Varnostni izzivi uporabe mobilnih naprav v zdravstvu

Simon Vrhovec
Univerza v Mariboru, Fakulteta za varnostne vede, Kotnikova 8, 1000 Ljubljana
simon.vrhovec@fvv.uni-mb.si

Izvleček

V zdravstvu vse pogosteje uporabljajo mobilne naprave, saj ponujajo nove priložnosti, kot so npr. izboljšana mobilnost, komunikacija in koordinacija zdravstvenih delavcev, manjša redundanca zdravstvenih podatkov in lažja dostopnost zdravstvenih delavcev. Zaradi svojih koristi in hitrega razvoja mobilnih tehnologij se uporaba mobilnih naprav v zdravstvu izjemno hitro širi, pri tem pa pogosto zanemarjamo njen varnostni vidik. Občutljivi osebni podatki, s katerimi pretežno delamo v zdravstvu, so zelo zanimivi za kibernetske kriminalce in kar 44 odstotkov vseh kraj in zlorab podatkov se zgodi ravno v zdravstvu. Velika večina teh zlorab je neposredna posledica uporabe mobilnih naprav, najpogosteje gre pri tem za kraje in izgube mobilnih naprav. V prispevku predstavljamo, na kaj morajo biti pri uvajanju uporabe mobilnih naprav pozorni zdravstvene ustanove in zdravstveni delavci, ki uporabljajo mobilne naprave.

Ključne besede: mobilne naprave, zdravstvo, informacijska varnost.

Abstract

Security issues of mobile device use in healthcare

Mobile devices are used progressively more in healthcare as they offer new possibilities, such as improved mobility, communication and co-ordination of healthcare workers, reduced redundancy of health data and better accessibility of healthcare workers. The use of mobile devices in healthcare is spreading extremely fast due to their benefits and the rapid development of mobile technologies; however, their security aspects are often neglected. Sensitive personal data used in healthcare is very appealing to criminals while as many as 44 percent of all data breaches occur in healthcare. The vast majority of these breaches are the direct consequence of mobile device use, most often due to mobile device theft and loss. In this paper, we demonstrate what healthcare institutions and workers using mobile devices need to pay attention to when adopting the use of mobile devices.

Keywords: mobile devices, healthcare, information security.

1 UVOD

V zdravstvu vse pogosteje uporabljajo mobilne naprave, saj ponujajo nove priložnosti za njegovo izboljšanje in optimizacijo (HIMSS Analytics, 2014). Izboljšana mobilnost, komunikacija in koordinacija zdravstvenih delavcev, manjša redundanca zdravstvenih podatkov, lažja dostopnost zdravstvenih delavcev ter izboljšanje odzivanja ob kriznih dogodkih so samo nekatere izmed koristi, ki lahko bistveno pripomorejo tako k dostopnosti in kakovosti zdravstvenih storitev kot tudi k zadovoljstvu z delom zdravstvenih delavcev in nižanjem stroškov zdravstva (HIMSS Analytics, 2014; Ren, Smith & Christensen, 2015; Slovensko društvo za medicinsko informatiko, 2014; Storbrauck, 2015). V Sloveniji na posameznih zdravstvenih ustanovah, med katere štejemo bolnišnice in zdravstvene domove, že uvajamo uporabo mobilnih naprav. Toda to niso prvi zametki uporabe mobilnih naprav v zdravstvu pri nas, saj lahko zdravstveni delavci pri delu uporabljajo svoje lastne mobilne naprave, npr. za dostop do službene elektronske pošte. V svetu to pravzaprav celo vse bolj spodbujajo in izkoriščajo za nižanje stroškov zdravstvenih ustanov (Bitglass, 2014; Martínez-Pérez, de la Torre-Díez & López-Coronado, 2015).

