Samanta Mikuletič, mag. Tamara Štemberger Kolnik, dr. Boštjan Žvanut

Informacijska zasebnost in varovanje pacientovih podatkov

Znanstveni članek

UDK 614.253.8:004

KLJUČNE BESEDE: zdravstvena nega, informacijske tehnologije, varnost, zaupnost, zdravstveni podatki

POVZETEK - V praksi je nevarnost za kršenje informacijske varnosti pacientovih osebnih podatkov velika. Pregled literature kaže na izredno slabo stanje na omenjenem področju, zato je bil cilj raziskave identificirati vzroke za tako stanje. Izvedena je bila kvalitativna študija v maju in juniju 2013. Intervjuvani so bili strokovnjaki s področja zdravstvene nege in informatike v zdravstvu primarne, sekundarne in terciarne zdravstvene ravni (4 vodilne medicinske sestre, 3 vodje informatike in en strokovnjak z obeh področij). Iz zapisov intervjujev smo identificirali naslednje elemente, ki lahko predstavljajo resno tveganje za informacijsko varnost: »nezadostno znanje s področja informatike«, »slabo poznavanje oz. nepoznavanje pojma informacijske varnosti«, in »neobstoj formalne varnostne politike na področju informacijske varnosti«. Prisotnost zgoraj navedenih elementov kažejo na alarmantno stanje na področju informacijske varnosti v zdravstveni negi in zdravstvu v Sloveniji. Omenjeni problematiki bomo morali v bodoče posvetiti posebno pozornost, saj predstavlja tempirano bombo pri zaščiti pravic in interesov pacientov. Na podlagi ugotovitev je smiselno oblikovati mehanizem opozarjanja na varnost pacientovih podatkov in dvigniti zavest zdravstvenih delavcev o odgovornosti pri ravnanju s temi podatki.

Scientific article

UDC 614.253.8:004

KEY WORDS: nursing, information technologies, security policy, confidentiality, healthcare data

ABSTRACT - In practice, there is a considerable risk of information security violation of the patients' personal data. Results of literature review indicate an extremely bad situation in this field. Hence, the aim of this study was to identify the reasons for such a risky situation. A qualitative study was performed in May and June 2013. Experts in the field of nursing and informatics in nursing from primary, secondary, and tertiary levels of healthcare were interviewed (4 nursing managers, 3 IT managers and one expert in both fields). The presence of the following elements, which could potentially increase the likelihood of information security violation, were identified form the interview transcripts: "Insufficient knowledge in the field of informatics," "Unfamiliarity with the information security concept", and "The absence of a formal security policy in the field of information security". The presence of the aforementioned elements in Slovenian nursing practice indicates an alarming situation in the field of nursing informatics and health care informatics in Slovenia. Special attention should be put to this problem immediately, as it represents a time bomb in the process of protecting the patients' rights and interests. Based on our findings, a warning mechanism for protecting the patients' data privacy should be established. Furthermore, the awareness of healthcare workers' responsibility for these data should be raised.

1 Uvod

Informacijsko komunikacijske tehnologije (v nadaljevanju IKT) so postale sestavni del življenja. Njihov razvoj je korenito posegel v spremembo delovnega okolja medicinskih sester (Prijatelj in sod., 2011). Svetovna zdravstvena organizacija v svoji resoluciji o e-zdravju WHA 58.28 opozarja države članice, da morajo usmeriti zdravstveno osebje v dopolnitev znanja in pridobivanje ustreznih kompetenc IKT (Svetovna zdravstvena organizacija, 2005). Medicinske sestre in zdravstveni tehniki (v nada-

ljevanju je uporabljen izraz medicinske sestre) predstavljajo največji delež v skupini izvajalcev zdravstvenih storitev. Številni viri poudarjajo pomen kompetenc IKT pri omenjeni populaciji (American Nurses Association, 2008; Fetter, 2009). Na primer, While in Dewsbury (2011) navajata, da medicinske sestre ne smejo biti zgolj pasivni uporabniki omenjenih tehnologij, temveč morajo na področju IKT prevzeti aktivno vlogo. Ne glede na navedeno pa razpoložljivi informacijski sistemi (v nadaljevanju IS) v Sloveniji še vedno zagotavljajo le nekatere podatke, ki so potrebni za izvajanje zdravstvene nege pacienta.

Zdravstveni sistem za svoje normalno delovanje potrebuje pravočasno dostopne informacije (Zabukovec in Bohinc, 2001). Slednje se med zdravstveno oskrbo pacienta uporabljajo pri izvajanju zdravstvene nege, zagotavljanju varne zdravstvene oskrbe, obračunavanju izvedenih storitev in porabljenega materiala, pri izobraževanju, raziskovanju, za nadzor nad izvajanjem in kakovostjo zdravstvene oskrbe ter za statistične analize (Prijatelj in sod., 2011). Na področje kompetenc IKT medicinskih sester sodijo tudi kompetence s področja informatike in informacijske varnosti (American Nurses Association, 2008; Fetter, 2009).

Nagel razvoj IKT je povzročil spolzko področje etično-pravnih pomislekov (Polito, 2012). Medicinska sestra pri svojem delu prevzema številne odgovornosti, ki jih ni mogoče določiti samo z zakoni in predpisi. Poleg njih morajo medicinske sestre spoštovati določbe Kodeksa etike medicinskih sester in zdravstvenih tehnikov (2010, 2014). Omenjeni Kodeks v III. načelu določa, da mora medicinska sestra varovati kot poklicno skrivnost osebne podatke o zdravstvenem stanju pacienta, o vzrokih, okoliščinah in posledicah določenega stanja. Zakon o varstvu osebnih podatkov pa definira osebni podatek kot vsak podatek, ki se nanaša na posameznika ne glede na obliko, v kateri je izražen (Zakon o varstvu osebnih podatkov, 2004). Zdravstvena ustanova mora vzpostaviti ustrezen IS, ki zagotavlja zaupnost pacientovih osebnih podatkov. Prav tako mora po IV. načelu Kodeksa etike medicinska sestra spoštovati dostojanstvo in zasebnost pacienta v vseh stanjih zdravja, bolezni in ob umiranju (Kodeks etike medicinskih sester in zdravstvenih tehnikov Slovenije – 2005, 2010).

Pravica do zasebnosti je v Republiki Sloveniji ustavna pravica in je eden izmed nepogrešljivih elementov človeškega obstoja (Ustava Republike Slovenije, 1991). Pri uporabi osebnih podatkov pacienta bi moralo biti zagotovljeno suvereno in varno rokovanje s strani osebja in ustanove, kar predstavlja le manjše, najnujnejše posege v odločitveno, duševno, prostorsko in informacijsko zasebnost pacienta (Lampe, 2004). Osebni podatki so nematerialne dobrine, ki jih posameznik le s soglasjem razkrije javnosti (Gradišar, 2003). Pravico do varstva zasebnosti in varstva osebnih podatkov v Republiki Sloveniji določa Zakon o varstvu osebnih podatkov (2004). Za paciente, ki vstopajo v zdravstveni sistem, pa so pomembna tudi določila iz Zakona o pacientovih pravicah (2008). Informacijska zasebnost je definirana kot pravica do sodelovanja posameznika pri odločitvah, ki se nanašajo na zbiranje, uporabo in razkrivanje osebnih podatkov ali informacij (Gradišar, 2003).

Dolžnost zaposlenih v zdravstvu je, da, ne glede na način, na katerega so bili podatki pridobljeni ali na katerega jih posredujejo, ohranjajo njihovo zaupnost in s tem

skrbijo za pacientovo zasebnost (Informacijski pooblaščenec Republike Slovenije, n. d.). Prav tako imajo pacienti pravico do nadzora nad dostopom in razkritjem osebnih zdravstvenih podatkov, tako da podelijo, odrečejo ali odvzamejo pooblastila, s katerimi določijo, kdo lahko dobi informacije od zdravstvenega osebja. Osebni podatki pacienta se lahko med zdravstvenimi delavci prenašajo, le če omogočajo kontinuirano zdravstveno negovalno obravnavo pacienta, vendar le tisti, ki so nujno potrebni. V primeru razkritja osebnih podatkov, na katerega pacient ni pristal, morajo zdravstveni delavci upoštevati nujnost in sorazmernost razkritja podatkov ter spremljajoče tveganje (Informacijski pooblaščenec Republike Slovenije, n. d.). Razkriti zaupni podatki ne morejo postati nikoli več tajni.

Osebni podatki so lahko neupravičeno dostopni in razkriti preko pooblaščenih uporabnikov informacijskega sistema. Številni incidenti opozarjajo na pomanjkljivosti IS (Neame, 2008), zaradi katerih prihaja do uhajanja informacij. Informacijske vire lahko ogrožajo nesreče in računalniški kriminal (tj. kakršna koli uporaba informacijskega sistema pri nezakonitih dejanjih: kraja, sabotaža in vandalizem). K nesrečam sodijo poškodbe računalniške opreme, njene neprimerne tehnične karakteristike, neodgovornost zaposlenih, napake v programih in podatkih, strojne okvare in napačno ravnanje (Gradišar, 2003). Že dalj časa je jasno, da sama tehnologija ni zadosten pogoj za ustrezno varnost podatkov v informacijskem sistemu (Trček in sod., 2007). Vsi uporabniki IS lahko potencialno ogrozijo zasebnost pacientov (Neame, 2008). Medicinske sestre kot primarni uporabnik v informacijskem sistemu prav tako dostopajo do podatkov, za katere so kompetentne. Velikokrat pa lahko dostopajo tudi do podatkov kot sekundarni uporabnik informacijskega sistema preko pooblastil druge osebe, kar poveča možnost zlorabe osebnih podatkov pacienta ali vpogled v podatke s strani drugih nepooblaščenih oseb (Polito in sod., 2012). Dodatno nevarnost pa predstavlja organizacija pacientovega zdravljenja v zdravstvenih ustanovah. V praksi so interakcije osebja z informacijskim sistemom organizirane tako, da do osebnih zdravstvenih podatkov lahko dostopa več članov zdravstvenega tima hkrati (Informacijski pooblaščenec Republike Slovenije, n. d.). V praksi se zelo pogosto dogaja, da je v IS prijavljen le en član tima (npr. zdravnik) in tako se zabeleži zgolj en vpogled v podatke, čeprav jih je dejansko bilo veliko več (npr. medicinska sestra, specializant, lahko tudi administratorka v ambulantnem timu) (Informacijski pooblaščenec Republike Slovenije, n. d.).

Glavni in najbolj pomemben dejavnik za zagotavljanje varnosti IS je človek sam. Da se zagotovi ustrezna varnost v sodobnih IS, moramo poleg tehnologije obravnavati tudi človeško vedenje in vprašanja, ki so utelešena v varnostni politiki (Trček in sod., 2007). Informacijska varnost je postala vse večji izziv, saj so hitro se razvijajoči IS postali vse bolj zapleteni in raznoliki (Glaser in Aske, 2010). Varnostna politika IS temelji na varovanju podatkov in zagotavlja celovit pogled na varnost IS ter zajema številne dejavnike, med njimi tudi organizacijska pravila in postopke, ki kakor koli vplivajo na varno in zanesljivo delovanje celotnega IS. Varnostna politika sama po sebi ne zagotavlja boljšega varovanja IS, če ni prisoten človeški faktor, ki določila iz varnostne politike prenese v prakso (Štrakl, 2003).

Organizacija, ki želi v svojem okolju vzpostaviti želeno raven informacijske varnosti, mora vzpostaviti ustrezen sistem za varovanje informacij (Brezavšček in Mo-škon, 2010). Proces za upravljanje z informacijsko varnostjo je nabor organizacijskih postopkov, odločitev in tehničnih ukrepov, ki jih izvaja organizacija zaradi varovanja podatkov in informacij v elektronski obliki in tudi v drugih materialnih oblikah (npr. na papirju) (Ministrstvo za zdravje, n. d.).

Vzdrževanje ustrezne ravni informacijske varnosti je neskončen proces, saj se število groženj neprestano povečuje (Glaser and Aske, 2010). Vzpostavitev informacijske varnosti ni zgolj uvajanje novih varnostnih tehnologij, temveč vključuje tudi usmeritve, postopke in ukrepe, ki skrbijo, da ostanejo podatki zaupni in so na voljo tistim, ki jih potrebujejo (Glaser in Aske, 2010). Pogosto uporabljeni standardi in priporočila na področju varovanja informacij so: npr. ISO/IEC 27000 (ISO, n.d.), »Control Objectives for Information and related Technology« - COBIT (IT Governance Institute, 2007); Information Technology Infrastructure Library« - ITIL (Cartlidge in sod., 2007).

Zaščititi organizacijo pred vsemi varnostnimi tveganji, povezanimi z informacijsko varnostjo, je praktično nemogoče. V večjih organizacijah je treba ustanoviti usmerjevalni odbor za informacijsko varnost. Slednji naj bi bil odgovoren za oblikovanje varnostne strategije in politike (Glaser in Aske, 2010). Vodstvo lahko imenuje odgovornega za informacijsko varnost (ang. »Chief Information Security Officer« - CISO). V večjih zdravstvenih organizacijah bi bil CISO nujno potreben in zaposlen za polni delovni čas (Glaser in Aske, 2010). Prej ali slej se vsi izvajalci zdravstvenih storitev soočijo z večjimi ali manjšimi informacijskimi incidenti. To je lahko npr. izguba prenosnika, na katerem so shranjeni podatki o pacientu, prisotnost virusa, ki zavira uporabo IS, ribarjenje (angl. »fishing«). Za odziv na takšne dogodke mora organizacija razviti t. i. odzivni načrt za informacijsko varnost, ki določa različne vrste varnostnih incidentov. Organizacije bi morale tesno sodelovati s pravnimi svetovalci pri oblikovanju načrtov za zagotovitev informacijske varnosti (Dimitropoulos in sod., 2011).

Tveganje za kršitev informacijske zasebnosti pacientov v praksi je v zdravstveni negi zelo veliko. Albarrak (2012) poroča o številnih nevarnih vsakodnevnih dejanjih medicinskih sester, ki ogrožajo informacijsko varnost. Pri pregledu strokovne in znanstvene literature ni bilo na voljo relevantnih virov, ki bi v slovenskem prostoru preučevali omenjeno problematiko z vidika medicinskih sester. Skladno s tem smo si zastavili naslednje raziskovalno vprašanje:

»Kateri elementi, ki lahko povečajo verjetnost kršitve informacijske varnosti, so pri medicinskih sestrah prisotni v praksi?«

2 Metoda

Uporabljen je bil kvalitativni pristop k raziskovanju, natančneje metoda intervjuvanja. Za slednjo smo se odločili predvsem zaradi ciljno usmerjenih vprašanj. Slednja

omogočajo pridobivanje dodatnih informacij, ki jih z ostalimi raziskovalnimi instrumenti ni možno pridobiti (Ivanko, 2007). V nadaljevanju je podrobneje predstavljen raziskovalni instrument, intervjuvanci in potek raziskave.

2.1 Opis instrumenta

Sodobna metodologija intervjuvanja predpostavlja odprtost vprašalnika, kar pomeni, da vprašalnik ni dokončen in da se ta lahko spremeni (Ivanko, 2007). Skladno s tem smo intervjuje izvedli s pomočjo vprašalnika s štirimi vprašanji odprtega tipa (tabela 1), ki smo ga razvili za potrebe pričujoče raziskave. Osnova za vprašanja so bili izsledki iz podobnih študij v tujini. Večina pogovorov je bila zvočno posnetih zaradi morebitnega napačnega razumevanja oziroma nerodnega zapisa odgovora. Le en intervjuvanec je izrazil željo, da se ga ne snema, zato smo si pogovor zabeležili. Iz zvočnih zapisov intervjujev smo naredili transkripte (razen v prej navedenem primeru, ko smo namesto transkripta uporabili zapise iz intervjuja).

Tabela 1: Vprašalnik

Zap. št./ No.	*Vprašanje Question*
1	Kako v vaši ustanovi medicinske sestre obvladajo potrebno znanje s področja informatike?/How nurses in your institution are proficient with the required knowledge in the field of informatics?
2	Ali se medicinske sestre zavedajo pomena informacijske varnosti za pacienta?/Are nurses in your institution aware of the importance of information security?
3	Kako bi ocenili znanje o informacijski varnosti s strani medicinskih sester?/ /How could you evaluate nurses' knowledge in the field of information security?
4	Ali ima vaša organizacija varnostno politiko na področju informacijske varnosti?/ Does your institution have information security policy?

2.2 Intervjuvanci

Odgovore na raziskovalno vprašanje in njegova podvprašanja smo želeli preveriti s kompetentnimi strokovnjaki s področja zdravstvene nege (pomočnica direktorja za zdravstveno nego) in informatike v zdravstvu (vodje informatike v zdravstveni ustanovi) z vsaj deset let izkušenj na tem področju. Intervjuje smo izvedli najprej z dvema pomočnicama direktorja za zdravstveno nego in dvema vodjema informatike v zdravstveni ustanovi. Število intervjuvancev smo postopoma povečevali, dokler nismo z novimi intervjuji pridobili novih relevantnih informacij. Skupaj so bili tako izvedeni štirje intervjuji z vodilnimi medicinskimi sestrami, trije z vodji informatike in en intervju z vodilno medicinsko sestro, strokovnjakinjo na področju informatike in zdravstvene nege, ki je vodja v eni od slovenskih zdravstvenih ustanov.

2.3 Opis poteka raziskave in obdelave podatkov

Sistematični pregled literature je vključeval različne znanstvene in strokovne članke, monografije in spletne strani. Iskanje je potekalo s pomočjo pregleda spletnih storitev, ki so relevantne za razumevanje konceptov s strokovnega področja zdravstvene nege. Pregledali smo spletne storitve: »COBISS«, »Google učenjak«, »Science Direct«, »EBSCO host«, »Wiley Online Library«, PubMed, Medline, CINAHL, Health

Source: Nursing/Academic Edition, Academic Search Complete. Iskanje literature je potekalo s pomočjo ključnih besed in njihovih kombinacij: zdravstvena nega (angl. »nursing«), informacijska tehnologija (angl. »information technology«), informacijsko komunikacijske tehnologije (angl. »information and communication technologies«), varnostna politika (angl. »security policy«) in varovanje osebnih podatkov (angl. »data protection«). Intervjuvanje je potekalo od 1. 5. do 5. 7. 2013. Vsakega intervjuvanca posebej smo preko elektronske pošte zaprosili za sodelovanje in dovoljenje za izvedbo intervjuja. Udeležba v raziskavi je bila prostovoljna. Eden od potencialnih intervjuvancev je odklonil sodelovanje, dva pa nista dala končnega odgovora. Pri intervjuvanju smo posebno pozornost posvetili izogibanju refleksivnosti (kjer izpraševalec izrazi, kar želi slišati) in ostalim pomanjkljivostim, ki so značilne za to metodo dela (Yin, 2009). Prav tako smo intervjuvance opozorili, da imajo pravico ne odgovoriti na vprašanja, če bi s tem razkrili podatke organizacije. Anonimnost intervjuvanca in organizacije, kjer je zaposlen, je bila zagotovljena.

Pred kodiranjem smo prebrali transkripte s pomočjo t. i. naivnega branja (»angl. »naïve reading«), kjer smo transkripte prebirali neobremenjeno, tako da predznanje ni predstavljalo ovire, kar omogoča identificiranje novih kategorij, ki jih sicer ne bi identificirali. Sledilo je kodiranje, ki smo ga izvedli v treh fazah (Neuman, 2006): (1) odprto kodiranje (angl. »open coding«), kjer smo identificirali t. i. preliminarne kode, katerih osnova je neobremenjeno branje in temeljit pregled literature; sledilo je (2) aksialno kodiranje (angl. »axial coding«), kjer smo skušali identificirane kategorije smiselno urediti; in nato smo v fazi (3) selektivnega kodiranja (angl. »selective coding«) transkripte natančno označili z identificiranimi kodami. V vseh treh fazah sta rezultate medsebojno usklajevala dva raziskovalca, ki sta intervjuje tudi analizirala.

3 Rezultati in razprava

V tem poglavju so predstavljene ključne izjave intervjuvancev in izsledki sorodnih študij. Izjave intervjuvancev so označene z naslednjimi oznakami: vodilne medicinske sestre (označene z oznako MS in zaporedno številko intervjuvanca/ke), vodje informatike (INF in zaporedna številka intervjuvanca/ke). Izjave vodilne medicinske sestre so označene z oznako MSINF. V nadaljevanju so po podpoglavjih predstavljene ključne teme, ki smo jih identificirali s kodiranjem teksta, pridobljenega z intervjuji: »Nezadostno znanje s področja informatike«, »Slabo poznavanje oz. nepoznavanje pojma informacijske varnosti«, in »Neobstoj formalne varnostne politike na področju informacijske varnosti«.

3.1 Nezadostno znanje s področja informatike

Staggers, Gassert in Curran so v svoji študiji identificirale kompetence s področja informatike v zdravstveni negi (Staggers in sod., 2002). Med temi so eksplicitno navedene tudi kompetence s področja informacijske varnosti. Slednje namreč sodijo na osnovni nivo potrebnih kompetenc s področja informatike v zdravstveni negi. Številne

študije so potrdile potrebo po omenjenih kompetencah (Chang in sod., 2011; McNeil in sod., 2005). Kljub številnim prizadevanjem Zbornice zdravstvene in babiške nege - Zveze strokovnih društev medicinskih sester, babic in zdravstvenih tehnikov Slovenije, potrebne kompetence medicinskih sester na področju informatike še vedno niso definirane (Poklicne aktivnosti in kompetence v zdravstveni in babiški negi, 2008). McNeil in sod. (2005) ugotavljajo, da je znanje s področja informatike v zdravstveni negi pomanjkljivo. Posledično je primanjkljaj znanja prisoten tudi na področju informacijske varnosti. Podobno mnenje imajo tudi intervjuvane vodilne medicinske sestre, kar potrjujejo tudi njihove izjave:

MS3: »Znanja je premalo, ker vidim, da bi si lahko na tem področju delo zelo poenostavili, pa si ga ne znamo.«

MS4: »Znanje je sicer različno in se razlikuje med posamezniki. Nekateri ga sicer imajo dovolj, ostali pa premalo.«

MSINF: »V šoli je premalo ur, posvečenih informatiki in kliničnemu usposabljanju na tem področju. Kot vzrok bi izpostavila še strah do neznanega in tehnologije, obremenitev na delovnem mestu in odpor pri starejših zaposlenih.«

Zanimivo je, da v odgovorih informatikov nismo zasledili izraženega pomanjkanja znanja pri medicinskih sestrah:

INF1: »Menim, da je v povprečju tega znanja dovolj, zato lahko delo na tem področju poteka normalno.«

INF3: »Znanje medicinskih sester s področja informatike bi ocenil kot zadovoljivo oziroma kot povprečno.«

Domnevamo, da je vzrok v navedenih odgovorih ta, da se informatiki v zdravstvenih ustanovah pri svojem delu srečujejo s skupinami zaposlenih, kjer je pomanjkanje znanja na tem področju še bolj pereče. Intervjuvanec dodaja:

INF3: »Vzrok (za zgolj zadovoljivo znanje, op. a.) je predvsem v osebni zainteresiranosti, ki je med posamezniki različna. Zahteve po znanju so različne glede na delovno okolje.«

S pomočjo pridobljenih odgovorov ne moremo sicer trditi, da je znanje s področja informatike velik problem pri medicinskih sestrah. Informatiki so namreč navedli, da je znanje pri tej skupini na zadovoljivem nivoju, vendar glede na to, da to znanje sodi med osnovne kompetence medicinskih sester (Staggers in sod., 2002; McNeil in sod., 2005; American Nurses Association, 2008; Chang in sod., 2011), lahko trdimo, da zgolj zadovoljivo znanje na tem področju ni dovolj. Napredek sodobnih IKT, smernice Svetovne zdravstvene organizacije in vse ostrejše zakonske določbe zahtevajo od medicinskih sester še dodatno znanje s področja informacijske varnosti.

Trije intervjuvanci so kot glavni vzrok za nezadostno znanje navedli pomanjkljive postopke izobraževanja. Vseživljenjsko učenje na področju informatike v zdravstveni negi in zdravstvu je lahko zanimiva tržna niša za ustanove, ki se ukvarjajo z izobraževanjem omenjene populacije (McNeil in sod., 2005). Rezultati študije, objavljene v monografiji »Informatics and nursing« kažejo, da je pridobivanje znanja le s pomočjo

literature in predavanj premalo (Thede, 2010). Pomembne so praktične izkušnje, razumevanje veščin in sposobnost povezovanja ter uporabe pridobljenega znanja v praksi. To pa lahko te ustanove medicinskim sestram ponudijo tudi v obliki praktičnega usposabljanja.

Zdravstvene ustanove nudijo izobraževanje po potrebi (npr. pri uvajanju novih IS, ob večjih spremembah na tem področju) in so pri tem že pregovorno finančno omejene. Nekateri intervjuvanci so navedli, da se izobraževanje izvaja le ob večjih kadrovskih spremembah ali spremembah na področju informatike:

INF1: »Problem je usklajevanje zdravstvenega kadra, ki ga je veliko … težko je uskladiti redno letno ali mesečno izobraževanje. Ob prihodu zaposlenega in novih sistemih izobraževanja naredimo, da jih soočimo z novostmi.«

MS2: »V naši organizaciji je dogovorjeno, da na določeno časovno obdobje organiziramo izobraževanje, vendar ne v smislu (informacijske, op. a.) varnosti, temveč v smislu, da bi znali pravilno uporabljati IS. Izobraževanje je sprotno, ob uvajanju novih programov.«

Le en intervjuvanec je izpostavil pomen kontinuiranega izobraževanja na področju uporabe informacijske tehnologije:

INF3: »Ustanova izobraževanje podpira, to je odvisno od potreb in sprememb (enkrat na leto oziroma enkrat na par let). Občasno izvajamo dodatno šolanje s področja informatike, predvsem ob pojavu večjih sprememb. Izobraževanje je kontinuirano.«

Zabukovec in Bohinc navajata, da so potrebe po pridobivanju dodatnega znanja s področja IS in računalništva precej izražene (Zabukovec in Bohinc, 2001). Thede in Sewel (2010, str. 16-17) v svoji monografiji uporabljata poleg uveljavljenega izraza računalniška oz. informacijska pismenost (angl. »computer literacy«) še izraz računalniško oz. informacijsko tekoče znanje (angl. »computer/information fluency«). Prvi pomeni, da posameznik pridobi osnovno znanje na tem področju, drugi pa, da se posameznik, sicer neformalno, zaveže k neprestanemu izpopolnjevanju na področju računalništva in informatike. Omenjeni avtorici poudarjata, da je slednji za sodobno zdravstveno nego ključnega pomena. Zanimivo bi bilo ugotoviti, ali je računalniška oz. informacijska »tekočnost« že ustaljena praksa slovenskih medicinskih sester. Vsekakor lahko glede na odgovore intervjuvancev sklepamo, da je izobraževanje na področju informatike izvedeno samo po potrebi, le eden intervjuvanec poroča o sprotnem izobraževanju. Glede na odgovornosti, ki jih za zaposlenega prinaša potreba po informacijsko tekočem znanju (Thede in Sewel, 2010), je izobraževanja, ki se pojavi zgolj ob večjih spremembah, definitivno premalo. Ne glede na v intervjujih ugotovljeno podporo ustanov omenjenemu izobraževanju pa lahko trdimo, da zdravstvene ustanove še vedno premalo prispevajo k poznavanju in izobraževanju zdravstvenih delavcev na področju informatike, predvsem pa na področju informacijske varnosti.

3.2 Nezavedanje pomena informacijske varnosti za pacienta

Skozi intervjuje smo zasledili večinoma enake opazke. Medicinske sestre se pri svojem delu premalo zavedajo pomena informacijske varnosti in kršitev, ki jih lahko pri svojem delu naredijo z neupoštevanjem veljavne zakonodaje. Rezultat ni presenetljiv, saj so podobno ugotovili tudi v raziskavi med podiplomskimi študenti zdravstvene nege, kjer so identificirali kompetence IKT pri medicinskih sestrah (Dixon in Newlon, 2010). Zanimivo je, da so le redke izjeme identificirale informacijsko varnost kot nujno potrebno znanje medicinskih sester pripravnic. Trček in sod. (2007) navajajo, da je glavni in najpomembnejši dejavnik za zagotavljanje informacijske varnosti človek. Intervjuvanci so izrazili različna strokovna mnenja:

MS1: »Bolj ali manj se medicinske sestre zavedajo (pomena informacijske varnosti, op. a.), vendar ne morebitnih sankcij. Verjetno je zaradi preobilice dela omenjena problematika zanemarjena.«

MS2: »Ko začneš delati, se ne zavedaš pomena informacijske varnosti za pacienta. Nato se z leti to znanje in zavedanje oplemeniti. Menim, da se zavedajo pojma informacijske varnosti, ne poznajo pa varnostne politike. Predvsem se zavedajo, da obstaja velik problem na področju varovanja podatkov ... ne bi pa trdila, da se zavedajo vseh posledic, ki jih prinaša kršenje zakonov s tega področja.«

MSINF: »Se premalo zavedajo problematike informacijske varnosti. Vedo, kaj pomeni izdajanje informacij, ne vedo pa, kako lahko nekdo zlorabi IS.«

INF3: »Mislim, da se le delno zavedajo tega pojma, glede na to, da jih stalno opozarjamo. Razlog je predvsem preobremenjenost z delom. Če pa se že zavedajo tega pojma, nimajo dovolj časa, da bi temu posvetile več pozornosti.«

Iz izjav intervjuvancev smo identificirali nezadostno zavedanje o pomenu informacijske varnosti. Green in Rubin (2011) opozarjata na probleme informacijske varnosti pri uvedbi elektronskega zdravstvenega zapisa. Kot primer izpostavljata identifikacijo, uporabo enkripcijskih ključev itn. Uporaba elektronskega podpisa, enkripcijskih ključev in ostalih tehnologij za zagotavljanje informacijske varnosti ne zadostujejo, če zaposleni ne poznajo oz. se ne zavedajo pomena informacijske varnosti in se skladno s tem tudi ravnajo. Albarrak (2012) v svoji študiji opozarja, da se medicinske sestre zavedajo problematike informacijske varnosti, a kljub temu njihove navade na tem področju predstavljajo resno grožnjo za varnost in zaupnost pacientovih osebnih podatkov. Omenjena študija kaže na veliko razliko med zavedanjem in dejanskim vedenjem medicinskih sester. Žal pa pri pregledu literature nismo zasledili podobnih študij tudi v drugih državah. Podobno problematiko smo identificirali tudi v izjavah informatikov:

INF1: »Iz zgodovine naše ustanove lahko sklepam, da zavedanje o informacijski varnosti ni na visokem nivoju, saj smo velikokrat naleteli na posojanje gesel, medsebojno zaklepanje računov, celo gesla zalepljena na monitorjih.«

INF2: »Mislim, da se ne zavedajo. Večkrat opazimo vse dokumente po mizah, so razpršeni in na nek način v nevarnosti. Premalo se zavedajo, da na ta način kršijo Zakon o varovanju osebnih podatkov.«

Skladno z navedenimi izjavami lahko trdimo, da je nezadostno poznavanje pojma varnostne politike očitno prisotno pri medicinskih sestrah. Domnevamo, da omenjeno problematiko sicer poznajo, vendar, glede na izjave intervjuvanih informatikov, njihovo ravnanje ni povsem skladno z znanjem, ki ga imajo. Slednje pa je ugotovil tudi Albarrak (2012).

Glede na zgoraj navedena dejanja lahko trdimo, da se pri medicinski sestrah pojavlja nezavedanje o pomenu informacijske varnosti za pacienta. Informacijska varnost je namreč proces, ki se v neki instituciji lahko razvije le postopoma (IT Governance Institute, 2007). Izobraževanje zaposlenih skozi delo in ne njihovo sankcioniranje so očitno pogosto uporabljen pristop, kar kažejo naslednje izjave:

MS1: »Vedno več medicinskih sester ob zaključenem delu izklopi računalnik oziroma opravi odjavo iz IS. Pri vsakem ugotovljenem odstopanju odreagiramo vzgojno tako, da poskušamo zaposlene osvestit, zakaj je potrebno varovati podatke.«

MS4: »Ne pomnim, da bi v naši ustanovi prišlo do hujših kršitev. Posameznike smo večkrat zgolj opozarjali.«

Zanimiva pa so tudi mnenja o vplivu izobrazbe na tako stanje:

MS2: »Vzrok za nezavedanje (omenjene problematike, op. a.) pa je gotovo v formalni izobrazbi, kjer ni bilo narejeno dovolj oziroma o takih stvareh sploh niso govorili.«

MS4: »Menim, da se diplomirane medicinske sestre bolj zavedajo posledic kršitev in sankcij kot zdravstveni tehniki.«

INF1: »Se ne zavedajo prav veliko (P2+) … v šoli niso dovolj podrobno obravnavali tega področja.«

3.3 Neobstoj formalne varnostne politike na področju informacijske varnosti

Prav tako smo ugotovili, da v vseh treh ustanovah, po navedbah informatikov, ni formalno zapisane varnostne politike na področju informatike. Varnostna politika pa je pomemben element informacijskega sistema (IT Governance institute, 2007). Le v enem primeru smo zasledili, da je le (sicer pomemben) del varnostne politike zapisan:

INF3: »Varnostna politika je formalno zapisana. Zajema varovanje osebnih podatkov na nivoju hrambe podatkov (kako se hranijo podatki in kako se arhivirajo), kako se določa uporabniška imena in gesla, dostopne pravice, pravila o ustrezni nameščenosti opreme na delovnih mestih (slednje pa še zdaleč ni celotna varnostna politika, op. a.).«

V enem primeru, kjer sta bila informatik in medicinska sestra iz iste ustanove, smo celo ugotovili, da so si odgovori informatika in medicinske sestre protislovni. Na vprašanje, ali imate varnostno politiko na področju informacijske varnosti in ali je slednja formalno zapisana in kaj zajema, so se pojavili nasprotujoči si odgovori. Slednje očitno nakazuje na napačno razumevanje pojma varnostna politika informacijskega sistema:

MS1: »Varnostno politiko IS imamo. Zadeva je še v razvoju, se spreminja in prilagaja. S pomočjo internih aktov in podatkov pripravljamo stvari, da bodo transparentne, jasne in enostavno pregledne za vsakega, tudi za nekoga, ki bo na novo prišel. Vsak uporabnik dobi svoje geslo in je tudi obveščen oziroma opozorjen, da je to geslo samo njegovo.«

INF1: »Varnostne politike IS v naši ustanovi nimamo. Pravna služba bi vedela, kaj je tisto oziroma kakšne so vsebine v pogodbah, s katerimi se ustanova ščiti. Vsebin prav veliko ni, ker je osnova za to varnostna politika. Tisti podatki, ki so v elektronski obliki, so definitivno zavarovani z vsaj eno prijavo in tudi z večstopenjsko prijavo. Podatki v pisni obliki so varovani drugače, v arhivih, in so dovolj dobro varovani.«

4 Zaključek

Rezultati pričujoče študije kažejo, da so pri delu medicinskih sester očitno prisotni elementi, ki lahko povečajo verjetnost kršitve informacijske varnosti, in sicer: »nezadostno znanje medicinskih sester s področja informatike«, »slabo poznavanje oz. nepoznavanje pomena informacijske varnosti«, in »neobstoj formalne varnostne politike na področju informacijske varnosti«. Velik identificiran problem je nepoznavanje informacijske varnosti oz. nezavedanje o možnih sankcijah, ki so lahko posledica kršenja veljavne zakonodaje.

Ali bi formalna varnostne politike v zdravstvene ustanove rešila identificirane probleme, ni znano. Dejstvo je, da imajo medicinske sestre vse manj časa za delo s pacienti predvsem zaradi administrativnih opravil. Nevarnost pa je, da bi oblikovana varnostna politika pomenila samo še dodatno breme in s tem dodatno administrativno delo. Slednjemu pa se lahko zdravstveni sistem izogne s formalno uvedbo varnostne politike v vse zdravstvene ustanove, na vseh ravneh zdravstvenega varstva tako, da zdravstvene delavce čim manj obremeni. Vsekakor je ob dodatni obremenitvi zaposlenih treba razmišljati tudi o zadostitvi kadrovskih normativov, ki jih predvideva stroka, saj le tako lahko zagotovimo učinkovito in varno delovanje vseh procesov (tako strokovnih kot informacijskih). Zato je smiselna integracija informacijskega znanja, ki bo dopolnila in oplemenitila strokovno znanje medicinskih sester in omogočila kakovostnejšo obravnavo pacienta. Poudariti moramo, da je treba v izobraževanje s področja informatike nujno uvesti poglavja o informacijski varnosti, saj poklicna molčečnost kot načelo iz Kodeksa etike velja za vse poklicne skupine v zdravstvu. Danes, v dobi informacijske tehnologije, se zaposleni premalo zavedajo potencialnih nevarnosti, ki jih prinašajo elektronske baze podatkov.

Raziskavo smo izvedli z intervjuvanci iz šestih zdravstvenih ustanov primarnega, sekundarnega in terciarnega zdravstvenega varstva. Ker gre za mnenja zaposlenih v zdravstvenih ustanovah iz vse Slovenije, bi lahko podobne rezultate pričakovali tudi drugod. Poudariti pa moramo, da je ugotovitve pričujoče študije težko posplošiti na celotno populacijo slovenskih medicinskih sester. Vseeno pa identificirane teme nakazujejo na alarmantno stanje na področju informacijske varnosti, zato bi bilo gotovo

smiselno preveriti stanje v celotni Sloveniji in širše, predvsem v času, ko se postopoma implementira projekt e-zdravje.

Informacijski varnosti v zdravstvu bomo morali v bodoče posvetiti posebno pozornost, saj uporaba IKT postaja oz. je pomembna kompetenca medicinskih sester, in brez ustreznega znanja na tem področju je lahko tempirana bomba v procesu zaščite pravic in interesov pacientov. Tako kot so medicinske sestre oblikovale kompetence na ožjih strokovnih področjih delovanja, bi bilo morda smiselno oblikovati dokument, ki bi določal kompetence na področju informatike, s poudarkom na informacijski varnosti.

Samanta Mikuletič, Tamara Štemberger Kolnik, MSc, Boštjan Žvanut, PhD

Patient's Information Privacy and Data Protection

Information and communication technologies have become an integral part of everyday life. Their development has substantially changed nurses' work processes and working environment. The World Health Organization (2005) in the resolution on e-health, named WHA58.28, reminds the member states to focus their healthcare workers on acquiring the appropriate information, including communication technologies knowledge and competences.

Nurses represent the largest group of healthcare workers. American Nurses Association and several other organizations emphasize the importance of information and communication technologies competences for this population. Dewsbury (2011) argues that nurses should not just be passive users of these technologies, but should take an active role in this field. However, the available information systems in Slovenia provide only some of the information required for the nursing process.

The rapid development of information and communication technologies and their implementation in healthcare led to different ethical and legal dilemmas. Nurses take different responsibilities that cannot be defined only by laws and regulations (e.g. Personal Data Protection Act). In addition, nurses are obliged to comply with the Code of Ethics for nurses, where, for example, the 3rd principle specifies that nurses should protect and respect the patients' data privacy. The right to privacy is a constitutional right of the Republic of Slovenia and other democratic countries and is one of the indispensable elements of human existence.

Information resources can be endangered by different accidents and computer crime (i.e. any use of the information system for unlawful acts: theft, sabotage, and vandalism). The accidents include damage to computer equipment, its inadequate technical characteristics, employees' irresponsibility, errors in programs and data, hardware failures and mismanagement. For a long time, it has been clear that the technology itself is not sufficient for the proper information security. All authorised information system users could potentially jeopardize the privacy of personal patients'

data. Nurses as primary users of the information systems also have access to personal patient data for which they are authorised. Often nurses and other healthcare workers access the data as secondary users by using other users' credentials. This increases the probability of data privacy violation or access of unauthorized users. Furthermore, the organization processes in healthcare institutions could represent a threat of violating the information system security. For example, very often only one member of the healthcare team is logged in the information system, when all other members have the possibility to access the patients' data, for which they are not authorized. To ensure adequate security in modern information systems, the human behaviour should be carefully addressed in addition to technology. The information security has become an increasing challenge as information systems are rapidly evolving and becoming more complex and diverse. The information system security policy provides a comprehensive view of information system security; it includes a number of elements, including organizational rules and procedures for effective and safe use of information systems. It does not guarantee a better protection of information systems if these rules and procedures are not manifested in the users' behaviour. An organization, which wants to establish a desired level of information security in its own environment, has to establish the appropriate procedures for information security management as well. Maintaining an adequate level of information security is an endless process, since the number of threats is constantly increasing.

In practice, it is impossible to protect organizations against all information security risks. In larger organizations, a steering committee for information security must be implemented, being responsible for information security strategies and policies development. For that matter, a Chief Information Security Officer (CISO) may be appointed by the management. According to some authors, a Chief Information Security Officer should be employed in healthcare organisations full-time, as all health care providers cope with larger or smaller information security incidents (e.g. loss of a laptop with patients' data, computer virus, and phishing). To respond to such security breaches, organizations have to develop the response plan for information security breaches, which defines different types of information security incidents. Furthermore, organisations should work closely with legal counselling in formulating plans to ensure the information security.

In healthcare practice, there is a considerable risk of information security violation of patient's data. For example, Albarrak (2012) reports on a number of potentially dangerous acts regarding the violation of information security. Results of the literature review indicate an extremely bad situation in this field. Moreover, no available relevant reference was identified, which examines the aforementioned problem in Slovenian context. Accordingly, the following research question was defined: »Which elements, that may potentially increase the likelihood of information security violation, are present in nursing practice in Slovenia? Furthermore, the aim of this study was to identify the reasons for such a risky situation.

Initially, a systematic literature review that included a variety of scientific and professional articles, monographs and websites was performed. Search was condu-

cted by examining the online services: »COBISS«, »Google Scholar«, »Science Direct«, »EBSCO host«, »Wiley Online Library«, PubMed, Medline, CINAHL, Health Source: Nursing / Academic Edition, Academic Search Complete. The literature search was conducted by using the following key words and their combinations: nursing, information technology, information and communication technologies, security policy and data protection.

The qualitative study was performed between May and June 2013. Experts in the field of nursing and informatics in nursing from primary, secondary, and tertiary levels of healthcare were interviewed (4 nursing managers, 3 IT managers and one expert in both fields).

Modern research methodology suggests the use of open-ended interviews. In the aforementioned interview type, the interviewers usually use question guides with open-ended questions that could be changed during the interview, allowing a flexible and open flow of the interview, if required. Accordingly, the interviews were conducted using a question guide with four open-ended questions (presented in the article in Table 1), developed for the needs of the present study. The bases for the questions were the findings of similar studies identified in the literature review.

The interview invitations were sent by e-mail, the participation in the study was voluntary. Initially, the interviews were performed with one expert in IT and nursing and two IT managers. The number of interviewees was increased gradually until the sample saturation was reached (i.e. no new relevant information was identified). One of the potential interviewees refused to cooperate, and two did not give their final response. During the interviews, particular attention was paid to avoid reflexivity and other problems that are typical for the interview. The interviewees could refuse answering the questions if the responses revealed the details of the organization. The anonymity of both the interviewee and the organization were granted. In order to avoid misunderstanding, the interviews were recorded, except in one case when the interviewee did not allow the recording. After each interview a transcript was made (except in the aforementioned case, the interview notes were used instead of the transcript).

Before the coding process, the "naïve reading" of the transcripts was performed, which allowed the identification of new categories, not identified in the literature. This was followed by the coding, which was carried out in three phases: (1) open coding, where the preliminary codes were identified; followed by (2) the axial coding, where final categories were identified, merged etc., and finally (3) selective coding, where transcripts were accurately labelled with the final set of codes. The coding process was performed by two researches in each phase. The coding results were compared and discussed. The following themes were identified from the transcripts: "Insufficient knowledge in the field of informatics," "Unfamiliarity with the information security concept", and "The absence of a formal security policy in the field of information security". A major problem identified in our study is the unawareness of possible sanctions that may result from violation of applicable laws related to the field of information security. Our study indicates that nurses are not aware of the importance of information security, its relevance for the patients, and the lack of knowledge in this field.

Hence, there is no adequate level of responsibility for patients' data. Similar results can be expected in the whole country, as our sample included all levels of healthcare and some important actors in the process of nursing informatisation in Slovenia.

Our findings indicate an alarming situation in the field of nursing informatics and healthcare informatics in Slovenia, which is consistent with studies performed in other countries. Special attention should be put to this problem immediately, as it represents a time bomb in the process of protecting the patients' rights and interests. Based on our findings, a warning mechanism for protecting the patients' data privacy should be established. Moreover, the awareness of health workers responsibility for these data should be raised. It is not known, whether the introduction of a formal security policy in healthcare institutions would solve the identified problems. In fact, due to their administrative tasks, nurses have less time to work with patients. The potential danger is that the introduction of formal security policy will manifest as an additional administrative work, i.e. bureaucracy. In order to avoid this situation, the introduction of a formal security policy in all health institutions at all levels should be carefully performed. Special attention should be paid to the integration of required information knowledge and skills that will refine the nurses' and other healthcare workers' expertise, improving the information security and, hence, the quality of healthcare. Therefore, special attention should be put to the education of nurses and other healthcare workers in the field of information and communication technologies, especially in the field of information security, especially to the appropriate presentations of potential hazards posed by the use of electronic health records.

The research was conducted with interviewees from six health institutions of primary, secondary and tertiary healthcare systems. