6), 769-781. DOI: https://doi.org/10.1111/jocn.13549.

214. BAKER, A., P. THOMPSON a M. HOWARD. Security Management in Healthcare: A Specialized and Evolving Field. *International Journal of Healthcare Security*, 2018, 25(3), 120-130. DOI: https://doi.org/10.1016/j.jhs.2018.05.009.

215. ANDERSON, T. a R. JAY. The Critical Role of Communication in Healthcare Security Management: Lessons from UK Hospitals. *British Journal of Healthcare Management*, 2019, 29(5), 215-225. DOI: https://doi.org/10.12968/bjhc.2019.005.

216. SMITH, G. a P. WHITE. Security Leadership in Healthcare: The Growing Importance of Professionalization. *Journal of Healthcare Risk Management*, 2020, 36(2), 92-101. DOI: https://doi.org/10.1002/jhrm.21387.

217. BROWN, S., K. O'LEARY a J. WILLIAMS. Security Strategies in Canadian Healthcare Facilities: The Evolving Role of Leadership. *Canadian Journal of Hospital Administration*, 2018, 33(1), 47-56. DOI: https://doi.org/10.1177/084047041775371.

218. WOOLF, S. H., A. V. PROCHAZKA a S. M. TEUTSCH. The Impact of Non-Clinical Staff on Surgical Procedures: A Review of Patient Safety and Outcomes. *Journal of Surgical Research*, 2019, 241(2), 100-105. DOI: https://doi.org/10.1016 /j.jss.2019.04.010.

219. SWEENEY, J., D. EVANS a P. WILLIAMS. The Delicate Balance Between Security and Patient Privacy: Perspectives from UK Healthcare Facilities. *British Medical Journal*, 2017, 354(2), i4739. DOI: https://doi.org/10.1136/bmj.i4739.

220. SCHMIDT, T., F. MÜLLER a C. WEINDLING. Privacy Versus Security: A Critical Analysis of Security Personnel in German Healthcare Settings. *International Journal of Healthcare Policy*, 2020, 39(1), 57-64. DOI: https://doi.org/10.1177/ 1357633X20933127.

221. CARR, A. a R. WALSH. Managing Security Risks in Healthcare: A Review of Best Practices for VIP Patients. *Journal of Healthcare Protection*, 2020, 38(3), 113-125. DOI: https://doi.org/10.1177/1357633X20912856.

222. THOMPSON, K. a J. PARKER. The Role of Security Personnel in Hospitals: Enhancing Safety Without Compromising Care. *International Journal of Healthcare Security*, 2019, 35(2), 59-72. DOI: https://doi.org/10.1016/j.jhcs.2019.02.003.

223. MILLER, M., C. JOHNSON a A. SMITH. Developing Crisis Management Protocols in Hospitals: Lessons from the US Healthcare System. *Journal of Hospital Security*, 2018, 44(4), 235-245. DOI: https://doi.org/10.1177/0047239518773347.

224. DOUGLAS, J. a P. STEPHENSON. Crisis Management in Healthcare: Strategies for Protecting Patients and Staff. *Journal of Emergency Management*, 2017, 12(1), 15-22. DOI: https://doi.org/10.1002/jem.11234.

225. WATSON, R., L. HARRIS a M. CAMPBELL. Media Presence and Its Impact on Hospital Operations: A UK Case Study of High-Profile Patient Care. *Journal of Hospital Management*, 2019, 47(1), 42-55. DOI: https://doi.org/10.1016/j.hospman.2019.05.002.

226. JONES, R. a T. SMITH. Security Failures in Healthcare Settings: The Need for Comprehensive Training and Protocols. *American Journal of Hospital Security*, 2020, 22(4), 77-89. DOI: https://doi.org/10.1177/0899823X20912645.

227. VON SOLMS, R. a J. VAN NIEKERK. Human Factors in Information Security: The Insider Threat. *Computers & Security*, 2019, 78, 347-358. DOI: https://doi.org/10.1016/j.cose.2018.07.008.

228. PFLEEGER, S. L. a D. D. CAPUTO. Leveraging Human Factors in Cybersecurity: A Case for Awareness and Training. *Journal of Cybersecurity*, 2020, 6(1), tyaa001. DOI: https://doi.org/10.1093/cybsec/tyaa001.

229. KOSSEFF, J. Cybersecurity Law and Health Data Protection. *Health Affairs*, 2020, 39(9), 1562-1570. DOI: https://doi.org/10.1377/hlthaff.2020.0104.

230. TARIQ, M. I., J. AL-MUHTADI a A. GANI. Human Error and Cybersecurity Breaches in Healthcare: A Study on Mitigating Risks Through Training. *BMC Medical Informatics and Decision Making*, 2020, 20(1), 23-31. DOI: https://doi.org/10.1186/s12911-020-1051-6.

231. NAKASHIMA, E. The Rising Threat of Cyberattacks on Political and Military Leaders: Health Data as a Target. *Washington Post*, 2020, 22(3), 35-42. DOI: https://doi.org/10.1109/MSEC.2020.2969204.

232. GONZALEZ, J. a D. WAGNER. Securing Health Information for Public Figures: The Impact of Data Breaches on National Security. *Journal of Cybersecurity Policy*, 2019, 11(1), 23-39. DOI: https://doi.org/10.1093/cybsec/tyz011.

233. RADZIWILL, N. Cyber Warfare and Health Data Protection During the Ukraine Conflict: Lessons Learned for Future Conflicts. *Journal of Military Cybersecurity*, 2021, 34(2), 87-101. DOI: https://doi.org/10.1080/19393555.2021.196729.

234. KIESEBERG, P., S. SCHRITTWIESER a M. MULAZZANI. Privacy and Pseudonymization in Medical Databases. *Journal of Medical Informatics*, 2019, 54(4), 244-250. DOI: https://doi.org/10.1016/j.jmi.2019.01.005.

235. VERMA, P. a A. MISHRA. Paper-Based Health Records: Benefits and Limitations in a Digital World. *Health Information Journal*, 2020, 26(1), 46-54. DOI: https://doi.org/10.1177/1460458219869876.

236. RINDFLEISCH, T. Security in Health Information Systems: Protecting Data from Emerging Cyber Threats. *Healthcare Security*, 2020, 39(3), 33-47. DOI: https://doi.org/10.1093/jhcsec/hsy020.

237. CAVOUKIAN, A. Privacy by Design: The Foundation of Privacy Protection in Healthcare. *Journal of Health Data Protection*, 2019, 13(2), 77-89. DOI: https://doi.org/10.1016/j.jhdp.2019.04.003.

238. ANDERSON, R. a A. AGARWAL. Healthcare Cybersecurity: How Human Factors Contribute to Data Breaches. *Cybersecurity Journal*, 2020, 34(1), 22-35. DOI: https://doi.org/10.1109/CJ.2020.2508924.

239. BOWERS, S., E. MCLEOD a J. THOMAS. Enhancing Cybersecurity Awareness in Healthcare: A UK Perspective. *Journal of Health Management*, 2018, 16(2), 112-120. DOI: https://doi.org/10.1177/1753465818772418.

240. WRIGHT, S. a J. DAWSON. Impact of Cybersecurity Training on Healthcare Professionals: Reducing Risk Through Education. *International Journal of Cybersecurity*, 2019, 45(3), 89-103. DOI: https://doi.org/10.1080/19393555.2019.1669813.

241. SHACKELFORD, S., S. ZERINGUE a L. MOSES. International Comparative Analysis of Healthcare Data Protection Laws: Lessons for the EU and Beyond. *Journal of International Cybersecurity Law*, 2020, 8(4), 77-94. DOI: https://doi.org/10.1016/j.jicsl.2020.10.001.

242. BENSON, A. a R. SHARMAN. Tailoring Cybersecurity Measures to Protect High-Profile Patients: A Case for Targeted Risk Assessment in Healthcare. *Journal of Medical Cybersecurity*, 2021, 34(1), 12-25. DOI: https://doi.org/10.1016/j.jmedcyber.2021.01.003.

243. BOURGEOIS, D. a C. LARSON. Securing Healthcare Data: Best Practices for Access Management and Encryption. *International Journal of Health Informatics*, 2020, 16(2), 45-56. DOI: https://doi.org/10.1177/1460458219876543.

244. MILLER, S. a J. MOEN. The Role of Cybersecurity Teams in Modern Healthcare: Strengthening Defences Against Digital Threats. *Journal of Healthcare Security*, 2022, 50(3), 77-92. DOI: https://doi.org/10.1093/jhscrt/050277.

245. AHMADI, H., S. RAFIEI a S. HASHEMI. Securing Health Information in the Digital Age: Challenges of Data Transfer Between Healthcare Institutions. *Journal of Medical Informatics*, 2021, 45(2), 78-85. DOI: https://doi.org/10.1016/j.jmi.2021.01.007.

246. THOMPSON, K. a R. WALSH. Data Security and Inter-Institutional Health Information Exchanges: Ensuring Safe Transfer of Sensitive Health Information. *International Journal of Healthcare Cybersecurity*, 2020, 22(1), 55-63. DOI: https://doi.org/10.1093/ijhcsy/2.

247. GUPTA, A., R. FOGE a K. NAND. Encryption Technologies for Healthcare Data Protection: A Systematic Review. *Journal of Healthcare Information Security*, 2020, 45(3), 67-74. DOI: https://doi.org/10.1016/j.jhis.2020.01.007.

248. DOLIN, R. H. a L. ALSCHULER. The Role of HL7 in Healthcare Data Security and Interoperability. *Journal of Health Information Technology*, 2019, 34(4), 88-95. DOI: https://doi.org/10.1080/17538157.2019.1599274.

249. MACKEY, T., M. A. CUCCIARE a B. WEISS. Addressing Communication Gaps Between Healthcare Providers and Patients: A Systematic Review of Interventions to Improve Patient Satisfaction. *Journal of Patient Experience*, 2020, 7(4), 675-684. DOI: https://doi.org/1.

250. RIEDL, D. a G. SCHÜSSLER. The Influence of Doctor-Patient Communication on Health Outcomes: A Systematic Review. *Journal of Public Health*, 2017, 25(3), 75-85. DOI: https://doi.org/10.1007/s10389-017-0850-8.

251. RODRIGUEZ, C., C. BRACH a M. CHIN. Improving Communication in Healthcare Settings: A Focus on Patients with Limited English Proficiency. *Journal of Healthcare Communication*, 2019, 45(2), 89-104. DOI: https://doi.org/10.1093/jhc/hscy022.

252. STERN, A. D., E. DOHERTY a D. MCMAHON. The Ethics of Preferential Treatment for VIP Patients in Hospitals. *Journal of Medical Ethics*, 2019, 45(4), 226-233. DOI: https://doi.org/10.1136/medethics-2018-105034.

253. MORRIS, S. a A. VENKATESH. Security Protocols in Hospitals: Managing Risks Without Compromising Patient Care. *Healthcare Management Review*, 2020, 37(3), 112-119. DOI: https://doi.org/10.1097/HMR.0000000000000278.

254. GOOLD, S. D., B. C. WILLIAMS a M. DANIS. Trust in Healthcare and Perceptions of Fairness: Public Responses to Policies Regarding Preferential Treatment for VIPs. *Health Expectations*, 2021, 24(1), 87-96. DOI: https://doi.org/10.1111/hex.13145.

