Zakonodajni in tehnični vidik varovanja osebnih podatkov v slovenskih zdravstveno-informacijskih sistemih

Luka Hrgarek, Leon Bošnjak, Tatjana Welzer Družovec, Aida Kamišalić
Univerza v Mariboru, Fakulteta za elektrotehniko, računalništvo in informatiko, Koroška cesta 46, 2000 Maribor
{luka.hrgarek leon.bosnjak tatjana.welzer aida.kamisalic}@um.si

Izvleček

Varovanje osebnih podatkov je problematika, ki je vsak dan bolj aktualna. Različne novodobne kršitve zasebnosti nastajajo tudi zaradi hitrega tehnološkega razvoja, ki mu zavedanje o potrebah po varovanju podatkov kljub naporom stroke ne sledi dovolj hitro. Omenjena problematika je v zdravstvu še posebno prisotna in pomembna. Velika večina zdravstvenih podatkov je digitaliziranih. Dostopnost in varnost teh podatkov lahko zato hitro postane vprašljiva. Vsi, ki so vključeni v zdravstvene procese, se morajo zavedati, da je varno in pravilno ravnanje s temi podatki ključnega pomena.

Direktiva Evropskega parlamenta o varstvu posameznikov pri obdelavi osebnih podatkov in prostem pretoku takšnih podatkov določa smernice za vse države članice Evropske unije. Ta priporočila morajo države članice upoštevati in spoštovati v svojih zakonodajah, povezanih z varstvom osebnih podatkov. V Sloveniji varstvo osebnih podatkov v zdravstvu obravnavajo Ustava Republike Slovenije, Zakon o varstvu osebnih podatkov in Zakon o pacientovih pravicah.

V članku se bomo osredinili na pregled direktiv Evropske unije, slovenske zakonodaje in dokumentacije s področja varovanja osebnih podatkov v zdravstvu. Pregledali bomo dostopno dokumentacijo o bolnišničnih informacijskih sistemih po Sloveniji. Z analizo de facto stanja v slovenskem zdravstvu želimo ugotoviti, kako dobro se slovensko zdravstvo prilega zakonodaji: na kakšen način so implementirani zakonsko zagotovljeni varnostni mehanizmi, kako so podatki zaščiteni pri prenosu in kako sistemi in osebje varujejo osebne podatke bolnikov.

Ključne besede: zdravstveno-informacijski sistemi, zasebnost podatkov, zaupnost podatkov, zakonodaja.

Abstract

Legislative and technical aspects of protection of personal data in Slovenian healthcare information systems

Privacy is an issue that is becoming increasingly more relevant. Various contemporary privacy violations are also linked to rapid technological development. Despite efforts in healthcare to increase the awareness of the necessity of data protection, users remain slow to adapt these changes. The aforementioned issues are particularly pressing and important in healthcare. The vast majority of healthcare data is digitized. Availability and security of such data can quickly become questionable. Those involved in healthcare processes should be aware that safe and proper handling of such data is crucial.

The Directive of the European Parliament on the protection of individuals with regard to the processing of personal data and on the free movement of such data provides guidelines for all Member States of the European Union. Member States must take into account and comply with these recommendations within their laws related to personal data protection. In Slovenia, the protection of personal data in healthcare is addressed by the Constitution, the Personal Data Protection Act and the Patient Rights Act.

In this article, we focus on the review of the directives of the European Union, the Slovenian legislation and technical documentation from the field of personal data protection in healthcare. We review the available documentation on hospital information systems in Slovenia. By analyzing the de facto situation in Slovenian healthcare, we determine how well it adheres to the legislation: how security mechanisms provided by law are implemented, how data is protected and how the systems and personnel protect the personal data of patients.

Keywords: healthcare information systems, data privacy, data confidentiality, legislation

1 UVOD

Povprečna starost prebivalstva v Sloveniji se veča, prav tako se podaljšuje življenjska doba. S tem se povečuje tudi potreba po storitvah v zdravstvu. Z napredkom, ki smo mu priča v sedanjem času, prihajajo nove tehnologije, katerih uporaba prinaša veliko izzivov. Vsaka nova vpeljava tehnologij odpira različna etična in varnostna vprašanja. Pred obdobjem naprednega računalništva in komunikacijskih tehnologij je bilo združevanje informacij tudi o eni sami osebi naporno, časovno potratno in močno odvisno od muhavosti človeških čuvajev teh podatkov (Hough, 2009). Varovanje zasebnosti lahko bolnišnicam z elektronsko izmenjavo podatkov koristi, vendar samo v primeru, če se bolniki zavedajo, da bodo njihove zdravstvene informacije obravnavane zaupno. Le na podlagi tega bodo namreč pripravljeni posredovati natančne podatke. Po drugi strani pa zaščita zasebnosti za elektronsko izmenjavo informacij pomeni višji strošek, kar zmanjša korist (Miller in Tucker, 2009).