Toda uporaba mobilnih naprav v zdravstvu ima poleg potencialnih koristi tudi nekatere pasti. V zdravstvu namreč delamo z občutljivimi zdravstvenimi podatki bolnikov, zato ima varnost teh podatkov izjemno visoko prioriteto. Kljub temu raziskave kažejo, da se kar 44 odstotkov vseh zlorab podatkov zgodi ravno v zdravstvu, predvsem zaradi privlačnosti medicinskih podatkov za kriminalce, saj na črnem trgu ti podatki dosegajo relativno visoko vrednost (Bitglass, 2014). Velik delež zlorab v zdrav-

stvu je neposredna posledica uporabe mobilnih naprav, predvsem zaradi kraj in izgub (Bitglass, 2014; McDavid, 2013; Storbrauck, 2015). Dodatno težavo pri tem povzroča dejstvo, da zdravstvene ustanove z ukrepi za varovanje zdravstvenih podatkov ne sledijo dovolj hitro hitremu tempu uvajanja mobilnih naprav (Martínez-Pérez idr., 2015).

Ključne šibke točke upravljanja varnosti občutljivih zdravstvenih podatkov so uporaba nevarnih mobilnih aplikacij in naprav, pomanjkljivo upravljanje varnosti v zdravstvenih ustanovah in nezadostna poučenost zdravstvenih delavcev o tehničnih ter organizacijskih vidikih zagotavljanja varnosti zdravstvenih podatkov (Martínez-Pérez idr., 2015; Storbrauck, 2015; The Office of the National Coordinator for Health Information Technology, 2015; Whipple, Allgood, & Larue, 2012). Pregleda nad stanjem formalne in neformalne uporabe mobilnih naprav v slovenskem zdravstvu ni mogoče zaslediti. Dejstvo je, da v slovenskem zdravstvu že uporabljajo mobilne naprave in da jih bodo uporabljali vedno bolj. Toda konkretnih podatkov o tem, kako razširjena in predvsem kako varna je uporaba mobilnih naprav v slovenskem zdravstvu, trenutno ni.

Z namenom dviga zavesti o pomembnosti varne uporabe mobilnih naprav v slovenskih zdravstvenih ustanovah so v nadaljevanju predstavljeni uporaba mobilnih naprav v zdravstvu, ključni varnostni izzivi in temelji za upravljanje varnosti.

2 MOBILNE NAPRAVE V ZDRAVSTVU

Mobilne naprave, med katere štejemo pametne telefone in tablične računalnike, so v zadnjih letih postale del našega vsakdana, hkrati pa jih vse pogosteje uporabljamo tudi v poslovne namene. Pri tem ni izjema niti zdravstvo, saj npr. v ZDA mobilne naprave uporabljajo v dobri četrtini bolnišnic (HIMSS Analytics, 2014; Martínez-Pérez idr., 2015; Storbrauck, 2015). Vse pogosteje zdravstvenim delavcem dovoljujejo oz. jih celo spodbujajo k uporabi lastnih mobilnih naprav pri delu (angl. bring your own device – BYOD), saj je to priročno za uporabnike in pomeni priložnost za prihranke pri stroških organizacij (Bitglass, 2014; Martínez-Pérez idr., 2015). V ZDA na ta način mobilne naprave pri svojem delu uporablja več kot devetdeset odstotkov zdravstvenih delavcev za dostop do elektronskih zdravstvenih zapisov (Bitglass, 2014; Martínez-Pérez idr., 2015). Mobilne naprave so torej v razvitih državah vseprisotne (Whipple idr., 2012), podoben trend pa lahko pričakujemo tudi v Sloveniji, kjer v posameznih bolnišnicah že uvajajo mobilne naprave, zdravstveni delavci pa lahko pri svojem delu uporabljajo svoje mobilne naprave, npr. za dostop do službene elektronske pošte.