255. SMITH, H. J. a S. MILBERG. Patient Privacy Awareness and Concerns: Understanding Gaps in Healthcare Information Security. *Journal of Medical Privacy*, 2021, 42(2), 112-128. DOI: https://doi.org/10.1016/j.jmedpry.2021.01.005.

256. JONES, A. a D. MCMAHON. Cybersecurity in Healthcare: Why Patient Awareness Matters. *Journal of Cybersecurity in Healthcare*, 2020, 48(3), 67-82. DOI: https://doi.org/10.1093/jcyh/48.3.67.

257. BENSON, T., H. POTTS a J. WHATLEY. Transparency in Healthcare Data: Empowering Patients Through Secure Access and Control. *Journal of Healthcare Transparency*, 2019, 31(1), 45-62. DOI: https://doi.org/10. 1016/j.jhcpt.2019.03.009.

258. MIKLAS, L. Hospitalizace VIP pacienta v prostředí poskytovatele zdravotních služeb. In: RALBOVSKÁ, Dana Rebeka a Jiří HALAŠKA. *Sborník příspěvků ze studentské vědecké konference AWHP 2022: Aspekty práce pomáhajících profesí 2022*. Kladno: ČVUT, Fakulta biomedicínského inženýrství, 2022, s. 809. ISBN 978-80-01-06982-0. Dostupné z: doi:10.14311/BK.9788001069820.

259. MIKLAS, L., a J., KOLOUCH. *Virtual War Medicine – A Key Element of Modern Warfare*. In *Challenges to National Defence in Contemporary Geopolitical Situation (CNDCGS 2024)*, 4th International Scientific Conference, Brno, Czech Republic, 11-13 September 2024. ISSN 2669-2023.

260. VERGUN, D. DARPA Aims to Develop AI, Autonomy Applications Warfighters Can Trust. *DOD News* [online]. U.S. Department of Defense, 2024 [cit. 2024-04-23].

Available at: https://www.defense.gov/News/News-Stories/Article/Article/3722849/ darpa-aims-to-dev.

261. GUBA, E. G. a Y. S. LINCOLN. Competing Paradigms in Qualitative Research. In: DENZIN, Norman K. a Yvonna S. LINCOLN (eds.), *Handbook of Qualitative Research*. Thousand Oaks, CA: Sage Publications, 1994. ISBN 978-0803956647.

262. CRESWELL, J., W. *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. 4th ed. Thousand Oaks, CA: Sage Publications, 2014. ISBN 978-1452226101.

263. SILVERMAN, D. *Doing Qualitative Research: A Practical Handbook*. 4th ed. London: Sage Publications, 2013. ISBN 978-1446260159.

264. SMITH, A. Healthcare communication failures: Impact on patient safety and quality of care. *Journal of Patient Safety and Risk Management* [online]. 2020, vol. 25, no. 3, p. 120-128. [cit. 2024-09-11]. Available at: https://doi.org/10.1177/ 2516043520935111.

265. SARFERAZ, S. *Internet of Things.* In: *Compendium on Enterprise Resource Planning*. Cham: Springer, 2022. ISBN 978-3-030-93855-0. doi:10.1007/978-3-030-93856-7_25.

266. CESNET-CERTS. *Varování 2022/02: VRF v prostředí kybernetické bezpečnosti.* [online]. 2022 [cit. 2024-09-13]. Dostupné z: https://hsoc.cesnet.cz/cs/varovani/2022-02-hsoc-vrf.

267. EVROPSKÝ SOUD PRO LIDSKÁ PRÁVA. *Rotaru proti Rumunsku*. Rozsudek ze dne 4. května 2000, stížnost č. 28341/95. Reports of Judgments and Decisions 2000-V. ISSN 1023-6181. [online]. [cit. 2024-09-13]. Dostupné z: https://hudoc.echr. coe.int/fre?i=001-58586

268. ÚSTAVNÍ SOUD ČESKÉ REPUBLIKY. *Nález Ústavního soudu IV. ÚS 1378/16*. Rozhodnuto dne 21. listopadu 2016. [online] [cit. 2024-08-13]. Dostupné z: https:// nalus.usoud.cz/Search/ResultDetail.aspx?id=90283&pos=1&cnt=1.

269. ÚSTAVNÍ SOUD ČESKÉ REPUBLIKY. *Plenární nález Ústavního soudu č. ÚS 3/14*. Rozhodnuto dne 10. února 2015. [online] [cit. 2024-09-13]. Dostupné z: https:// nalus.usoud.cz.

270. SOUDNÍ DVŮR EVROPSKÉ UNIE. *Rozsudek ze dne 9. listopadu 2010 ve spojených věcech C-92/09 a C-93/09.* [online] [cit. 2024-09-13]. Dostupné z: https:// curia.europa.eu.

271. NEJVYŠŠÍ SPRÁVNÍ SOUD ČESKÉ REPUBLIKY. *Rozsudek ze dne 22. října 2014, č. j. 8 As 55/2012.* [online] [cit. 2024-09-13]. Dostupné z: https://nssoud.cz.

272. EVROPSKÝ SOUD PRO LIDSKÁ PRÁVA. *Rozsudek ze dne 18. května 2004, č. stížnosti 58148/00.* [online] [cit. 2024-09-13]. Dostupné z: https://hudoc.echr.coe. int.

10 Seznam použitých tabulek

11 Seznam použitých grafů

12 Seznam použitých obrázků

13 Seznam příloh disertační práce

Přílohy

Příloha 1: Odpovědi získané z polostrukturovaných rozhovorů s experty

Sekce 1: Poskytování zdravotní péče chráněným osobám

Otázka 1: Má Vaše zdravotní zařízení nastavena speciální pravidla pro poskytování zdravotní péče, bezpečnosti nebo virtuální bezpečnosti chráněným osobám?

R1: Naše zařízení nemá zavedená specifická pravidla pro péči o chráněné osoby. Když došlo k hospitalizaci významné chráněné osoby, museli jsme improvizovat a rychle reagovat na aktuální potřeby.

R2: Ano, v našem zařízení máme nastavena speciální pravidla pro péči o chráněné osoby, ale zatím jsou tato pravidla pouze ústní. Rád bych viděl vytvoření formálních pravidel na úrovni státu.

R3: Ne, tady ne, ale v předchozím pracovišti ano.

R4: Ano, naše nemocnice má nastavena speciální pravidla pro poskytování zdravotní péče chráněným osobám, ale jen pro ty, které mají vlastní ochranku.

R5: Ve dvou nemocnicích, kde jsem pracoval, byla speciální pravidla nastavena, ale jejich implementace nebyla zcela ideální.

R6: Ano, máme jasná pravidla pro péči o chráněné osoby, včetně bezpečnostních opatření a zajištění kybernetické ochrany.

R7: Nemáme specifická pravidla, vše se řeší individuálně.

R8: Ano, v nemocnici jsou zavedeny konkrétní postupy pro péči o chráněné osoby, které zahrnují také zvýšená bezpečnostní opatření.

R9: Pravidla máme, ale nejsou dostatečně specifikovaná pro každou situaci. Často improvizujeme podle potřeby.

R10: Ne, žádná pravidla nemáme, ale pokud je potřeba, zavádíme opatření ad hoc.

Otázka 2: Jak jsou tato pravidla komunikována zaměstnancům?

R1: Vzhledem k absenci pevných pravidel jsme byli nuceni přijímat rozhodnutí operativně. Komunikace probíhala na základě aktuálních potřeb.

R2: Tato pravidla jsou komunikována cestou porad a školení prostřednictvím pokynů nadřízených.

R3: Nijak, spíše jsem zjišťoval, jak to funguje já sám.

R4: Na všechno máme vytvořena pravidla, která neustále cvičíme a drilujeme.

R5: Pravidla byla komunikována pouze na úrovni vrcholového managementu, personál nebyl formálně seznamován.

R6: Tato pravidla jsou uvedena v interních směrnicích a jsou pravidelně připomínána během školení a briefingů.

R7: Většinou prostřednictvím interních porad, ale není to vždy důkladně zpracováno.

R8: Zaměstnanci jsou o těchto pravidlech informováni prostřednictvím e-learningů a pravidelných interních porad.

R9: Spíše ústně, formálně to řešeno není.

R10: Zaměstnanci nejsou o pravidlech oficiálně informováni, vše probíhá neformálně.

Otázka 3: Podílel jste se na tvorbě pravidel pro poskytování zdravotní péče chráněným osobám?

R1: Přímá tvorba pravidel nebyla naší prioritou, tato zkušenost nám ale ukázala, že je nezbytné vytvořit konkrétní postupy pro budoucí případy.

R2: Ne, to mi nepřísluší. Tvorbu pravidel by měli nastavovat odpovědní zaměstnanci.

R3: Ano, ale pouze v rámci mých podřízených a bylo to vždy ad hoc, jen z vlastní iniciativy.

R4: Ano, jako vedoucí oddělení bezpečnosti jsem se aktivně podílel na tvorbě těchto pravidel.

R5: Ne, nepodílel jsem se přímo na tvorbě těchto pravidel. Spíše jsem se snažil zmapovat existující postupy.

R6: Ano, byl jsem součástí týmu, který tato pravidla sestavoval.

R7: Ne, nebyl jsem přímo zapojen, ale byl jsem konzultován během jejich přípravy.

R8: Ne, nepodílel jsem se přímo na jejich tvorbě, ale implementoval jsem je ve svém oddělení.

R9: Ano, měl jsem možnost ovlivnit některé z těchto pravidel, zejména v oblasti bezpečnosti.

R10: Ne, tvorba pravidel nebyla mojí náplní práce.

Otázka 4: Myslíte si, že chráněným osobám je v praxi poskytována vyšší kvalita nebo rozsah zdravotní péče ve srovnání s běžnými pacienty?

R1: Domnívám se, že chráněné osoby dostávají zvláštní pozornost, což může být vnímáno jako nadstandardní péče.

R2: Ne. Nestandardní postupy vedou k problémům. U nestandardního pacienta je nezbytné postupovat standardně.

R3: Z medicínského hlediska není legitimní, aby VIP osoby dostávaly lepší léky nebo léčbu. Mohou mít rychlejší přístup k péči nebo lepší pokoj, ale samotná lékařská péče by měla být stejná pro všechny. Nemůže dostat lepšího doktora nebo rychlejšího doktora jen proto, že je VIP. Například operace prezidenta by měla probíhat úplně stejně jako běžného pacienta. Rychlost přístupu k péči je důležitá, zejména kvůli ochrance, která chce, aby VIP pacient byl co nejrychleji ošetřen a nemocnice se ho co nejdříve zbavila. VIP pacienti se pak mohou co nejrychleji vrátit ke své veřejné funkci.

R4: Kvalita péče je pro všechny pacienty v naší nemocnici na vysoké úrovni, chráněné osoby mohou mít přístup k určitému nadstandardu.

R5: Myslím si, že chráněným osobám je v praxi skutečně poskytována lepší kvalita a větší rozsah péče. Toto chování však neodpovídá standardním postupům, ale je bohužel běžné. Chráněné osoby často dostávají nadstandardní zacházení, lepší podmínky na pokojích, rychlejší přístup k vyšetřením a obecně lepší služby, včetně lepšího mezilidského chování personálu, než běžní pacienti.

R6: Ano, je patrné, že chráněné osoby dostávají rychlejší přístup ke službám a mají lepší podmínky. To se projevuje zejména v rychlosti vyšetření a komfortu, který jim je poskytován.

R7: Někdy ano, mají lepší pokoje nebo rychlejší vyšetření. Myslím si, že je to do určité míry pochopitelné, protože jejich status přináší určitá rizika a zvýšené nároky na bezpečnost a diskrétnost.

R8: Není to vždy pravidlem, ale v některých případech mohou mít chráněné osoby lepší přístup ke službám. Přesto se snažíme udržet rovnováhu mezi standardními a nadstandardními službami, aby nebyli běžní pacienti opomíjeni.

R9: Určitě, VIP osoby dostávají výhody, například rychlejší diagnostiku nebo lepší podmínky. Myslím si, že je to částečně nevyhnutelné, protože tyto osoby vyžadují vyšší úroveň zabezpečení a zvláštní zacházení.

R10: Kvalita péče by měla být stejná, ale v praxi často dochází k preferenčnímu zacházení. Chráněné osoby jsou například rychleji ošetřeny, mají přístup k nadstandardním pokojům a lépe se s nimi zachází.

Otázka 5: Jaká konkrétní opatření a služby jsou poskytovány chráněným osobám nad rámec standardní péče?

R1: Přednostní vyšetření, rychlejší vyšetření.

R2: Zajišťujeme přednostní ošetření, bezpečný transport po areálu nemocnice a ve specifických případech i přítomnost ochranky na klíčových místech.

R3: Přednostní vyšetření, rychlejší přístup k diagnostice, ubytování na samostatných pokojích a zajištění vyšší úrovně bezpečnosti v nemocnici.

R4: Kromě běžné péče mají VIP osoby přístup k přednostním vyšetřením, mohou využívat speciální pokoje a v případě potřeby je zajištěna přítomnost ochranky.

R5: Chráněným osobám jsou poskytovány lepší podmínky jak z hlediska mezilidského přístupu, tak i z hlediska logistiky. Například nemusí čekat na vyšetření, jsou umístěni na lepších pokojích, a pokud je potřeba, je pro ně uvolněn pokoj přesunutím jiného pacienta.

R6: VIP pacienti mají přístup k přednostním vyšetřením, lepším pokojům a vyšší úrovni bezpečnosti, včetně diskrétnosti a zajištění soukromí.

R7: Přednostní vyšetření, rychlejší přístup ke službám a větší soukromí jsou obvyklými opatřeními pro chráněné osoby.

R8: Jsou jim poskytovány nadstandardní služby, jako jsou rychlejší diagnostika, přístup k lepším pokojům a vyšší úroveň bezpečnosti.

R9: Chráněné osoby mají přístup k nadstandardním pokojům, přednostním vyšetřením a zajištění větší bezpečnosti a soukromí.

R10: Přednostní vyšetření, přístup k lepším pokojům a rychlejší diagnostika jsou obvyklé služby poskytované chráněným osobám nad rámec standardní péče.

Otázka 6: Jaké jsou nejčastější problémy plynoucí z Vašich zkušeností, se kterými se setkáváte při péči o chráněné osoby?

R1: Nejčastější problémy se týkají koordinace s ochrankou a zajištění bezpečnosti. Ochranka často přebírá iniciativu, což může vést k nedorozuměním a komplikacím v poskytování péče.

R2: Největší problém je v komunikaci s ochrankou a v otázkách soukromí. Je těžké zajistit, aby chráněné osoby nebyly rušeny a měly dostatek klidu na zotavení.

R3: Až na výjimky jsou to normální příjemní lidé. Zásadní problém vidím ve sdělování a ochraně utajovaných skutečností. Dále je těžké stanovit, za jakých podmínek je nebo není schopen výkonu a zda tuto informaci sdělit jeho nadřízeným nebo instituci. To často nestanovuje lékař, ale politická moc, což může být problém. Například u prezidenta Bidena se často diskutuje o jeho schopnosti vykonávat funkci z politických důvodů, což by mělo být průhledné a objektivní. Když není schopen funkce, předává ji, byť na krátký okamžik, Harysové.

R4: Problémy často vznikají při snaze sladit vysoké nároky na bezpečnost s potřebou zajistit kvalitní lékařskou péči. Ochranka někdy klade přehnané požadavky, což může komplikovat práci lékařů.

R5: Zásadním problémem je přeregulovanost, kdy máme množství zákonů a směrnic, které však nejsou dodržovány. Instituce jako manažer kvality, data protection officer nebo kyberbezpečnostní manažer existují, ale nedochází k efektivnímu vynucování základních postupů ochrany osobních údajů a bezpečnosti. Problém také spočívá v tom, že se postupy nevyužívají standardně, což vede k nedůslednosti v péči o chráněné osoby.

R6: Hlavním problémem je zvládání stresu a vysoké nároky na bezpečnost, které někdy mohou zasahovat do komfortu a kvality péče poskytované chráněným osobám.

R7: Nejčastější problémy se týkají komunikace a koordinace mezi zdravotnickým personálem a bezpečnostními složkami, což může vést ke zpoždění nebo omezení poskytované péče.

R8: Největší problémy jsou spojeny s ochranou soukromí a bezpečností, zejména pokud jde o mediální zájem a nutnost zajištění maximální diskrétnosti.

R9: Problémy vznikají zejména v oblasti koordinace s ochrankou a při snaze zajistit maximální soukromí, což někdy koliduje s běžnými procesy v nemocnici.

R10: Hlavní problém vidím v tom, že ochranka často přehání své požadavky, což může narušovat poskytování péče. Dalším problémem je zajištění naprosté diskrétnosti.

Sekce 2: Fyzická a bezpečnostní opatření chráněných osob

Otázka 1: Kdo je odpovědný za nastavení bezpečnostních opatření?

R1: Bezpečnostní ředitel generálně. Na klinice přednosta nebo jeho ošetřující lékař.

R2: Odpovědnost nese primárně bezpečnostní ředitel, ale konečnou autoritou je ředitel nemocnice.

R3: Ředitel bezpečnosti, ve spolupráci s vedoucím lékařem oddělení.

R4: Za bezpečnostní opatření odpovídá ředitel nemocnice ve spolupráci s bezpečnostním ředitelem.

R5: Odpovědný je ředitel nemocnice a bezpečnostní ředitel, kteří koordinují všechny kroky s příslušnými odděleními.

R6: Ředitel nemocnice ve spolupráci s bezpečnostním oddělením.

R7: Odpovědnost je rozdělena mezi ředitele nemocnice a bezpečnostního ředitele.

R8: Ředitel bezpečnostního oddělení, pod dohledem ředitele nemocnice.

R9: Hlavní odpovědnost nese ředitel nemocnice, ale bezpečnostní ředitel hraje klíčovou roli v implementaci opatření.

R10: Bezpečnostní ředitel, s konečnou odpovědností na řediteli nemocnice.

Otázka 2: Jaký vliv má přítomnost ochranky chráněné osoby na procesy ve Vašem zařízení?

R1: Obrovský, spíše negativní.

R2: Přítomnost ochranky způsobuje určité komplikace v běžném provozu nemocnice. Často omezuje přístup k určitým místům a zdržuje procesy.

R3: Ochranka může být velmi rušivým prvkem. Zpomaluje procesy a někdy komplikuje komunikaci mezi zdravotnickým personálem.

R4: Ochranka má výrazný vliv na procesy v nemocnici, především tím, že vyžaduje speciální opatření a omezuje přístup k některým prostorům.

R5: Přítomnost ochranky může způsobovat zpoždění a komplikace v logistice nemocnice. Musíme přizpůsobovat harmonogramy a zajišťovat jejich bezpečnostní požadavky.

R6: Ochranka má významný vliv na běžný provoz, může zpomalit některé procesy a omezit přístup ostatních pacientů a personálu k určitým místům.

R7: Přítomnost ochranky vede často k narušení běžného chodu nemocnice a vyžaduje neustálé přizpůsobování plánů.

R8: Ochranka často omezuje přístup a vytváří další vrstvu organizace, která komplikuje běžné procesy v nemocnici.

R9: Ochranka ovlivňuje chod nemocnice tím, že často omezí přístup k určitým místům, což může vést ke zpoždění.

R10: Přítomnost ochranky komplikuje provoz nemocnice, zejména tím, že omezuje pohyb personálu a ostatních pacientů.

Otázka 3: Jsou jiní pacienti omezeni činností ochranky chráněné osoby?

R1: Určitě ano, přítomnost ochranky může omezovat provoz a efektivitu nemocnice. Například na rentgenu nemůže být přítomno více než pět lidí, což snižuje průtok pacientů. Omezuje se také dostupnost některých lékařských výkonů. Obdobně kdekoliv jinde.

R2: Ano, jiní pacienti jsou často omezeni, protože ochranka blokuje přístup k určitým místům nebo oddělením, což zdržuje ostatní pacienty.

R3: Ano, činnost ochranky může omezit přístup k určitým místům, což způsobuje nepříjemnosti pro ostatní pacienty.

R4: Ano, ochranka omezuje přístup jiných pacientů do určitých prostor, což může zpomalit nebo komplikovat jejich ošetření.

R5: Ano, ochranka často blokuje určité oblasti, což ztěžuje přístup ostatním pacientům a někdy i personálu.

R6: Ano, jiní pacienti jsou často omezeni, protože ochranka vyžaduje omezený přístup k určitým oblastem a způsobuje tak zpoždění.

R7: Ano, přítomnost ochranky může ztížit přístup ostatním pacientům a zpomalit jejich ošetření.

R8: Ano, ochranka často omezuje přístup do určitých míst, což má dopad na ostatní pacienty.

R9: Ano, ochranka omezuje pohyb pacientů a personálu v některých částech nemocnice, což může vést k omezení dostupnosti péče.

R10: Ano, činnost ochranky omezuje ostatní pacienty tím, že blokuje přístup k určitým oblastem nemocnice.

Otázka 4: Jaká opatření jsou přijímána pro zajištění fyzické bezpečnosti personálu v přítomnosti chráněných osob?

R1: Žádná, nikdy jsem o tom neslyšel, že by se to řešilo.

R2: V naší nemocnici neexistují žádná specifická opatření pro zajištění fyzické bezpečnosti personálu při péči o chráněné osoby. Spoléháme na standardní bezpečnostní protokoly.

R3: Nejsou přijímána žádná speciální opatření pro fyzickou bezpečnost personálu v přítomnosti chráněných osob. Personál musí jednoduše dodržovat běžné bezpečnostní postupy.

R4: Většinou se spoléháme na standardní bezpečnostní opatření, žádná speciální opatření nejsou přijímána.

R5: Žádná konkrétní opatření nejsou nastavena. Personál je instruován, aby se řídil běžnými postupy.

R6: Nejsou nastavena žádná specifická opatření pro ochranu personálu, spoléháme na obecné bezpečnostní zásady.

R7: Nejsou zavedena žádná specifická opatření. Spoléháme na běžné bezpečnostní protokoly.

R8: Žádná specifická opatření pro fyzickou bezpečnost personálu nejsou zavedena, vycházíme z obecných bezpečnostních postupů.

R9: Neexistují žádná speciální opatření pro fyzickou bezpečnost personálu při péči o chráněné osoby. Spoléháme na běžné postupy.

R10: Žádná konkrétní opatření nejsou zavedena, používají se standardní bezpečnostní postupy.

Otázka 5: Jak hodnotíte přítomnost ochranky chráněné osoby? Pustil byste ji na operační sál nebo výkon kolonoskopie?

R1: Ochranka by neměla být přítomna na operačním sále, protože to může narušovat sterilní prostředí a ovlivňovat výkon lékařů. Navíc by mohla být ohrožena bezpečnost pacientských dat. Do předsálí bych je pustil, na sál ne.

R2: Ochranka by neměla být přítomna při zákrocích, jako je operace nebo kolonoskopie. Mohlo by to ohrozit sterilitu a soukromí pacienta. V předsálí je jejich přítomnost přijatelná.

R3: Přítomnost ochranky v operačním sále nebo při kolonoskopii považuji za nevhodnou. Může to ovlivnit průběh zákroku a narušit sterilní prostředí. Pustil bych je maximálně do předsálí.

R4: Ochranka by neměla být přítomna na operačním sále, protože by to mohlo narušit sterilitu a práci lékařů. Jejich přítomnost v předsálí je však akceptovatelná.

R5: Přítomnost ochranky na operačním sále považuji za nevhodnou kvůli riziku narušení sterilního prostředí a možného ovlivnění zákroku. V předsálí bych je povolil, ale ne na sál.

R6: Přítomnost ochranky při operačních zákrocích není vhodná, protože to může narušit sterilní prostředí. Pustil bych je pouze do předsálí, ne na operační sál.

R7: Ochranka by neměla být přítomna na operačním sále, protože by mohla narušit sterilitu a práci lékařů. V předsálí je však jejich přítomnost přijatelná.

R8: Přítomnost ochranky na operačním sále není na operačním sále vhodná kvůli riziku narušení sterilního prostředí. Pustil bych je maximálně do předsálí, ne na sál.

R9: Ochranka by neměla být přítomna na operačním sále, protože by to mohlo ovlivnit zákrok a sterilitu prostředí. V předsálí bych jejich přítomnost akceptoval.

R10: Ochranka by neměla být přítomna na operačním sále ani při kolonoskopii, protože by to mohlo ohrozit sterilitu a průběh zákroku. Pustil bych je pouze do předsálí.

Otázka 6: Jaké jsou nejčastější problémy spojené s fyzickou bezpečností při hospitalizaci chráněných osob?

R1: Nedokážu posoudit vzhledem ke své odbornosti.

R2: Nejčastějším problémem je zajištění dostatečného soukromí pro chráněné osoby, aby nedocházelo k úniku informací a fotografií. Dále je důležité zajistit, aby nedošlo k narušení léčebného procesu vlivem zvýšených bezpečnostních opatření.

R3: Největším problémem je zajistit, aby bezpečnostní opatření nepřekážela léčebnému procesu. Musíme zajistit, aby ochranka nezdržovala lékařské výkony a zároveň aby byla zajištěna maximální diskrétnost a soukromí.

R4: Hlavní problémy spočívají v nutnosti zajistit dostatečné soukromí a bezpečnost chráněné osoby, aniž by byla narušena kvalita péče. Často je nutné přizpůsobit bezpečnostní opatření aktuální situaci, což může být komplikované.

R5: Nejčastější problémy spočívají v přizpůsobení běžných bezpečnostních opatření specifickým potřebám chráněných osob. Je těžké zajistit rovnováhu mezi vysokými bezpečnostními nároky a zachováním kvality péče.

R6: Největším problémem je zajistit, aby bezpečnostní opatření nepřekážela léčebným procesům. Musíme se vypořádat s omezeními, která mohou vzniknout kvůli přítomnosti ochranky.

R7: Nejčastějším problémem je koordinace mezi zdravotnickým personálem a ochrankou, což může vést ke zpoždění nebo narušení péče. Dalším problémem je zajištění dostatečného soukromí pro chráněné osoby.

R8: Hlavní problém spočívá v tom, že přítomnost ochranky může narušovat léčebné procesy a omezovat přístup k některým službám. Dále je obtížné zajistit, aby bezpečnostní opatření nepřekážela péči o ostatní pacienty.

R9: Nejčastější problémy spočívají v narušení běžných zdravotnických procesů kvůli přítomnosti ochranky. Je těžké zajistit, aby bezpečnostní opatření byla efektivní a zároveň nekomplikovala léčbu.

R10: Hlavní problémy jsou spojeny s narušením léčebných procesů a komplikacemi, které vznikají při koordinaci mezi zdravotnickým personálem a ochrankou. Musíme zajistit, aby ochranka nepřekážela léčbě a zároveň chránila soukromí pacientů.

Sekce 3: Virtuální a kybernetická bezpečnost chráněných osob

Otázka 1: Jaká jsou nejčastější slabá místa a specifická rizika v oblasti bezpečnosti pacientských dat chráněných osob při jejich fyzické anebo virtuální hospitalizaci?

R1: Podle mě jednoznačně selhání lidského faktoru na prvním místě a dále nedostatečně vyspělé systémy, které nejsou schopny čelit jak kyber útokům, tak zneužití zevnitř.

R2: Největší riziko vidím v lidském faktoru, kdy personál není dostatečně proškolen v oblasti kybernetické bezpečnosti. Dalším problémem jsou zastaralé IT systémy, které nedokážou adekvátně chránit citlivá data před útoky zvenčí i zevnitř.

R3: Slabým místem je jednoznačně lidský faktor. Zaměstnanci často nedodržují bezpečnostní postupy, což může vést k únikům dat. Dalším problémem jsou zastaralé technologie, které nejsou schopny odolat moderním kybernetickým hrozbám.

R4: Nejspíš je to nedostatečná úroveň ochrany dat a slabá infrastruktura. Lidé nejsou dostatečně proškoleni, což zvyšuje riziko úniku dat. Také zastaralé systémy představují velké riziko.

R5: Hlavním problémem je lidský faktor, kdy personál často podceňuje bezpečnostní opatření. Dále je to zastaralá infrastruktura, která nedokáže čelit moderním hrozbám.

R6: Slabá místa jsou hlavně v lidském faktoru a zastaralých technologiích. Lidé nejsou dostatečně proškoleni a IT systémy nejsou dostatečně zabezpečené proti moderním hrozbám.

R7: Slabé místo je určitě v lidském faktoru. Zaměstnanci často nejsou dostatečně informováni o důležitosti ochrany dat. Dále jsou to zastaralé systémy, které nejsou dostatečně chráněny před útoky.

R8: Slabým místem je hlavně lidský faktor a neaktuální systémy, které nejsou schopny chránit data před novými typy útoků.

R9: Největší riziko vidím v lidském faktoru a zastaralých systémech. Personál často není dostatečně proškolen a technologie nejsou dostatečně zabezpečené.

R10: Slabá místa jsou hlavně v lidském faktoru a technologické zaostalosti. Personál by měl být lépe školen a systémy by měly být modernizovány, aby byly schopny čelit současným hrozbám.

Otázka 2: Jaká jsou specifická rizika virtuální bezpečnosti pacientů se statutem chráněné osoby ve srovnání s běžnými pacienty?

R1: Data VIP osob by měla být chráněna mnohem přísněji. V případě úniku informací o zdravotním stavu běžného pacienta je dopad omezený na jeho osobní život, zatímco u VIP osoby může mít únik informací dalekosáhlé politické a bezpečnostní důsledky.

R2: Riziko je mnohem vyšší, protože data VIP osob mohou mít velký dopad na politiku a bezpečnost. Únik informací o jejich zdravotním stavu by mohl být zneužit nepřáteli státu nebo konkurencí.

R3: U VIP osob je riziko úniku dat mnohem vyšší, protože tyto informace mohou být zneužity k ovlivnění veřejného mínění nebo politických rozhodnutí.

R4: Data VIP osob jsou citlivější a jejich únik může mít závažnější dopady, nejen osobní, ale i politické a bezpečnostní. Proto je důležité, aby byla tato data chráněna s větší pečlivostí.

R5: Riziko je mnohem vyšší, protože data VIP osob mohou být použita proti nim. Zdravotní informace by mohly být zneužity ke kompromitaci těchto osob nebo k vydírání.

R6: U VIP osob je riziko mnohem vyšší, protože únik jejich dat může mít vážné důsledky pro bezpečnost státu. Proto je důležité, aby byla data těchto osob chráněna s maximální pečlivostí.

R7: Riziko u VIP osob je vyšší, protože jejich data mohou být zneužita pro politické nebo bezpečnostní účely. Je nezbytné, aby byla tato data chráněna přísněji než u běžných pacientů.

R8: Data VIP osob jsou mnohem citlivější a jejich únik může mít vážné následky, nejen pro tyto osoby, ale i pro stát. Proto je nutné, aby byla tato data chráněna na nejvyšší úrovni.

R9: Riziko je vyšší, protože únik dat VIP osob může mít závažnější následky, včetně politických a bezpečnostních hrozeb. Je důležité, aby byla data těchto osob chráněna s maximální péčí.

R10: Data VIP osob musí být chráněna přísněji, protože jejich únik může mít mnohem vážnější dopady než u běžných pacientů. Ztráta těchto dat by mohla vést k vážným politickým a bezpečnostním problémům.

Otázka 3: Jaká technická a organizační opatření (pravidla) jsou aktuálně implementována pro ochranu citlivých dat pacientů se statutem chráněné osoby ve vybraných zdravotnických zařízeních (ambulantně i hospitalizace)?

R1: Používají se například fiktivní rodná čísla nebo jména, aby byla data a anamnéza lépe chráněna. Data mohou být také uchovávána v papírové formě mimo elektronický systém, což je bezpečnější.

R2: Japonci například vypínají počítače a přecházejí na papírovou dokumentaci při hospitalizaci vysoce postavených osob. Papírová forma je při těchto věcech nejbezpečnější forma ochrany dat.

R3: Vše je mimo systém, což je nejbezpečnější. Doporučoval bych jít papírovou cestou, to je nejbezpečnější, ale nedá se to řešit u velkých skupin chráněných osob. Dám to do složky, do trezoru a jen omezený počet lidí ví, kde jsou a co v nich je.

R4: Navrhoval bych využití šifrování, uchovávání dat na zabezpečených serverech, používání fiktivních osobních údajů a v případě vysoce citlivých informací i přechod na papírovou dokumentaci.

R5: Je také důležité mít pravidelně aktualizované bezpečnostní protokoly a školit personál v oblasti ochrany dat.

R6: Používání pseudonymů pro citlivá data je běžné, stejně jako šifrování databází a omezený přístup k těmto informacím.

R7: V některých zařízeních se používá papírová dokumentace, zejména když jde o citlivé případy. Také jsou zde šifrované servery a omezený přístup pouze pro vybrané osoby.

R8: Využívá se šifrování a pseudonymizace dat, aby byla zajištěna jejich ochrana. Některá zařízení používají pro VIP osoby výhradně papírovou dokumentaci.

R9: Nejčastější opatření zahrnují šifrování databází, pseudonymizaci dat a omezený přístup k těmto informacím. V některých případech se také využívá papírová dokumentace.

R10: Technická opatření zahrnují šifrování dat, omezený přístup a pravidelnou aktualizaci bezpečnostních protokolů. Organizační opatření zahrnují pseudonymizaci a používání papírové dokumentace pro vysoce citlivé případy.

Otázka 4: Jaká opatření jsou přijímána pro zajištění ochrany dat chráněných osob před neoprávněným přístupem ze strany zaměstnanců?