Na področju zdravstva srečujemo pojme, kot so elektronska zdravstvena kartoteka, storitve eNaročanja in eRecepti, ki se arhitekturno izvajajo v različici modela odjemalec – strežnik, v katerem vsa vmesna komunikacija poteka prek interneta. To komunikacijo je treba zavarovati, sicer so podatki izpostavljeni napadom: kraji, nepooblaščenem spreminjanju in ponarejanju. V postopku razvoja programske opreme razvijalci pogosto izberejo linijo najmanjšega odpora in rešitev razvijajo z vidika funkcionalnosti, medtem ko je varnost stranskega pomena. Takšen površen pristop se »obrestuje« v vseh razvijalskih domenah, še posebno pa v zdravstvu.

Zdravstveni podatki so občutljivi osebni podatki (Zakon o varstvu osebnih podatkov RS, 2004), katerih razkritje pomeni invaziven vdor v posameznikovo zasebnost. Westin definira zasebnost kot »trditev posameznikov, skupin ali institucij, da lahko sami zase odločajo, kdaj, kako in v kakšnem obsegu bodo drugim razkrili informacije o sebi«. Poleg občutljivih osebnih podatkov morajo zdravstvene institucije varovati tudi druge občutljive podatke, ki niso nujno osebni podatki (slika 1). Danes se v svojem digitalnem življenju prostovoljno odpovedujemo različnim vidikom zasebnosti in razkrivamo več informacij, kot se sami zavedamo. Čeprav takšno početje za namene izkoriščanja ugodnosti, ki nam jih ponujajo socialna omrežja, morda ni varnostno kritično, pogosto pozabljamo, da je področje zdravstvenih podatkov veliko bolj občutljivo.

Slika 1: **Odnos med osebnimi in občutljivimi podatki**

Zdravstveni podatki so kot posebna kategorija domensko specifičnih podatkov izpostavljeni različnemu osebju, ki dostopa do njih in jih uporablja. Prav tako marsikje s temi podatki upravljajo z zastarelo programsko opremo, ki še vedno deluje, vendar ne zagotavlja vseh potrebnih konceptov varnosti in zasebnosti. Pri upravljanju in varovanju podatkov je treba zagotoviti tudi njihovo sledljivost, saj s tem omogočamo možnost kasnejšega ugotavljanja zlorab. Sledljivost je prav tako preventivni mehanizem, saj lahko v nekaterih primerih že zavedanje o tem odvrne posameznika, da bi neupravičeno dostopal do osebnih podatkov (Informacijski pooblaščenec RS, 2008). Kljub visokim moralnim standardom, ki jih vsi bolniki pričakujemo od zdravstvenih delavcev, je izjemno pomembna zakonodaja, ki predpisuje, »kdaj, kako in v kakšen obsegu« je treba podatke varovati.

V članku bomo povzeli evropsko in slovensko zakonodajo s področja varnosti zdravstvenih podatkov, pregledali javno dostopno dokumentacijo o zdravstveno-informacijskih sistemih v Republiki Sloveniji ter njihovo prileganje obstoječi zakonodaji. Konkretno smo se osredinili na varovanje komunikacijskih poti, saj so te najbolj izpostavljene napadalcem. Po drugi strani gre pri varovanju prostorov, sistemske programske opreme ter uporabi in obdelavi podatkov, ki jih ZVOP in prilegajoča zakonodaja prav tako naslavljata, za občutljive informacije, do katerih nezdravstveno osebje nima dostopa.

2 ZAKONODAJA

2.1 Evropska zakonodaja

Krovni dokument evropske zakonodaje, ki omenja varstvo osebnih podatkov, je Listina Evropske unije o temeljnih pravicah. Ta v svojem 8. členu pravi, da »ima vsakdo pravico do varstva osebnih podatkov, ki se nanašajo nanj«.