Uporaba mobilnih naprav ima veliko potencialnih koristi za zdravstvo. Trenutno mobilne naprave najbolj uporabljajo kot alternativo delovnim postajam (osebnim oz. prenosnim računalnikom) za dostop do informacij (HIMSS Analytics, 2014). Z njimi je mogoče dostopati do občutljivih zdravstvenih informacij, kot so npr. zdravstveni zapisi, zgodovina zdravljenja ali načrti zdravljenja, in jih shranjevati, ne glede na to, kje se nahajajo zdravstveni delavci, v bolnišnični sobi, na sestanku, na obisku na domu ali kje drugje (Storbrauck, 2015). Uporaba mobilnih naprav pripomore tudi k učinkovitosti in kakovosti v zdravstvu, saj odpravlja redundanco podatkov in izboljšuje komunikacijo ter koordinacijo med različnimi deležniki znotraj zdravstvenih ustanov in med njimi (HIMSS Analytics, 2014; Slovensko društvo za medicinsko informatiko, 2014; Storbrauck, 2015). Poleg tega uporaba mobilnih naprav zaradi svoje priročnosti pozitivno vpliva tudi na zadovoljstvo zdravstvenih delavcev z delom (HIMSS Analytics, 2014). K uporabi mobilnih naprav v zdravstvu se nagibajo tudi bolniki, ki vedno bolj stremijo k elektronski komunikaciji z zdravstvenimi delavci prek elektronske pošte ali s kratkimi sporočili (The Office of the National Coordinator for Health Information Technology, 2015).

Mobilne naprave poleg obstoječih koristi za zdravstvo ponujajo še nove priložnosti, ki bi lahko v bližnji prihodnosti povzročile bistvene spremembe v zdravstvu (Safavi & Shukur, 2014). Že danes je mogoče v uradnih trgovinah mobilnih aplikacij (npr. Apple App Store, Google Play) najti več deset tisoč mobilnih aplikacij, povezanih z medicino in zdravstvom (Martínez-Pérez idr., 2015). Mobilne naprave je namreč mogoče povezati z merilniki srčnega utripa, krvnega sladkorja idr., ki podatke zbirajo in prenašajo na svetovni splet v realnem času (Bitglass, 2014). Proizvajalci poleg tega proizvajajo mobilne naprave, ki imajo že vgrajene zmožnosti za zajem in prenos podatkov (npr. Google Glasses), pred kratkim pa so predstavili tudi ustrezne aplikacije, npr. Apple HealthKit, Google Fit in Samsung S Health (Safavi & Shukur, 2014).

Poleg navedenih koristi je mogoče mobilne naprave smiselno uporabiti tudi za podporo zdravstva

med kriznimi dogodki in po njih – od obsežnejših kriz zaradi naravnih nesreč ali epidemij do izoliranih in omejenih primerov. Mobilne naprave imajo potencial, da v to vključijo in povežejo večje število deležnikov, npr. civilne uporabnike je mogoče prek operativnih centrov povezati z oddaljenimi zdravstvenimi delavci (Ren idr., 2015).

3 VARNOSTNI IZZIVI UPORABE MOBILNIH NAPRAV V ZDRAVSTVU

3.1 Pregled varnostnih izzivov

Problem hitre širitve uporabe mobilnih naprav v zdravstvu je v tem, da se hkrati povečuje tudi tveganje za zlorabo podatkov (Storbrauck, 2015). Uporabniki namreč hitreje adoptirajo mobilne tehnologije, kot lahko zdravstvene ustanove zagotavljajo ustrezne pogoje za varovanje občutljivih zdravstvenih podatkov (Martínez-Pérez idr., 2015). Podobne težave imajo tudi zakonodajalci, ki težko sledijo razvoju novih tehnologij (Martínez-Pérez idr., 2015). Kako velik problem je zloraba podatkov v zdravstvu v primerjavi z drugimi panogami, nazorno pove informacija, da ta pomeni kar 44 odstotkov vseh zlorab podatkov (Bitglass, 2014). Težava pri tako velikem deležu zlorab je tudi zaupanje bolnikov v zagotavljanje zasebnosti in točnosti elektronskih zdravstvenih zapisov (The Office of the National Coordinator for Health Information Technology, 2015). Pri bolnikih se tako pojavljajo različne oblike odpora do razkrivanja občutljivih informacij zdravstvenim delavcem (The Office of the National Coordinator for Health Information Technology, 2015). Z namenom vračanja zaupanja bolnikov v zdravstvene ustanove in motiviranja zdravstvenih ustanov za zagotavljanje varnosti občutljivih informacij so npr. v ZDA postavili portal z javno dostopnimi podatki o zlorabah občutljivih podatkov v zdravstvenih ustanovah, t. i. The Wall of Shame, dostopen na spletnem naslovu www.hhs.gov (Bitglass, 2014).