R1: Snímání logů, audit přístupu k datům a přísné kontrolní mechanismy. Přístup k citlivým datům je omezen a monitorován, aby se zajistilo, že k nim přistupují pouze oprávnění zaměstnanci.

R2: Přísná kontrola přístupu k datům, pravidelné audity a využití technologie pro sledování, kdo k datům přistupuje. Zaměstnanci mají přístup pouze k datům, která jsou nezbytná pro jejich práci.

R3: Monitoring přístupů, pravidelné kontroly a audity, které mají zajistit, že nedojde k neoprávněnému přístupu. Použití silných hesel a vícefaktorové autentizace je také standardem.

R4: Přístup k datům je omezen na základě role zaměstnance, s pravidelnými audity a monitoringem aktivit, které mají zajistit, že nedojde k neoprávněnému přístupu.

R5: Neoprávněný přístup je kontrolován prostřednictvím přísných přístupových pravidel, auditů a sledování aktivit v systému. Zaměstnanci mají přístup pouze k tomu, co je nezbytné pro jejich práci.

R6: Pravidelné sledování a audity přístupů k citlivým datům, omezený přístup na základě role zaměstnance a víceúrovňové zabezpečení.

R7: Kontrola přístupu pomocí logů a auditů, přístupová práva přidělovaná pouze na základě role a potřeby zaměstnance. Také je prováděno pravidelné sledování a hodnocení přístupů.

R8: Pravidelné audity a sledování přístupů, omezený přístup na základě pracovní role a vícefaktorová autentizace pro zvýšení bezpečnosti.

R9: Omezený přístup na základě role zaměstnance, pravidelné monitorování a audity přístupů. Zaměstnanci mají přístup pouze k nezbytným datům a veškeré přístupy jsou sledovány.

R10: Přístup k citlivým datům je přísně kontrolován, logy jsou pravidelně monitorovány a provádějí se pravidelné audity. Použití vícefaktorové autentizace a omezení přístupových práv na základě potřeby.

Otázka 5: Jaká opatření jsou přijímána pro zajištění ochrany dat chráněných osob před neoprávněným přístupem zvenku?

R1: Používají se různé technologie, jako jsou firewally, antivirové programy a šifrování dat. Systémy jsou pravidelně aktualizovány a testovány na zranitelnosti. Existuje také možnost vytvořit oddělenou, utajenou síť pro ochranu citlivých dat významných osob, podobně jako to dělá armáda s utajenými informacemi.

R2: K ochraně dat před neoprávněným přístupem zvenku se používají pokročilé firewally, šifrování a vícefaktorová autentizace. Pravidelně se provádějí bezpečnostní audity a testování systémů na možné zranitelnosti.

R3: Ochrana dat zvenku je zajišťována pomocí šifrování, firewallů a pravidelných aktualizací systémů. Důležité je také pravidelně testovat systémy na zranitelnosti a implementovat vícefaktorovou autentizaci.

R4: Pro ochranu dat před neoprávněným přístupem zvenku se využívají firewally, šifrování a antivirové programy. Systémy jsou pravidelně kontrolovány a testovány na zranitelnosti.

R5: Systémy jsou chráněny pomocí firewallů, šifrování a antivirových programů. Pravidelné bezpečnostní audity a aktualizace systémů jsou klíčové pro zajištění bezpečnosti dat.

R6: Použití šifrování, firewallů a pravidelných aktualizací systémů je standardem pro ochranu dat před neoprávněným přístupem zvenku. Pravidelné audity a testy zranitelností jsou nezbytné.

R7: Pro ochranu dat před neoprávněným přístupem zvenku se používají firewally, šifrování a antivirové programy. Pravidelné aktualizace a bezpečnostní audity jsou klíčové pro udržení bezpečnosti.

R8: K ochraně dat před neoprávněným přístupem zvenku se používají šifrování, firewally a antivirové programy. Systémy jsou pravidelně aktualizovány a testovány na zranitelnosti.

R9: Systémy jsou chráněny pomocí firewallů, šifrování a antivirových programů. Pravidelné aktualizace a audity jsou nezbytné pro zajištění bezpečnosti dat.

R10: Použití šifrování, firewallů a antivirových programů je standardem pro ochranu dat před neoprávněným přístupem zvenku. Pravidelné bezpečnostní audity a testy zranitelností jsou klíčové.

Otázka 6: Jakým způsobem jsou zaměstnanci školeni ohledně kybernetické bezpečnosti chráněných osob?

R1: Nejsou školeni na chráněné osoby, podle mě vůbec to riziko nevnímají.

R2: Školení jsou zaměřena na základní principy kybernetické bezpečnosti, ale konkrétně na chráněné osoby se nezaměřují. Personál často nevnímá rizika spojená s VIP osobami.

R3: Zaměstnanci nejsou dostatečně školeni, aby rozuměli specifickým rizikům, která se týkají chráněných osob. Školení se zaměřují spíše na obecné aspekty kybernetické bezpečnosti.

R4: Školení se zaměřují hlavně na základní bezpečnostní postupy, ale specifická rizika spojená s VIP osobami nejsou dostatečně zdůrazněna. Personál není dostatečně informován o významu ochrany těchto dat.

R5: Zaměstnanci nejsou dostatečně školeni ohledně specifických rizik spojených s ochranou dat chráněných osob. Školení se zaměřují spíše na obecné bezpečnostní postupy.

R6: Školení nejsou dostatečně zaměřena na ochranu dat chráněných osob. Personál často nevnímá rizika spojená s těmito osobami a nevěnuje dostatečnou pozornost jejich ochraně.

R7: Školení jsou spíše obecná a nezaměřují se na specifická rizika spojená s ochranou dat VIP osob. Personál není dostatečně informován o důležitosti ochrany těchto dat.

R8: Zaměstnanci nejsou dostatečně školeni, aby chápali rizika spojená s ochranou dat chráněných osob. Školení se zaměřují spíše na obecné aspekty kybernetické bezpečnosti.

R9: Školení se zaměřují na obecné bezpečnostní postupy, ale konkrétní rizika spojená s ochranou dat VIP osob nejsou dostatečně zdůrazněna. Personál není dostatečně informován o těchto rizicích.

R10: Zaměstnanci nejsou dostatečně školeni ohledně specifických rizik spojených s ochranou dat chráněných osob. Školení se zaměřují spíše na obecné bezpečnostní postupy.

Otázka 7: Jaké jsou nejčastější problémy, se kterými se setkáváte v oblasti kybernetické bezpečnosti chráněných osob?

R1: Ideální by bylo, aby vše bylo nastaveno pro všechny stejně, standardně, dle zákonů a vyhlášky, ale to nejde. Státní instituce by měly nastavit standardy, které bude potřeba zabezpečit v případě chráněných osob. Ideálně vytvořit samostatnou síť, včetně počítačů atd., do které se nedostane nikdo z venku. Jde to dělat jiným způsobem, aby to bylo offline.

R2: Největším problémem je nedostatečná infrastruktura a nejednotné standardy ochrany dat. Mnoho nemocnic nemá dostatečné zdroje na to, aby chránilo data VIP osob na úrovni, kterou by si to zasloužilo. Je potřeba stanovit jasná pravidla a postupy.

R3: Problémem je, že neexistují jednotné standardy a postupy, které by řešily ochranu dat VIP osob. Každé zařízení si to dělá po svém, což zvyšuje riziko úniku informací.

R4: Často chybí dostatečné technické a organizační zázemí pro ochranu dat VIP osob. Také není dostatečná spolupráce mezi různými institucemi, což komplikuje ochranu těchto dat.

R5: Hlavním problémem je, že neexistují jasné a jednotné standardy ochrany dat VIP osob. Každé zařízení si to řeší po svém, což může vést k vážným nedostatkům v zabezpečení.

R6: Největším problémem je absence jednotných standardů a postupů. Neexistuje jednotná metodika, jak chránit data VIP osob, což zvyšuje riziko úniku informací.

R7: Problémem je nejednotnost postupů a standardů. Každé zařízení přistupuje k ochraně dat VIP osob jinak, což zvyšuje riziko, že data budou nedostatečně chráněna.

R8: Nedostatek jednotných standardů a postupů je hlavním problémem. Je nutné, aby státní instituce nastavily jasné požadavky na ochranu dat VIP osob.

R9: Hlavním problémem je neexistence jednotných standardů pro ochranu dat VIP osob. Každé zařízení si to řeší po svém, což zvyšuje riziko úniku informací.

R10: Největším problémem je nejednotnost standardů a postupů. Je třeba vytvořit jednotnou metodiku pro ochranu dat VIP osob, která by byla závazná pro všechny zdravotnické instituce.

Otázka 8: Řešíte ochranu dat chráněných osob nebo skupin osob (vojáků/policistů/příslušníků zpravodajských služeb atd.) ve velkých souborech dat (tzv. „big data“), která jsou předávána například za účelem výzkumu?

R1: Ano, souhlasím, že je potřeba je chránit. Ze zákona jsou chráněny více. Třeba v registru obyvatel můžou být informace o tom, že je daná osoba voják. Stát to musí chránit sám. Musí to poskládat tak, aby to bylo bezpečné. To samé v případě realizace výzkumů atd. Jinak v tom ale nevidím velký problém, podle mě by pro potenciálního útočníka byly taková data bezcenné. Potřebuju něco jiného, když budu dělat analýzu rizik, potřebuju hlavně údaje geolokační. Viz američani, obíhali svou základnu a dávali si to do Garminu do telefonu a sdíleli to. Nepřítel pak hned viděl, kde je tajná základna. Něco takového si představte tady u zdravotních dat, musím nad nimi přemýšlet jinak. Není potřeba řešit ty údaje, ale vždy udělat pořádnou analýzu rizik u kyberbezpečnosti a podle toho postupovat a vnímat ty data i jinak než obsahem, ale hlavně kde jsou uložené atd. Pozor ještě i na pojišťovny, tam jsou všechna data a nikdo to neřeší. Seženu si rodná čísla nebo pojišťovny, spáruju to s daty od mobilního operátora a můžu hned vidět, kdo kde je.

R2: Ano, chráníme data skupin osob, jako jsou vojáci a policisté, s vyšší mírou bezpečnosti. Data jsou více anonymizována a šifrována. Musíme pečlivě analyzovat rizika a zvolit odpovídající úroveň zabezpečení.

R3: Ochrana dat chráněných osob je nezbytná, ale není vždy snadné zajistit adekvátní úroveň ochrany ve velkých datových souborech. Používáme anonymizaci a šifrování, ale je potřeba dělat více.

R4: Ochrana dat chráněných osob ve velkých souborech dat je klíčová. Používáme anonymizaci a šifrování, ale stále existuje riziko zneužití. Je třeba zlepšit analýzu rizik a implementovat přísnější opatření.

R5: Ochrana dat je důležitá, ale je náročné ji zajistit ve velkých souborech dat. Používáme anonymizaci a šifrování, ale stále existují mezery v ochraně, které je třeba řešit.

R6: Ochrana dat ve velkých souborech je náročná, ale nezbytná. Používáme anonymizaci a šifrování, ale je potřeba zlepšit analýzu rizik a zajistit lepší zabezpečení dat.

R7: Data chráněných osob jsou ve velkých souborech více anonymizována a šifrována. I přesto existuje riziko úniku, proto je nutné neustále zlepšovat analýzu rizik a implementovat přísnější bezpečnostní opatření.