Direktiva Evropskega parlamenta in Sveta o uveljavljanju pravic pacientov pri čezmejnem zdravstvenem varstvu v svojem 25. členu govori o zagotavljanju pretoka osebnih podatkov med državami članicami, hkrati pa tudi o potrebi po varstvu temeljnih pravic posameznikov – v tem primeru varstvu osebnih podatkov. V nadaljevanju se sklicuje na Direktivo 95/46/ES Evropskega parlamenta in Sveta iz leta 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in prostem pretoku takih podatkov, pri čemer je posameznikom zagotovljena pravica dostopa do lastnih osebnih podatkov o zdravju.

Ena ključnih komponent digitalnega zdravstva je elektronska zdravstvena kartoteka (angl. Electronic health record, EHR), ki je sistematična zbirka elektronsko hranjenih zdravstvenih informacij o pacientu in populaciji v digitalni obliki (Gunter in Terry, 2005). Ti zapisi so na voljo različnim vejam zdravstvene dejavnosti, saj lahko v eni elektronski zdravstveni kartoteki hranimo demografske podatke, zgodovino bolezni, seznam alergij, imunizacijski status, radiološke zapise in podobno. Celovita in obširna elektronska zdravstvena kartoteka lahko zdravniku zagotovi boljši pregled nad bolnikovim zdravstvenim stanjem, kar omogoča sprejetje celovitejših diagnoz in posledično ustreznejših ukrepov. Prav tako pa lahko množica medicinskih informacij, ki so vsebovane v elektronski zdravstveni kartoteki, pomeni grožnjo posameznikovi zasebnosti, saj so na enem mestu shranjeni vsi podatki o bolniku (npr. podatki o spolno prenosljivih boleznih, duševnih motnjah, odvisnostih od drog ali alkohola) in je do njih laže dostopati in jih replicirati kot podatke na papirnatih zapisih (Adamski, 2014).

Zaradi stopnje občutljivosti podatkov, ki so hranjeni v elektronski zdravstveni kartoteki, ravnanje z njo pogosto obravnava zakonodaja. V tabeli 1 vidimo, katere države članice EU imajo urejeno zakonodajo glede elektronskih zdravstvenih kartotek. Čeprav področje zdravstvenih podatkov ureja v različnih zakonih, slovenska zakonodaja ne obravnava pojma elektronska zdravstvena kartoteka. Obstoječi nacionalni sistem eZdravje podpira storitvi eRecept in eNaročanje, hkrati pa spletni portal Zavoda za zdravstveno zavarovanje Slovenije omogoča dostop do osebnih podatkov zavarovanca, izbranega zdravnika in zobozdravnika. Prav tako portal ZZZS omogoča prikaz seznama obiskov zdravnika in podatke o stroških zavarovanja za posamezni obisk, ne vključuje pa nobenih medicinskih podrobnosti obiska.

Tabela 1: **Določitev posebnih pravil o vsebini elektronskih zdravstvenih kartotek po državah članicah EU (Adamski, 2014)**

Avstrija	✓	Latvija	✓
Belgija		Litva	✓
Bolgarija		Luksemburg	✓
Ciper		Madžarska	
Češka		Malta	
Danska	✓	Nizozemska	
Estonija	✓	Poljska	
Finska	✓	Portugalska	✓
Francija	✓	Romunija	✓
Nemčija	✓	Slovaška	✓
Grčija		Slovenija	
Hrvaška	✓	Španija	✓
Irska		Švedska	✓
Italija	✓	Združeno kraljestvo	

2.2 Slovenska zakonodaja

Ustava Republike Slovenije v svojem 38. **členu (Varstvo osebnih podatkov) zagotavlja varstvo osebnih podatkov in prepoveduje uporabo osebnih podatkov v nasprotju z namenom njihovega zbiranja. Podrobnosti glede zbiranja, obdelovanja, namena uporabe, nadzora in varstva tajnosti osebnih podatkov določa Zako**n o varstvu osebnih podatkov. (Ustava Republike Slovenije, 2006)

Zakon o varstvu osebnih podatkov (ZVOP) definira osebni podatek kot »kateri koli podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen«, pri čemer je posameznik fizična oseba, ki jo je mogoče enolično določiti in identificirati. V svojem 6. členu opredeljuje različne pojme, ki jih uporablja v nadaljevanju, med drugim tudi pojem občutljivih osebnih podatkov, med katere uvršča podatke o zdravstvenem stanju. V 13. členu ZVOP določa primere, ko občutljive osebne podatke lahko obdelujemo. Takšno dovoljenje dobijo zdravstveni delavci, če gre za namen zdravstvenega varstva prebivalstva in

posameznikov ter vodenja ali opravljanja zdravstvenih služb.