Razlogi za zlorabo občutljivih medicinskih podatkov so raznoliki. Kibernetski kriminalci lahko poskušajo pridobiti neposredne finančne koristi, izvesti elektronsko prevaro, ukrasti identiteto ali izsiljevati žrtve (Storbrauck, 2015). Poleg tega se do podatkov neupravičeno dostopa tudi manj zlonamerno, npr. za zadovoljevanje radovednosti zdravstvenih delavcev. Tudi pri teh primerih gre za grob poseg v zasebnost posameznikov. V primerih, ko gre za vpogled v občutljive zdravstvene podatke visokih državnih funkcionarjev, je lahko ogrožena tudi nacionalna varnost. V tujini je vse pogostejša kraja medicinske identitete, pri kateri se kriminalec zdravstveni ustanovi predstavlja kot žrtev in izrablja zdravstvene storitve ali dostop do prepovedanih substanc v njenem imenu (Bitglass, 2014; McDavid, 2013). Za kibernetske kriminalce je kraja medicinske identitete zelo mamljiva, saj je zdravstvenim delavcem relativno preprosto ukrasti mobilno napravo (Bitglass, 2014). Poleg finančnih posledic ima lahko kraja medicinske identitete tudi hujše, medicinske posledice. V zdravstvene kartoteke žrtve kriminalci z uporabo zdravstvenih storitev dodajajo neresnične zdravstvene podatke, kar lahko privede do zmede pri diagnosticiranju, resne medicinske škode ali celo smrti (Bitglass, 2014; McDavid, 2013).

Kibernetski kriminalci največkrat napadejo mobilne naprave prek elektronske pošte in zlonamerne programske opreme (Storbrauck, 2015), vendar to še zdaleč ni največja težava, saj je velika večina – več kot dve tretjini – zlorab v zdravstvu povezanih z izgubo ali krajo mobilnih naprav (Bitglass, 2014; McDavid, 2013; Storbrauck, 2015). Pri odzivanju na nujne primere se lahko hitro zgodi, da zdravstveni delavec nehote pusti mobilno napravo za krajši čas nenadzorovano, kar ponuja priložnost za njeno neavtorizirano uporabo ali krajo (Storbrauck, 2015). Že uporaba uveljavljenih varnostnih mehanizmov, kot so zaklenitev mobilne naprave, uporaba gesla za njeno odklepanje in šifriranje podatkovnih nosilcev, bi tatovom preprečila zlorabo informacij (Storbrauck, 2015). Skrb vzbuja podatek, da večina zdravstvenih delavcev svoje mobilne naprave ne zaklene nikoli (Whipple idr., 2012). Poleg tega se večina uporabnikov mobilnih naprav ne zaveda ali ni seznanjena z vidiki varnosti in zasebnosti pri uporabi mobilnih naprav (Martínez-Pérez idr., 2015; Storbrauck, 2015; Whipple idr., 2012). V zdravstvenih ustanovah tako pogosto naletimo na neuporabo gesel, uporabo šibkih gesel (npr. abcd) in skupna gesla (Storbrauck, 2015). Zagotavljanje varnosti in zasebnosti je deljena odgovornost, česar se v večini zdravstvenih ustanov premalo zavedajo, saj jih le 38 odstotkov opredeljuje formalno politiko dela z mobilnimi napravami (Martínez-Pérez idr., 2015; Storbrauck, 2015; The Office of the National Coordinator for Health Information Technology, 2015).