R8: Ochrana dat chráněných osob ve velkých souborech je obtížná, ale nezbytná. Používáme šifrování a anonymizaci, ale stále existují mezery, které je třeba řešit.

R9: Ochrana dat je náročná, zejména ve velkých souborech. Anonymizace a šifrování jsou standardem, ale je třeba provádět důkladnou analýzu rizik, aby se minimalizovalo riziko úniku informací.

R10: Ochrana dat chráněných osob ve velkých souborech je klíčová. Používáme anonymizaci a šifrování, ale je potřeba zlepšit analýzu rizik a zajistit, že data budou chráněna na nejvyšší možné úrovni.

Otázka 9: Řešíte nějak vyšší míru bezpečnosti dat chráněných osob v případě jejich předávání do jiných zdravotních zařízení (například laboratoří, jiných poskytovatelů zdravotních služeb atd.)?

R1: Ne, neřešíme.

R2: Přenos dat mezi zařízeními není dostatečně zabezpečen. Data jsou často přenášena bez potřebných bezpečnostních opatření, což zvyšuje riziko úniku informací.

R3: Při předávání dat mezi zařízeními se nedostatečně dbá na jejich zabezpečení. Riziko úniku je vyšší, protože bezpečnostní opatření nejsou vždy dodržována.

R4: Přenos dat mezi zařízeními není dostatečně chráněn. Mělo by se více dbát na zabezpečení těchto dat, protože riziko úniku je značné.

R5: Přenos dat mezi zařízeními je problém, protože se nedostatečně chrání. Riziko úniku je vysoké, protože bezpečnostní opatření nejsou vždy na potřebné úrovni.

R6: Předávání dat mezi zařízeními není dostatečně zabezpečeno. Riziko úniku informací je vysoké, protože nejsou vždy dodržována bezpečnostní opatření.

R7: Předávání dat mezi zařízeními není dostatečně chráněno a vůbec se neřeší nebo o tom nevím. Mám zkušenost s tím, že se mne dokonce jednou ptala zaměstnankyně jedné pojišťovny na případ, který jsme u nás řešili a věděla všechny informace z lékařských zpráv pacienta. Riziko úniku informací je vysoké, protože bezpečnostní opatření neexistují.

R8: Přenos dat mezi zařízeními neřešíme. Jak data tečou a kdo je pak vidí je problémem, zejména toho druhého správce osobních údajů.

R9: Nevím o tom, že by to někdo řešil, je to problém státu, který je za to podle mě odpovědný. To, že máme pravidla GDPR neznamená, že by neměly být vytvořeny nějaké standardy a ty by se měly dodržovat všude.

R10: Při předávání dat mezi zařízeními nejsou vždy dodržována bezpečnostní opatření, což zvyšuje riziko úniku informací. Bezpečnost dat není dostatečně zajištěna.

Otázka 10: Jak by měl vypadat přenos dat chráněných osob, vojáků, z bojiště kdekoliv na světě do zdravotnického zařízení v ČR? Online, offline, vlastní sítí, proč?

R1: V takové situaci je klíčové využít metody rychlého a bezpečného přenosu dat. Jednou z možností je mikrodatový přenos, což znamená odeslání maximálního množství informací v krátkém záblesku. Tento přenos může probíhat online nebo offline, ale musí být velmi rychlý, aby minimalizoval riziko odhalení polohy nepřítelem. Nesmí to ale probíhat přes internet, to okamžitě zjistí. Při online přenosu, například přes internet nebo satelitní spojení, existuje riziko, že nepřítel zjistí polohu raněného vojáka nebo zdravotnické jednotky. Proto je lepší využít mikrodatový přenos, který zahrnuje krátký datový záblesk, jenž může obsahovat všechny potřebné informace a je obtížnější jej zachytit a lokalizovat. Tento krátký záblesk by mohl být proveden pomocí speciálních šifrovaných vysílaček, které jsou navrženy tak, aby minimalizovaly detekci. Satelitní přenosy přes vysílačky, když to uděláš, tak víš hned, kde jsou. Všechno, co jde zachytit, je špatně. Musíš mít takovou technologii, kterou nejde zachytit, to je

zcela zásadní. Musíš vymyslet, jak to poslat. Šifrování vůbec nepomůže. Jakmile něco přenášíš vzduchem, tak je to zachytitelné. Dává mi smysl to dělat offline, ale posílat to zašifrované, dát velké množství dat do malého záblesku a poslat to. Elmg. impulzy jsou konečná. Nepřítel to zachytí a pošle tam raketu. Řešení je tedy to posílat opravdu záblesky. Může se přijímat, to je v pohodě, to nikdo nezachytí, ale odesílání je konečná. Dovedu si představit dron, který bude hledat ty signály a bude je ničit. Raketa S300 tak byla například nastavena, rušila signál a jak zachytila rušičku, automaticky ji zaměřila a ničila. Toto je to samé, musí se to udělat rychle.

R2: Přenos dat by měl probíhat online, ale za použití nejmodernějších šifrovacích technologií, které umožní rozkouskovat data a přenést je různými cestami. Takto přenesená data by se na konci spojila do jednoho celku. I když je rychlost přenosu klíčová, neměli bychom podceňovat rizika spojená s online komunikací, a proto by měla být zajištěna bezpečnost přenosu i na úkor menšího zpoždění.

R3: Přenos dat by měl být kombinací online a offline metod. Offline přenos by mohl zahrnovat fyzický transport zašifrovaných disků, zatímco online přenos by měl být zajištěn pomocí šifrovaných spojení s vícevrstvou ochranou. Klíčové je minimalizovat riziko zachycení dat nepřítelem.

R4: Preferuji offline přenos dat za využití fyzického transportu šifrovaných médií. Je to bezpečnější, protože minimalizuje riziko zachycení dat. Online přenos by měl být používán pouze jako záloha, s použitím pokročilých šifrovacích technologií.

R5: Přenos dat by měl probíhat offline, aby se minimalizovalo riziko zachycení dat. Fyzický transport šifrovaných disků je stále nejbezpečnější metoda, i když to může být pomalejší. Online přenos by měl být šifrovaný a co nejvíce rozdělený.

R6: Offline přenos dat je nejbezpečnější, zejména v krizových situacích. Fyzický transport zašifrovaných médií by měl být upřednostněn před online přenosem. Pokud se používá online přenos, měl by být silně šifrovaný a rozkouskovaný.

R7: Offline přenos dat je preferovaný, protože minimalizuje riziko zachycení. Fyzický transport šifrovaných disků je bezpečnější. Online přenos by měl být použit jen v nouzových situacích a měl by být silně šifrovaný.

R8: Pro přenos dat preferuji offline metody, jako je fyzický transport šifrovaných disků. Pokud je nutné použít online přenos, měl by být šifrovaný a data by měla být rozdělena na malé části, aby se minimalizovalo riziko zachycení.

R9: Offline přenos dat je nejbezpečnější, zejména v krizových situacích. Fyzický transport šifrovaných médií je ideální, ale pokud je nutné použít online přenos, musí být šifrování na nejvyšší úrovni a data by měla být rozdělena na menší části.

R10: Offline přenos dat je preferovaný, protože snižuje riziko zachycení. Fyzický transport šifrovaných disků by měl být upřednostněn, a pokud je nutné použít online přenos, měl by být šifrovaný a co nejvíce rozdělený.

Otázka 11: Jak vnímáte tzv. cloudová úložiště a jejich využití pro uchování zdravotních dat? Využíval byste je pro přenos a ukládání zdravotních dat vojáků (chráněných osob)?

R1: Ne. Podle toho, který. Zase bych šel analýzou rizik. Je potřeba si vyhodnotit, jaká data a kde. Vojenská data určitě do cloudu nelze. V případě výpadku Microsoftu vše spadne a neuděláš nic. Nic nepojede. V Černé Hoře při výpadku elektřiny nešlo nic, internet, wifi, telefony, čerpací stanice a nic. Když se to stane tady, pojedou jen diesel agregáty, které jsou jen u armády nebo v nemocnicích. Jak víte, že když se to stane tady, že soukromý cloud bude fungovat? Nebude, nebo jen dočasně. Třeba pákistánská armáda není napíchlá na internet, jsou úplně mimo síť. Nelze tam a ani k nim. Když se pojede v nouzovém režimu, je otázka, zda budu potřebovat elektronická data vůbec. Podle mě armáda umí postavit mnohem lepší cloudy než soukromý sektor. Jedině armádní cloudy v kompletní správě armády. Data vojenských osob by měla být chráněna přísněji než data civilních osob, protože únik těchto dat může mít vážné bezpečnostní důsledky. Například pokud by nepřátelská strana získala informace o zdravotním stavu vojáků, mohla by tyto informace zneužít k plánování útoků. Vojenská data by měla být chráněna pomocí šifrování, fyzického zabezpečení a omezeného přístupu pouze pro oprávněné osoby. V krizových situacích by měla být data chráněna pomocí šifrování a fyzického zabezpečení. Mohou být také uchovávána offline, aby nebyla náchylná na kybernetické útoky. V případě války je důležité zajistit, aby citlivá data nebyla přenášena přes nezabezpečené sítě a byla chráněna před nepřátelskými útoky. Cesnet je například super, ale v případě války je zničí a co? Armádní cloud si bude armáda hlídat.

R2: Cloudová úložiště jsou nevyhnutelnou součástí moderní infrastruktury a mohou být velmi užitečná pro rychlý přístup k datům. Avšak pro uchovávání a přenos zdravotních dat

chráněných osob by měl být použit specifický, vysoce zabezpečený cloudový systém, který je určen pouze pro tuto oblast. Používání běžných cloudových úložišť by mohlo představovat riziko, a proto je nezbytné, aby byla tato úložiště důkladně zabezpečena a řízena s vysokou úrovní kontroly.

R3: Cloudová úložiště mohou být velmi užitečná pro uchování zdravotních dat, pokud jsou správně zabezpečena. Je nutné používat šifrování a další bezpečnostní opatření, aby byla data chráněna před neoprávněným přístupem. Pro vojenské účely by měl být cloud spravován armádou, nikoli soukromými společnostmi.

R4: Cloudová úložiště mají své výhody, ale pro uchování citlivých dat, jako jsou zdravotní údaje vojáků, je nutné zajistit maximální úroveň zabezpečení. Je lepší používat specializované cloudy, které jsou spravovány státními institucemi, aby se minimalizovalo riziko úniku informací.

R5: Cloudová úložiště mohou být riziková, pokud nejsou dostatečně zabezpečena. Pro uchování zdravotních dat vojáků bych upřednostnil offline metody nebo speciálně zabezpečené cloudy spravované armádou. Použití běžných komerčních cloudových služeb není dostatečně bezpečné.

R6: Cloudová úložiště mohou být výhodná pro uchování dat, pokud jsou dostatečně zabezpečena. Vojenská data by však měla být uchovávána na speciálně zabezpečených cloudech, které jsou spravovány armádou, aby se zajistila jejich ochrana před kybernetickými útoky.

R7: Pro uchování zdravotních dat vojáků bych používal pouze speciálně zabezpečená cloudová úložiště spravovaná armádou. Běžné komerční cloudové služby nejsou dostatečně bezpečné a mohly by představovat riziko úniku dat.

R8: Cloudová úložiště mohou být užitečná, ale pro vojenská data by měla být využívána pouze speciálně zabezpečená úložiště spravovaná státem. Použití běžných cloudových služeb by mohlo ohrozit bezpečnost těchto dat.

R9: Cloudová úložiště jsou praktická, ale pro citlivá vojenská data bych používal pouze státní, speciálně zabezpečené cloudy. Komerční služby nejsou dostatečně spolehlivé pro uchování těchto dat.

R10: Pro uchování zdravotních dat vojáků bych používal pouze speciálně zabezpečená cloudová úložiště, která jsou spravována armádou. Použití běžných cloudových služeb by mohlo představovat riziko, proto je důležité zvolit řešení, které zajistí maximální bezpečnost těchto dat.

Otázka 12: Jaká doporučení byste dali pro zlepšení kybernetické bezpečnosti při hospitalizaci chráněných osob?

R1: Budoucnost ochrany dat ve zdravotnictví spočívá v zavádění nových technologií a standardů, které zajistí vyšší úroveň bezpečnosti. Je důležité, aby zdravotnická zařízení pravidelně aktualizovala své bezpečnostní protokoly a školila personál v oblasti ochrany dat. Zavedení standardů jako HL7 pro výměnu zdravotních dat je správný krok, ale je potřeba zajistit jejich rychlé a efektivní zavedení. Ochrana dat by měla být prioritou nejen pro VIP osoby, ale pro všechny pacienty, aby byla zajištěna jejich bezpečnost a soukromí.

R2: Zvýšení úrovně kybernetické bezpečnosti by mělo zahrnovat pravidelné školení personálu, zavádění nových technologií a pravidelnou aktualizaci bezpečnostních protokolů. Důležité je také zavést standardizované postupy pro výměnu zdravotních dat a zajistit, aby byla data chráněna na všech úrovních.

R3: Důležité je zajistit pravidelné školení zaměstnanců v oblasti kybernetické bezpečnosti a zavádět nové technologie, které zvyšují ochranu dat. Standardizované postupy a pravidelné aktualizace bezpečnostních protokolů by měly být základem každého zdravotnického zařízení.

R4: Pro zlepšení kybernetické bezpečnosti je nezbytné zavádět nové technologie, školit personál a pravidelně aktualizovat bezpečnostní protokoly. Standardizace postupů pro ochranu dat je klíčová pro zajištění jejich bezpečnosti.

R5: Ochrana dat při hospitalizaci chráněných osob by měla zahrnovat zavádění nových technologií, pravidelné školení personálu a pravidelnou aktualizaci bezpečnostních protokolů. Důležité je také zavést standardizované postupy pro výměnu a ochranu dat.

R6: Kybernetická bezpečnost by měla být zajištěna pravidelným školením personálu, zaváděním nových technologií a pravidelnou aktualizací bezpečnostních protokolů. Standardizace postupů je nezbytná pro zajištění ochrany dat.

R7: Zvýšení úrovně kybernetické bezpečnosti by mělo zahrnovat pravidelné školení personálu, zavádění nových technologií a pravidelnou aktualizaci bezpečnostních protokolů. Standardizace postupů je klíčová pro ochranu dat chráněných osob.

R8: Pro zlepšení kybernetické bezpečnosti je nezbytné zavádět nové technologie, školit personál a pravidelně aktualizovat bezpečnostní protokoly. Důležité je také zavést standardizované postupy pro ochranu a výměnu dat.

R9: Ochrana dat při hospitalizaci chráněných osob by měla zahrnovat zavádění nových technologií, pravidelné školení personálu a pravidelnou aktualizaci bezpečnostních protokolů. Důležité je také zajistit, aby všechny tyto postupy byly standardizovány a implementovány napříč celým zdravotnickým sektorem.

R10: Doporučil bych zlepšit školení zaměstnanců, zavést nové technologie pro ochranu dat a pravidelně aktualizovat bezpečnostní protokoly. Je také nutné zavést standardizované postupy pro ochranu a výměnu dat, aby byla zajištěna jejich maximální bezpečnost.

Otázka 13: Máte nějaké zkušenosti ze zahraničí v diskutované oblasti?

R1: Pracoval jsem na zabezpečení zdravotnických zařízení na vojenských základnách v různých zemích několikrát. Zabezpečoval jsem několik vojenských nemocnic. Viděl jsem, jak se tam používají přísná bezpečnostní opatření a jak jsou data chráněna. V NATO například používají standardy pro propojení různých systémů a výměnu informací, což zajišťuje vysokou úroveň bezpečnosti. Mají nastavené standardy pro přenos dat napříč všemi činnostmi, od logistiky až po zdravotní data. Je důležité se umět napojit mezi systémy, mít vytvořené datové standardy. Nesmyslná rozhodnutí v minulosti nás teď budou stát miliardy.

R2: Ano, pracoval jsem na několika mezinárodních projektech zaměřených na ochranu dat ve zdravotnictví. Viděl jsem, jak různé země přistupují k ochraně citlivých informací, a naučil jsem se, že je klíčové mít zavedené standardizované postupy a moderní technologie. V některých zemích se například využívá decentralizovaná správa dat, což zajišťuje vyšší úroveň bezpečnosti.

R3: Mám zkušenosti s praxí v zahraničí, kde je při hospitalizaci chráněných osob nastaven speciální režim a existují týmy lékařů, kteří se těmto pacientům věnují. Všechny postupy jsou často analogické a dokumentované ve speciálních formách, což zajišťuje vysokou úroveň ochrany a bezpečnosti.

R4: Ano, viděl jsem, jak zahraniční zařízení přistupují k ochraně dat a využívají moderní technologie k zabezpečení citlivých informací. V některých zemích se používají pokročilé šifrovací technologie a decentralizovaná správa dat, což poskytuje vyšší úroveň bezpečnosti.

R5: Ano, v zahraničí jsem se setkal s různými přístupy k ochraně citlivých dat, zejména ve zdravotnictví. V některých zemích jsou zavedené přísné bezpečnostní standardy, které se soustředí na šifrování a ochranu dat při jejich přenosu. Tyto zkušenosti ukazují, že moderní technologie a standardizované postupy jsou klíčem k ochraně citlivých informací.

R6: Ano, pracoval jsem v několika zemích, kde jsou zavedené přísné standardy ochrany dat, zejména v oblasti zdravotnictví. Tyto zkušenosti mi ukázaly, jak důležité je mít standardizované postupy a využívat moderní technologie pro zabezpečení citlivých dat.

R7: Mám zkušenosti ze zahraničí, kde jsou data chráněna velmi přísnými standardy. V některých zemích se používají pokročilé šifrovací technologie a jsou zavedeny standardizované postupy pro ochranu dat. Tyto postupy zajišťují vysokou úroveň bezpečnosti.

R8: Ano, pracoval jsem na několika mezinárodních projektech, kde byly zavedeny přísné bezpečnostní standardy pro ochranu citlivých dat ve zdravotnictví. Tyto zkušenosti ukazují, že je klíčové mít standardizované postupy a využívat moderní technologie pro zabezpečení dat.

R9: Ano, mám zkušenosti ze zahraničí, kde jsou zavedené přísné bezpečnostní standardy pro ochranu dat, zejména ve zdravotnictví. V těchto zemích jsou data chráněna šifrovacími technologiemi a standardizovanými postupy, což zajišťuje vysokou úroveň bezpečnosti.

R10: Ano, pracoval jsem na několika mezinárodních projektech zaměřených na ochranu citlivých dat ve zdravotnictví. Viděl jsem, jak různé země přistupují k ochraně dat, a naučil jsem se, že moderní technologie a standardizované postupy jsou klíčem k zajištění bezpečnosti těchto informací.

Otázka 14: Měla by, dle Vašeho názoru, mít veřejnost právo bez souhlasu ústavního činitele (chráněné osoby) znát informace o jeho zdravotním stavu?

R1: Ano, ale jen v míře, kterou potřebuje.

R2: Ano, ale jen pokud to neohrozí bezpečnost nebo soukromí dané osoby. Veřejnost by měla být informována pouze o těch aspektech, které jsou nezbytné pro její povědomí, například zda je ústavní činitel schopen vykonávat svou funkci.

R3: Myslím si, že veřejnost má právo vědět o zdravotním stavu ústavního činitele pouze v případě, že to ovlivňuje jeho schopnost vykonávat svou funkci. Detaily by však měly zůstat soukromé.

R4: Veřejnost by měla mít omezený přístup k informacím o zdravotním stavu ústavních činitelů. Je důležité chránit jejich soukromí, ale zároveň zajistit, že veřejnost bude informována o tom, zda je činitel schopen vykonávat své povinnosti.

R5: Ano, ale jen v omezené míře a pouze pokud to neohrozí soukromí nebo bezpečnost ústavního činitele. Informace by měly být poskytovány jen tehdy, pokud jsou nezbytné pro zajištění důvěry veřejnosti.

R6: Veřejnost by měla být informována o zdravotním stavu ústavního činitele pouze v případě, že to může ovlivnit jeho schopnost vykonávat funkci. Ostatní informace by měly zůstat soukromé.

R7: Myslím si, že veřejnost má právo na informace pouze v případě, že to přímo ovlivňuje schopnost činitele vykonávat své povinnosti. Detailní informace by měly zůstat soukromé.

R8: Veřejnost by měla mít přístup k informacím o zdravotním stavu ústavního činitele pouze tehdy, pokud je to nezbytné pro zajištění důvěry ve schopnost činitele vykonávat svou funkci. Ostatní detaily by měly být chráněny.

R9: Veřejnost by měla být informována pouze o těch aspektech, které přímo ovlivňují výkon funkce ústavního činitele. Ostatní informace by měly být chráněny jeho právem na soukromí.

R10: Ano, ale jen pokud je to nezbytné pro udržení důvěry ve schopnost ústavního činitele vykonávat svou funkci. Detaily by však měly zůstat chráněny a veřejnost by měla být informována jen o základních skutečnostech.

Příloha č. 2: Dotazník pro zaměstnance ve zdravotnických zařízeních

Hospitalizace, léčba a bezpečnost chráněných osob

Vážené paní kolegyně, vážení kolegové,

dovoluji si obrátit se na Vás se zdvořilou žádostí o vyplnění dotazníku k výzkumnému šetření týkajícímu se zajištění bezpečnosti a poskytování zdravotních služeb chráněným osobám (tzv. VIP pacientům).

Dotazník se skládá ze tří částí - Péče o chráněné osoby, Fyzická a bezpečnostní opatření a Virtuální/kybernetická bezpečnost chráněných osob.

Vaše rozhodnutí o účasti ve výzkumu a vyplnění dotazníku je zcela dobrovolné a anonymní. Jeho vyplněním dáváte souhlas s použitím anonymních údajů k výzkumným účelům. Získaná data budou sloužit pouze pro účely výzkumu disertační práce s názvem Bezpečnost hospitalizovaných chráněných osob (tvorbu systémových opatření a postupů pro poskytovatele zdravotních služeb týkajících se poskytování zdravotních služeb a zajištění bezpečnosti chráněným osobám).

Předem Vám mnohokrát děkuji za Váš čas a ochotu.

mjr. PhDr. Lukáš Miklas, MBA

vedoucí Odboru právního

Ústřední vojenská nemocnice - Vojenská fakultní nemocnice Praha

e-mail: lukas.miklas@uvn.cz;

Definice chráněné osoby (dále jen „VIP pacient")

VIP pacientem se rozumí pacient:

- který má ochranku (je chráněnou osobou dle zákona), např. prezident, předseda vlády, ministr vnitra aj. nebo
- kterého si zdravotní zařízení/stát samo určí jako chráněnou osobu (např. ústavní činitelé, politici, hejtmani, starostové, veřejně známé osobnosti, celebrity, sportovci, youtubeři, velvyslanci, vojáci, příslušníci bezpečnostních sborů, příslušníci zpravodajských služeb, novináři, umělci atd.)