Nepooblaščenim osebam mora biti onemogočen dostop do občutljivih osebnih podatkov, kar mora biti zagotovljeno s posebnim načinom njihovega označevanja in zavarovanja (14. člen). ZVOP zahteva uporabo kriptografskih metod in elektronskega podpisa pri prenosu po telekomunikacijskih omrežjih za zagotavljanje nečitljivosti oziroma neprepoznavnosti.

V tretjem poglavju (24. člen) določa ukrepe, ki jih je treba zagotoviti, da se podatki lahko ustrezno varujejo. Zahteva varovanje prostorov, opreme in sistemske programske opreme, v kar spada tudi skupina vhodno-izhodnih enot. Prav tako je treba zagotoviti varno aplikativno programsko opremo, ki se uporablja za obdelavo podatkov. Zakon zahteva preprečevanje nepooblaščenega dostopa do osebnih podatkov pri njihovem prenosu, posebno pri prenosu po telekomunikacijskih omrežjih. Da bi dosegli sledljivost in nezanikanje, ZVOP predpisuje implementacijo možnosti poznejšega ugotavljanja metapodatkov o vnašanju, uporabi in obdelavi podatkov. Vsi zaposleni, ki obdelujejo osebne podatke, so dolžni varovati tajnost osebnih podatkov, tako v času zaposlitve kot tudi po njenem prenehanju. (Zakon o varstvu osebnih podatkov RS, 2004)

Zakon o pacientovih pravicah (ZPacP) ureja množico pacientovih pravic, med drugimi tudi pravico do varstva zasebnosti in varstva osebnih podatkov. S tem se podrobno ukvarja 44. člen zakona, ki v svojem prvem stavku pravi: »Pacient ima pravico do zaupnosti osebnih podatkov, vključno s podatki o obisku pri zdravniku in drugih podrobnostih o svojem zdravljenju.« Določa, da morajo zdravstveni delavci in zdravstveni sodelavci s podatki ravnati »v skladu z načelom zaupnosti in predpisi, ki urejajo varstvo osebnih podatkov« (Zakon o pacientovih pravicah RS, 2008).

Zakon o zbirkah podatkov s področja zdravstvenega varstva (ZZPPZ) določa načine obdelave podatkov in upravljanja z zbirkami podatkov na področjih zdravstvenega varstva in storitve eZdravje. Poleg drugih izvajalcev zdravstvene dejavnosti zakon navaja Nacionalni inštitut za javno zdravje (NIJZ) kot »upravljalca zbirk podatkov s področja zdravstvenega varstva«.

Način zbiranja osebnih podatkov je lahko posredni ali neposredni. Pri posrednem zbiranju ZZPPZ pravi, da posameznika ni treba seznaniti z dejstvom, da bodo njegovi podatki pridobljeni iz drugih zbirk podatkov. Prav tako opredeljuje, do katerih podatkov iz Centralnega registra prebivalstva (CRP) imajo upravljalci zbirk pravico brezplačnega dostopa. To so: EMŠO, ime in priimek, kraj rojstva, leto rojstva, spol, prebivališče in vrsta prebivališča, državljanstvo, zakonski stan, šolska izobrazba, EMŠO matere, EMŠO očeta, EMŠO zakonca, EMŠO otrok, datum in podatki o dogodkih, spremembah ali popravkih. Kot primarni ključ oziroma enotni identifikator, po katerem se ti podatki lahko povezujejo med seboj, lahko upravljalci zbirk uporabljajo številko zdravstvenega zavarovanja s kartice zdravstvenega zavarovanja.