Za mobilne aplikacije je značilno, da se razvijajo

izjemno hitro. Hkrati ni zaslediti standardnih metod za zagotavljanje razvoja varnih mobilnih aplikacij, ki bi jih lahko pri razvoju uporabljali razvijalci (Martínez-Pérez idr., 2015). Razvite aplikacije zaradi tega pogosto ne zagotavljajo ustrezne varnosti. Če zdravstveni delavci uporabljajo mobilne aplikacije, ki jih ne razvijejo zdravstvene ustanove oz. njihovi podizvajalci, je varnost uporabe teh mobilnih aplikacij zelo vprašljiva. Dostopni in pogosto občutljivi podatki so pri tem izjemno izpostavljeni. Niso pa le mobilne aplikacije tiste, ki vzbujajo dvom v varno uporabo mobilnih naprav. Tudi mobilne naprave same bi morale omogočati varen dostop do občutljivih podatkov (HIMSS Analytics, 2014). Toda nekatere najsodobnejše naprave so pomanjkljive in varnega dostopa sploh ne omogočajo, zaradi česar je potrebna previdnost pri njihovi izbiri (Safavi & Shukur, 2014).

V Sloveniji v posameznih bolnišnicah že uvajajo mobilne naprave, npr. na Pediatrični kliniki UKC Ljubljana. Poleg tega zdravstveni delavci pri svojem delu tudi že uporabljajo svoje mobilne naprave, npr. za dostop do službene elektronske pošte, kar pomeni, da z njimi lahko dostopajo do občutljivih zdravstvenih podatkov bolnikov. Celovitega pregleda nad trenutnim stanjem in trendi adopcije mobilnih naprav v slovenskem zdravstvu ni. Ravno tako ni podatkov o tem, koliko so zdravstvene ustanove sploh pripravljene na adopcijo mobilnih naprav in kako dobro so zdravstveni delavci, ki sicer pri svojem delu že uporabljajo mobilne naprave, seznanjeni z vidiki varnosti in zasebnosti pri njihovi uporabi. Tudi razvojna strategija zdravstvenega varstva ne vključuje razvoja na področju zagotavljanja varnosti in zasebnosti pri uporabi mobilnih naprav v zdravstvu (Ministrstvo za zdravje, 2015). To je problematično, saj trendi iz tujine kažejo, da se bodo v zdravstvu uporabljale mobilne naprave, in sicer vedno bolj. Brez celovitega pregleda nad stanjem v slovenskem zdravstvu ni mogoča priprava učinkovitih ukrepov na nacionalni ravni. Ti ukrepi so nujni, če bi želeli v slovenskem zdravstvu izkoristiti koristi mobilnih naprav, saj sicer tvegamo bistveno znižanje varnosti občutljivih zdravstvenih podatkov v zdravstvenih ustanovah.

3.2 Soočanje z varnostnimi izzivi

Temelj upravljanja varnosti občutljivih zdravstvenih podatkov pri delu z mobilnimi napravami je vzpostavitev sistema za upravljanje kibernetske varnosti v zdravstvenih ustanovah. Najprej je treba opredeliti administrativne ukrepe, politike in procedure za preprečevanje, ugotavljanje in popravljanje varnostnih kršitev (Storbrauck, 2015; The Office of the National Coordinator for Health Information Technology, 2015). Administrativni ukrepi temeljijo na analizi varnostnih tveganj, v okviru katere najprej identificiramo in analiziramo tveganja, nato pa implementiramo varnostne ukrepe za njihovo zmanjševanje (The Office of the National Coordinator for Health Information Technology, 2015). V tujini so se zaradi pomembnosti varovanja podatkov začele pojavljati tudi nove vloge, npr. pooblaščenec za zasebnost (angl. privacy officer), ki imajo odgovornost in avtoriteto za zagotavljanje varovanja občutljivih podatkov v zdravstvenih ustanovah (McDavid, 2013).

Administrativni ukrepi ne morejo biti uspešni, če za njihovo implementacijo v praksi ustrezno ne izobrazimo zdravstvenih delavcev (Storbrauck, 2015). Zaradi razširjenosti uporabe mobilnih naprav med študenti medicine je mogoče in potrebno s splošnim izobraževanjem o varnosti uporabe mobilnih naprav začeti že med študijem, saj se že študenti srečujejo z občutljivimi zdravstvenimi podatki (Whipple idr., 2012). V zdravstvenih ustanovah je treba vzdrževati pregled nad znanjem in poznavanjem varnostnih tematik zdravstvenih delavcev (McDavid, 2013). Izobraževanje zdravstvenih delavcev je sicer zahtevna naloga za vodstva zdravstvenih ustanov, saj so vsi zdravstveni delavci tipično zelo obremenjeni z vsakdanjim delom, vse t. i. podrobnosti, med katere štejejo predvsem informacijsko tehnologijo in zagotavljanje kibernetske varnosti, pa so zanje sekundarnega pomena. Zaradi tega je pomembno, da med zdravstvenimi delavci prek vodstev zdravstvenih ustanov in programov opismenjevanja dvignemo zavest o pomembnosti zasebnosti in varnosti občutljivih zdravstvenih informacij ter posledicah izgube ali kraje mobilnih naprav. Že s preprostimi ukrepi, kot so šifriranje zdravstvenih podatkov, zaklepanje mobilnih naprav in uporaba gesel za njihovo odklepanje, lahko kriminalcem preprečimo krajo medicinskih identitet tudi v primerih, ko ukradejo mobilno napravo (McDavid, 2013; Storbrauck, 2015). Izobraževanje je treba prilagoditi različnim zdravstvenim delavcem (zdravnikom, medicinskim sestram idr.) in njihovim načinom dela. Tako dobijo zdravstveni delavci na voljo predvsem tiste ključne informacije o varni uporabi mobilnih naprav, ki jih vsakodnevno potrebujejo pri svojem delu.

Drugi temelj so fizični ukrepi, ki so namenjeni varovanju celotnega informacijskega sistema in z njim povezanih prostorov ter naprav (The Office of the National Coordinator for Health Information Technology, 2015). Glede na to, da je več kot dve tretjini zlorab podatkov v zdravstvu povezanih z izgubo ali krajo mobilnih naprav, gre za pomembne ukrepe, ki lahko ublažijo velik del verjetnosti zlorab podatkov (Bitglass, 2014; McDavid, 2013; Storbrauck, 2015). Fizični ukrepi obsegajo tako tehnološke rešitve kot tudi varnostno politiko in procedure za njihovo uporabo (The Office of the National Coordinator for Health Information Technology, 2015). Tudi o fizičnih ukrepih je treba seznaniti zdravstvene delavce in pridobiti njihovo podporo, saj brez njihovega sodelovanja fizični ukrepi ne morejo biti učinkoviti.

Tretji temelj se nanaša na organizacije, ki na kakršen koli način izmenjujejo občutljive zdravstvene podatke z zdravstvenimi ustanovami (The Office of the National Coordinator for Health Information Technology, 2015). Mobilne naprave s številnimi mobilnimi aplikacijami omogočajo lažje povezovanje z različnimi organizacijami in za različne namene. Bistveno pri tem je, da občutljive podatke izmenjujemo samo z organizacijami, ki so pogodbeno vezane k varovanju občutljivih podatkov in ki so tega tudi sposobne, kar je priporočljivo tudi preverjati (McDavid, 2013; The Office of the National Coordinator for Health Information Technology, 2015). Kljub temu je pričakovanje, da lahko pogodbeni partnerji sami zagotavljajo varnost podatkov, nekoliko utopično. Na primer ponudniki elektronske pošte lahko na svojih strežnikih zelo dobro zagotavljajo njeno varnost, vendar nimajo nobenega nadzora, kaj se dogaja z elektronsko pošto, ko jih zapusti – npr. kaj se zgodi s prejeto pošto na zdravnikovi mobilni napravi (Bitglass, 2014).