Sekce 1: Péče o VIP pacienty

Údaje o respondetech:

1. Lokalita (pouze u zahraničních respondentů)
2. Jste:
    - Lékař
    - Sestra
    - Ostatní zdravotnický pracovník (např. fyzioterapeut, laborant, farmaceut)

- Vedoucí zaměstnanec (např. manažer, primář, vrchní sestra)
- Administrativní pracovník (např. kvalitář, právník, personalista, logista, IT pracovník, asistent)

Sekce 1: Péče o VIP pacienty

1. Má Vaše zdravotní zařízení nastavena speciální pravidla pro poskytování zdravotní péče tzv. VIP pacientům? (ano, ne)
2. Pokud ano, jakým způsobem jsou zaměstnanci o těchto pravidlech informováni? (vnitřní předpisy, metodika, porady, pokyny nadřízených, jiné - uveďte)
3. Podílel jste se někdy na tvorbě pravidel nebo poskytování zdravotní péče pro VIP pacienty? (ano, ne)
4. Byl jste svědkem toho, že VIP pacientovi byla poskytnuta péče v následujících oblastech? (vyšší kvalita, větší rozsah, přednostní vyšetření, kvalitnější strava, kvalitnější léky nebo výživa, nadstandardní vybavení, porušení standardních procesů, jiné - uveďte)
5. Má VIP pacient určeného hlavního ošetřujícího lékaře? (ano, vždy; ano, ale jen u některých; ne; nevím)
6. Vyčleňuje Vaše zdravotní zařízení kvůli přítomnosti nebo hospitalizaci VIP pacienta konkrétní prostory (místnosti)? (ano, vždy; ano, ale jen u některých; ne; nevím)
7. Jaká opatření jsou přijímána pro zajištění soukromí VIP pacientů během jejich hospitalizace? (Vyšší kvalita, Větší rozsah, Přednostní vyšetření, Kvalitnější strava, Kvalitnější léky nebo výživa, Nadstandardní vybavení, Nedodržení standardních postupů, jiné - uveďte)
8. Myslíte si, že VIP pacienti mají právo na vyšší kvalitu nebo rozsah poskytovaných zdravotních služeb? (rozhodně ano, spíše ano, spíše ne, rozhodně ne)
9. Jaké jsou nejčastější problémy, se kterými se setkáváte při péči o VIP pacienty? (nepovinné)

Sekce 2: Fyzická a bezpečnostní opatření VIP pacientů

1. Kdo je (nebo by byl) odpovědný za nastavení bezpečnostních opatření pro VIP pacienty? (vedoucí lékař/primář/přednosta, vedoucí oddělení bezpečnosti, vedoucí oddělení kvality, bezpečnostní ředitel, náměstek, ředitel, jiný - uveďte)
2. Zasahuje/zasahovala by přítomnost ochranky VIP pacienta do procesů Vašeho zařízení? (ano, spíše ano, spíše ne, ne, nedokážu posoudit)
3. Jak hodnotíte přítomnost ochranky VIP pacienta? (velmi pozitivní, pozitivní, neutrální, negativní, velmi negativní)
4. Máte vytvořena pravidla, kterými se členové ochranky VIP pacienta musí řídit? (ano; ne; nevím)
5. Umožnil(a) byste přítomnost ochranky při operaci na operačním sále? (ano, spíše ano, spíše ne, ne)

6. V případě návštěvy VIP pacienta, kdo rozhoduje o jejím vpuštění? (odpovědný lékař; určený ošetřující lékař; jiný určený zaměstnanec; vedení nemocnice; pouze ochranka; standardně bez ohledu na VIP statut, nevím)
7. Jaká opatření jsou přijímána pro zajištění fyzické bezpečnosti personálu v přítomnosti VIP pacientů? (žádná, více strážných, ochranu zabezpečuje ochranka a PČR/VP, jiné - uveďte)
8. Jaké jsou další možné nejčastější problémy spojené s fyzickou bezpečností při hospitalizaci VIP pacientů? (nepovinné)

Sekce 3: Virtuální/kybernetická bezpečnost VIP pacientů

1. Má Vaše zdravotní zařízení nastavena speciální pravidla pro zajištění virtuální/kybernetické bezpečnosti VIP pacientů? (ano; ne)
2. Je přístup k informacím o VIP pacientech omezen pouze na oprávněné osoby? (ano, ano, ale jen některé informace, ne, nevím)
3. Jaká opatření jsou přijímána k zajištění ochrany dat pro případ pokusu o neoprávněný přístup k datům VIP pacienta zevnitř? (GDPR logy, oddělený IS systém, papírová dokumentace, fiktivní jméno, monitorování přístupu, omezení přístupu, zaheslování, vedení pouze papírové dokumentace, jiné - uveďte)
4. Dochází ke kontrole oprávněnosti nahlížení do zdravotní dokumentace VIP pacienta? (ano, ne, nevím)
5. V případě předávání dat VIP pacientů do jiných zdravotních zařízení/laboratoří, jsou přijímána vyšší bezpečnostní opatření oproti standardním pacientům? (ano, ne, nevím)
6. Probíhají ve Vašem zdravotním zařízení školení a osvěta pro zaměstnance ohledně nakládání a ochrany dat VIP pacientů? (ano, všem zaměstnancům; ano, ale jen části zaměstnanců; ne; nevím)
7. Jaká doporučení byste dali pro zlepšení kybernetické bezpečnosti při hospitalizaci VIP pacientů? (nepovinné)

Příloha č. 3: Dotazník pro chráněné osoby

Hospitalizace, léčba a bezpečnost chráněných osob

Vážené paní kolegyně, vážení kolegové,

dovoluji si obrátit se na Vás se zdvořilou žádostí o vyplnění dotazníku k výzkumnému šetření týkajícímu se zajištění bezpečnosti a poskytování zdravotních služeb chráněným osobám (tzv. VIP pacientům).

Dotazník se skládá ze tří částí - Péče o chráněné osoby, Fyzická a bezpečnostní opatření a Virtuální/kybernetická bezpečnost chráněných osob.

Vaše rozhodnutí o účasti ve výzkumu a vyplnění dotazníku je zcela dobrovolné a anonymní. Jeho vyplněním dáváte souhlas s použitím anonymních údajů k výzkumným účelům. Získaná data budou sloužit pouze pro účely výzkumu disertační práce s názvem Bezpečnost hospitalizovaných chráněných osob (tvorbu systémových opatření a postupů pro poskytovatele zdravotních služeb týkajících se poskytování zdravotních služeb a zajištění bezpečnosti chráněným osobám).

Předem Vám mnohokrát děkuji za Váš čas a ochotu.

mjr. PhDr. Lukáš Miklas, MBA

vedoucí Odboru právního

Ústřední vojenská nemocnice - Vojenská fakultní nemocnice Praha

e-mail: lukas.miklas@uvn.cz;

Definice chráněné osoby (dále jen „VIP pacient")

VIP pacientem se rozumí pacient:

- který má ochranku (je chráněnou osobou dle zákona), např. prezident, předseda vlády, ministr vnitra aj. nebo
- kterého si zdravotní zařízení/stát samo určí jako chráněnou osobu (např. ústavní činitelé, politici, hejtmani, starostové, veřejně známé osobnosti, celebrity, sportovci, youtubeři, velvyslanci, vojáci, příslušníci bezpečnostních sborů, příslušníci zpravodajských služeb, novináři, umělci atd.)

Sekce 1: Péče o VIP pacienty

1. Byl(a) jste někdy hospitalizován(a) nebo vyšetřen(a) jako VIP pacient?
    - Ano
    - Ne
2. Pokud ano, byl(a) jste informován(a) o existenci speciálních pravidel týkajících se péče o VIP pacienty?
    - Ano, ústně od personálu

- Ano, písemně (brožura, leták)
- Ne
- Jinak (uveďte)

3. Byl Vám při vyšetření nebo hospitalizaci někdy poskytnut některý z následujících benefitů?
    - Vyšší kvalita zdravotní péče
    - Větší rozsah zdravotní péče
    - Rychlejší vyšetření
    - Kvalitnější strava
    - Kvalitnější léky nebo výživa
    - Nadstandardní vybavení pokoje
    - Léčba pomocí málo dostupných přístrojů
    - Samostatný pokoj
    - Nebyl mi poskytnut žádný z výše uvedených benefitů
    - Jinak (uveďte prosím)
4. Cítil(a) jste se během hospitalizace dostatečně informován(a) o svém zdravotním stavu a průběhu léčby?
    - Ano
    - Spíše ano
    - Spíše ne
    - Ne
5. V případě hospitalizace, byl Vám přidělen konkrétní lékař, který měl na starost jen Vás?
    - Ano, měl(a) osobního lékaře
    - Ne, lékaři se v péči o mne střídali
    - Nedokážu posoudit
    - Nebyl(a) jsem hospitalizován(a)
6. Myslíte si, že VIP pacienti mají právo na vyšší kvalitu nebo rozsah poskytovaných zdravotních služeb?
    - Rozhodně ano
    - Spíše ano
    - Spíše ne
    - Rozhodně ne.

Sekce 2: Fyzická a bezpečnostní opatření

1. Byla Vám během hospitalizace zajištěna fyzická bezpečnost některým z následujících způsobů?
    - Přítomnost ochranky (Vaší nebo nemocniční)
    - Omezení přístupu na oddělení
    - Umístění na speciální/samostatný pokoj
    - Vyšetření/hospitalizace probíhala v utajení

- Nebyla přijata žádná bezpečnostní opatření
- Jinak (uveďte)

2. Omezovala bezpečnostní opatření (činnost ochranky atd.) Vaše soukromí nebo pohyb po nemocnici?
    - Ano
    - Spíše ano
    - Spíše ne
    - Ne
    - Nedokážu posoudit

Sekce 3: Virtuální/kybernetická bezpečnost

1. Byl(a) jste informován(a) o opatřeních pro zajištění kybernetické bezpečnosti Vašich osobních a zdravotních dat?
    - Ano
    - Ne
2. Zajímal(a) jste se někdy, zda do Vaší zdravotní dokumentace nahlíží/nahlíželi pouze oprávnění zaměstnanci nemocnice?
    - Ano
    - Ne
3. Jak často se zajímáte o to, s kým a kde jsou sdíleny informace o Vašem zdravotním stavu?
    - Velmi často
    - Často
    - Občas
    - Výjimečně
    - Nikdy
4. Došlo někdy během hospitalizace nebo vyšetření k úniku informací o Vašem zdravotním stavu?
    - Ano
    - Ne nebo o tom nevím
5. Jaká byla Vaše celková zkušenost se zabezpečením Vašich dat během hospitalizace nebo vyšetření?
    - Pozitivní
    - Spíše pozitivní
    - Neutrální
    - Spíše negativní
    - Negativní
6. Domníváte se, že je legitimní, aby veřejnost měla právo na informace o Vašem zdravotním stavu i bez Vašeho souhlasu?
    - Ano
    - Spíše ano

- Spíše ne
- Zásadně ne