S področjem zavarovanja podatkov se ukvarja samo 7. člen zakona, ki pravi: »Tehnične in organizacijske ukrepe za zavarovanje podatkov v zbirkah podatkov predpiše minister, pristojen za zdravje, v soglasju z ministrom, pristojnim za pravosodje, in ministrom, pristojnim za znanost in tehnologijo.« V nadaljevanju se ZZPPZ ukvarja z metodološkimi načeli: predpisuje uporabo enotnih standardov – definicij, klasifikacij in šifrantov, ki jih določi minister, pristojen za zdravje. (Zakon o zbirkah podatkov s področja zdravstvenega varstva RS, 2000)

Pravilnik o varovanju zaupnih in osebnih podatkov ter o varovanju dokumentarnega gradiva je nastal na podlagi določb Zakona o varstvu osebnih podatkov in 9. člena Statuta Zbornice zdravstvene in babiške nege Slovenije – Zveze društev medicinskih sester, babic in zdravstvenih tehnikov Slovenije. Pravilnik določa »organizacijske in logično tehnične postopke in ukrepe za varovanje zaupnih in osebnih podatkov« v Zbornici – Zvezi. V svojem 3. členu pravilnik pravi, da morajo biti prostori, v katerih se nahajajo strojna oprema in nosilci zaupnih ali osebnih podatkov, varovani z ukrepi, ki nepooblaščenim osebam onemogočajo dostop. V šestem stavku istega člena govori tudi o izklapljanju in fizičnem ali programskem zaklepanju računalnikov in druge strojne opreme izven delovnega časa. Glede poslovanja s strankami 6. člen zahteva, da so »nosilci podatkov in računalniški prikazovalniki nameščeni tako, da stranke nimajo vpogleda vanje«.

V nadaljevanju pravilnik opisuje dovoljene načine vzdrževanja in popravila strojne, računalniške in druge opreme. To opremo lahko vzdržujejo samo pooblaščeni servisi in vzdrževalci (8. in 11. člen), ki imajo z Zbornico – Zvezo sklenjeno ustrezno pogodbo. V 9. členu določa, da se zaposleni, ki nimajo dovoljenja

za vpogled v podatke, lahko gibljejo samo v prostorih, kjer je vpogled v podatke onemogočen. Zaposlenim je prepovedano nameščanje programske opreme brez eksplicitnega dovoljenja upravnega odbora.

Z identifikacijo in avtorizacijo se ukvarja 15. člen pravilnika, ki predpisuje uporabo sistema gesel za dostop do podatkov prek aplikativne programske opreme. Razmislek nadaljuje 16. člen, ki govori o generalnih, »supervizorskih« geslih. Ta bi se naj hranila »v zapečatenih ovojnicah« in varovala kot »uradna tajnost – strogo zaupno«.

17. člen zahteva redno izdelavo varnostnih kopij, ki se hranijo na za to določenih in ustrezno varovanih mestih. Prav tako mora biti vsako prenašanje podatkov prek telekomunikacijskih ali drugih omrežij ustrezno varovano (člen 18). Pravilnik se v svojem 19. členu navezuje na 38. člen Ustave RS, ki pravi, da se lahko »zbirajo in obdelujejo samo tisti podatki, ki imajo ustrezno zakonsko osnovo«. Definirano je tudi brisanje podatkov po preteku roka hranjenja (20. člen), in to s tako metodo, »da je nemogoča restavracija vseh ali le dela brisanih podatkov« (21. člen). (Pravilnik o varovanju zaupnih in osebnih podatkov ter o varovanju dokumentarnega gradiva, 2005)

3 ZDRAVSTVENO-INFORMACIJSKI SISTEMI V SLOVENIJI

Svetovna zdravstvena organizacija je opredelila zdravstveno-informacijski sistem kot temeljni pogoj za uresničevanje ciljev Zdravja v 21. stoletju (World Health Organization, 1999). Po pregledu domenske zakonodaje smo izvedli pregled zdravstvenih informacijskih sistemov z območja Republike Slovenije. Ti sistemi so komercialni in njihova dokumentacija ni prosto dostopna. Zato smo pregledali dostopne podatke o krovnem sistemu Ministrstva za zdravje.

Ministrstvo za zdravje je leta 2008 začelo z izvedbo podpornih podprojektov nacionalnega projekta eZdravje, leta 2011 pa je ustanovilo tudi sektor eZdravje. Danes v okviru eZdravja deluje 17 aplikacij. Za dostop do nekaterih storitev je za uporabnike zahtevana uporaba digitalnega potrdila. Uporabnikom je na voljo portal zVEM (zdravjeVsenaEnemMestu), ki omogoča dostop do storitev eZdravja. Od pomladi 2016 omogoča dostop do storitev eRecept in eNaročanje. Prvotna investicijska dokumentacija ministrstva je razdelila nacionalni zdravstveni informacijski model na tri komponente: ogrodje slovenskega referenčnega zdravstvenega informacijskega modela, slovenski terminološki slovar zdravstvene informatike in slovenski podatkovni slovar zdravstvene informatike (Ministrstvo za zdravje RS, 2009).

Razen nacionalnih sistemov, za katere skrbi Ministrstvo za zdravje, posamezne bolnišnice razvijajo tudi lastne sisteme, ki so prilagojeni njihovim potrebam in specifikam. Takšni sistemi se pogosto uporabljajo za naročanje bolnikov na posamezne preiskave ali posege. Spletni portal Slo-Tech je 16. marca 2017 poročal o razkritju nevarnosti v sistemu ustanove, ki bolnikom omogoča prijavljanje na preglede po spletu. Razkrili so, da spletna stran ne uporablja zaščitene povezave HTTPS, temveč nezaščiteno povezavo HTTP, kar pomeni, da so pacienti posredovali svoje osebne podatke z uporabo nezaščitene povezave. Prenos podatkov prek povezave HTTPS zagotavlja varnost in zasebnost ter zmanjšuje tveganje, da bi tretja oseba prestregla, spremenila ali zlorabila podatke. Uporaba nezaščitene povezave za prenos osebnih podatkov je v nasprotju z zahtevami Zakona o varstvu osebnih podatkov, ki v svojem 14. členu zahteva uporabo kriptografskih metod in elektronskega podpisa za prenos takšnih podatkov po telekomunikacijskih omrežjih. Po javnem opozorilu je omenjena zdravstvena ustanova namestila varovano povezavo HTTPS (Kovačič, 2017b).

Omenjeni spletnih portal je 3. aprila objavil članek, v katerem je opozoril na dejstvo, da imajo tudi druge zdravstvene ustanove v Sloveniji težave z informacijsko varnostjo svojih sistemov. Razkrili so, da ena izmed ustanov ne uporablja povezav HTTPS kljub temu, da morajo pacienti v sistem, s katerim se naročajo na preiskave ali posege, vnesti zdravstveno diagnozo poleg drugih osebnih podatkov, kot so ime, priimek, naslov in številka kartice zdravstvenega zavarovanja. Kot primer so navedli še dve drugi ustanovi, ki prav tako nista imeli implementirane povezave HTTPS. Članek je vseboval tudi zaslonske posnetke, iz katerih je razvidno, da povezava HTTPS dejansko ni bila uporabljena (Kovačič, 2017a). Nekaj dni po izidu članka smo preverili stanje na spletnih sistemih omenjenih bolnišnic in ugotovili, da se je stanje nekoliko izboljšalo, saj so vse omenjene bolnišnice implementirale povezavo HTTPS.

Prav tako smo pregledali spletne strani vseh slovenskih bolnišnic in ugotovili, da na svojih spletnih straneh uporablja povezavo HTTPS trinajst bolnišnic, dvanajst pa ne. Poiskali smo tudi spletne obrazce za naročanje na preglede ali posege in ugotovili,

da naročanja na lastnih spletnih straneh omogoča devet bolnišnic, šestnajst pa ne. Poleg tega, da večina bolnišnic bolnike usmerja na centralni portal za eNaročanje (https://narocanje.ezdrav.si/), je pomemben podatek tudi to, da nobena bolnišnica ne omogoča naročanja brez uporabe povezave HTTPS.

4 RAZPRAVA

Veliko podatkov, ki jih trenutno zbirajo in o njih poročajo v okviru zdravstveno-informacijskega sistema, v resnici ni potrebnih za uresničevanje ciljev zdravstvene dejavnosti (Eržen, 2004). Obdelava osebnih podatkov se lahko nanaša na kakršno koli ravnanje s podatki, vključno s samim dostopom do njih. Zato mora zdravstveno-informacijski sistem omogočati sledljivost celotne obdelave osebnih podatkov. Sledljivost lahko razdelimo na tri ravni: sledljivost sprememb, sledljivost dostopa do podatkov in popolno sledljivost z beleženjem dostopov, sprememb podatkov ter beleženjem tako izvornih kot popravljenih podatkov. Na prvi ravni sledljivosti je kasneje mogoče identificirati uporabnika, ki je vnašal, spreminjal ali brisal določeni podatek, ter ugotoviti čas tega dogodka. Druga raven sledljivosti izpolnjuje enake zahteve kot prva, ob tem pa omogoča še sledljivost podatkov o času in identiteti uporabnika, ki dostopa do posameznega podatka. Tretja raven sledljivosti omogoča pregled zgodovine sprememb, kar pomeni, da hrani celotni življenjski cikel podatka z vsemi metapodatki (Informacijski pooblaščenec RS, 2008). Informacijski pooblaščenec RS tolmači, da ZVOP zahteva drugo raven sledljivosti podatkov.

Pri pripravi zakonov se zakonodajalec ne more spuščati v specifike in tehnične podrobnosti, saj morajo biti ti dovolj široki in tehnološko nevtralni, da lahko zajamejo različna realna stanja (Informacijski pooblaščenec RS, 2008). Vendar lahko poudarimo, da potrebna tehnična specifikacija zakonskega okvira ni javno dostopna in zaradi tega ni mogoče ugotavljati skladnosti obstoječih sistemov z zakonodajo. Hkrati ugotavljamo, da je tehnična dokumentacija zdravstveno-informacijskih sistemov prav tako nedostopna. Ker gre za komercialne proizvode, je to razumljivo, saj želimo implementacijske podrobnosti ohraniti zasebne, da ne izpostavljamo morebitnih ranljivosti sistema. Po drugi strani pa pričakujemo, da bi znotraj vladnih institucij moralo obstajati telo, ki bi pripravljalo tehnične specifikacije zakonskega okvira in skrbelo za njihovo ažuriranje glede na svetovne smernice s posameznega področja. Eden izmed možnih primerov bi lahko bilo predpisovanje uporabe konkretnih kriptografskih algoritmov (npr. algoritma AES) za šifriranje občutljivih osebnih podatkov ali obvezna uporaba povezave HTTPS. Prav tako bi morali odgovoriti na vprašanje, kdo ima lahko dostop do šifrirnega ključa (npr. osebni zdravnik, specialist, zdravstveni tehnik, bolnik), in tako pokriti področje zaupnosti osebnih podatkov. Tako pripravljene tehnične specifikacije bi morale biti javno dostopne. S tem bi omogočili validacijo zdravstveno-informacijskih sistemov in zagotavljali primerno raven kakovosti, kar je v končni fazi v interesu javnosti.

5 SKLEP

Zdravstveni delavci so tisti, ki se morajo držati visokih etičnih standardov, primernih za njihov poklic, saj v nasprotnem primeru izgubijo zaupanje svojih bolnikov. Pri kroničnih bolnikih ter pripadnikih rasnih in etničnih manjšin obstaja še večja skrb glede zasebnosti njihovih zdravstvenih podatkov, zato se bolj pogosto dogaja, da zadržijo informacije, ker se bojijo njihove neustrezne uporabe. Za vzpostavitev večjega javnega zaupanja v informacijske tehnologije na področju zdravstva in olajšanje hitrejšega sprejetja obetavnih novih tehnologij je treba obravnavati varnostna in zasebnostna tveganja.

Ugotovili smo, da evropska in slovenska zakonodaja postavljata podlage za varno delovanje zdravstveno-informacijskih sistemov, kar pomeni zgolj temelj za zagotavljanje ustrezne ravni varnosti. Tudi če obstajajo tehnične specifikacije zakonskih okvirov, ki bi omogočale doseganje in zagotavljanje primerne ravni varnosti, niso javno dostopne. Prav tako ni dostopna dokumentacija o zdravstveno-informacijskih sistemih, zaradi česar nismo uspeli analizirati stopnje prileganja obstoječi zakonodaji. To študijo bomo izvedli na podlagi osebnih stikov z odgovornimi za implementacijo zdravstveno-informacijskih sistemov v slovenskem zdravstvu. Prav tako želimo izvesti primerjalno študijo, v kateri bomo pregledali stanje v bolnišničnih informacijskih sistemih sosednjih držav, saj bo takšna študija podala širši in kompleksnejši pogled na trenutno stanje informatike v slovenskih bolnišnicah in pokazala morebitne smernice za prihodni razvoj.

6 LITERATURA

[1] Adamski, D. (2014). *Overview of the National Laws on Electronic Health Records in the EU Member States. National Report for Poland.* Brussels, Belgium: Milieu Ltd & Time. lex. Retrieved from http://ec. europa. eu/health/ehealth/docs/laws_poland_en. pdf.

[2] Eržen, I. (2004). Zdravstveno informacijski sistem v Sloveniji na razpotju – potrebe in praksa. V *Informatica medica slovenica, 9*, 3–8.

[3] Gunter, T. D., Terry, N. P. (2005). The Emergence of National Electronic Health Record Architectures in the United States and Australia: Models, Costs, and Questions. *Journal of Medical Internet Research, 7*(1).

[4] Hough, M. G. (2009). Keeping it to ourselves: Technology, privacy, and the loss of reserve. *Technology in Society, 31*(4), 406–413.

[5] Informacijski pooblaščenec RS. (2008). Smernice za zavarovanje osebnih podatkov v informacijskih sistemih bolnišnic.

[6] Kovačič, M. (2017a, april). Piškotki kot dimna zavesa spletne varnosti in zasebnosti. *Slo-Tech | Tehnoloski koticek spleta*. Pridobljeno s https://slo-tech.com/novice/t697519.

[7] Kovačič, M. (2017b, marec). Odgovorno razkritje ali neodgovorno nerazkritje. *Slo-Tech | Tehnoloski koticek spleta*. Pridobljeno s https://slo-tech.com/novice/t696199.

[8] Miller, A. R., Tucker, C. (2009). Privacy protection and technology diffusion: The case of electronic medical records. *Management Science, 55*(7), 1077–1093.

[9] Ministrstvo za zdravje Republike Slovenije. (2009). Študija izvedljivosti projekta eZdravje – predinvesticijska zasnova in investicijski program s študijo izvedbe.

[10] World Health Organization. (1999). Health21: The health for all policy framework for the who european region. *Health21: The Health for All Policy Framework for the WHO European Region.*

[11] Pravilnik o varovanju zaupnih in osebnih podatkov ter o varovanju dokumentarnega gradiva. (2005).

[12] Ustava Republike Slovenije. (2006).

[13] Westin, A. F. (1968). Privacy and freedom. *Washington and Lee Law Review, 25(1)*, 166.

[14] Zakon o pacientovih pravicah RS. (2008).

[15] Zakon o varstvu osebnih podatkov RS. (2004).

[16] Zakon o zbirkah podatkov s področja zdravstvenega varstva RS. (2000).

▪

Luka Hrgarek je magister informatike in tehnologij komuniciranja. Diplomiral je leta 2015 na Fakulteti za elektrotehniko, računalništvo in informatiko Univerze v Mariboru na študijskem programu Računalništvo in informacijske tehnologije. Leta 2017 je magistriral z magistrsko nalogo Zbiranje podatkov in profiliranje uporabniških naprav s pomočjo spletnih brskalnikov. Zaposlen je na Fakulteti za elektrotehniko, računalništvo in informatiko kot tehniški sodelavec. Njegovo raziskovalno področje vključuje sodobne spletne tehnologije, informacijsko varnost ter medicinske sisteme.

▪

Leon Bošnjak je asistent in raziskovalec na Fakulteti za elektrotehniko, računalništvo in informatiko Univerze v Mariboru. Leta 2014 je magistriral s področja informatike in je trenutno doktorski študent na računalništvu in informatiki. Njegova raziskovalna področja obsegajo sistemsko varnost, tekstovna in grafična gesla ter metode dvofaktorskega overjanja.

▪

Tatjana Welzer Družovec je redna profesorica in vodja Laboratorija za podatkovne tehnologije na Fakulteti za elektrotehniko, računalništvo in informatiko Univerze v Mariboru. Njena glavna raziskovalna področja so konceptualno oblikovanje podatkovnih baz, podatki v podatkovnem skladiščenju in rudarjenju, ponovna uporaba in vzorci, varnost ter izobraževanje na področju informatike in mobilnosti. Svoje raziskovalne ugotovitve objavlja v znanstvenih revijah in knjigah ter na domačih in mednarodnih konferencah.

▪

Aida Kamišalić je asistentka in raziskovalka na Fakulteti za elektrotehniko, računalništvo in informatiko Univerze v Mariboru. Doktorirala je leta 2014 na računalništvu in informatiki. Njena raziskovalna področja vključujejo podatkovne tehnologije, modeliranje medicinskih postopkov za kronične bolnike in pridobivanje znanja iz podatkov za medicinske postopke.