Četrti temelj se nanaša na periodično prilagajanje in vzdrževanje vseh varnostnih ukrepov glede na spremembe v okolju ali organizacijske spremembe, ki kakor koli vplivajo na varnost občutljivih zdravstvenih podatkov (McDavid, 2013; The Office of the National Coordinator for Health Information Technology, 2015).

4 SKLEP

V prispevku smo predstavili uporabo mobilnih naprav v zdravstvu, varnostne izzive, ki se pojavljajo pri tem, in temelje za upravljanje varnosti. Medtem ko se v svetu uporaba mobilnih naprav v zdravstvu izjemno hitro širi, v Sloveniji mobilne naprave šele začenjamo uporabljati. Podoben trend lahko v kratkem pričakujemo tudi pri nas, saj prinašajo mobilne naprave veliko koristi tako zdravstvenim delavcem kot zdravstvenim ustanovam. Zdravstvene ustanove bodo tako soočene z izzivom, kako se ustrezno pripraviti na to in zagotavljati zadovoljivo raven varnosti in zasebnosti občutljivih zdravstvenih podatkov.

5 LITERATURA

[1] Bitglass. (2014). *The 2014 Bitglass Healthcare Breach Report*. Dostopno na http://pages.bitglass.com/rs/bitglass/images/WP-Healthcare-Report-2014.pdf.

[2] HIMSS Analytics. (2014). *2014 Mobile Devices Study*. Dostopno na http://www.himssanalytics.org/research/essentials--brief-mobile-devices-study.

[3] Martínez-Pérez, B., de la Torre-Díez, I. & López-Coronado, M. (2015). Privacy and Security in Mobile Health Apps: A Review and Recommendations. *Journal of Medical Systems*, *39*(1), 181: 1–8. http://doi.org/10.1007/s10916-014-0181-3.

[4] McDavid, J. P. (2013). HIPAA Risk Is Contagious: Practical Tips to Prevent Breach. *The Journal of Medical Practice Management*, *29*(1), 53–55.

[5] Ministrstvo za zdravje. (2015). *Resolucija o nacionalnem planu zdravstvenega varstva 2015–2025* (ResNPZV 2015–2025).

[6] Ren, C. H., Smith, W. K. & Christensen, J. (2015). A Medical System for Supporting Civilian Crisis Response. *Journal of Homeland Security and Emergency Management*, *12*(2), 299–318. http://doi.org/10.1515/jhsem-2014-0040.

[7] Safavi, S. & Shukur, Z. (2014). Conceptual Privacy Framework for Health Information on Wearable Device. *PLOS ONE*, *9*(12), e114306: 1–16. http://doi.org/10.1371/journal.pone.0114306.

[8] Slovensko društvo za medicinsko informatiko. (2014). Zaključki kongresa MI'2014. Dostopno na http://www.sdmi.si/tl_files/Strokovna_srecanja/Zakljucki kongresa MI 2014.pdf.

[9] Storbrauck, L. (2015). *Mobile Device Use: Increasing Privacy and Security Awareness for Nurse Practitioners*.

[10] The Office of the National Coordinator for Health Information Technology. (2015). *Guide to Privacy and Security of Electronic Health Information.*

[11] Whipple, E. C., Allgood, K. L. & Larue, E. M. (2012). Third--year medical students' knowledge of privacy and security issues concerning mobile devices. *Medical Teacher*, *34*(8), e532–e548. http://doi.org/10.3109/0142159X.2012.670319.

▪

Simon Vrhovec je zaposlen na Fakulteti za varnostne vede Univerze v Mariboru. Doktoriral je leta 2015 na Fakulteti za računalništvo in informatiko Univerze v Ljubljani. Njegova glavna raziskovalna področja so vodenje projektov, odpor deležnikov do sprememb, agilne metode, globalni razvoj programske opreme, informacijska varnost in digitalna forenzika.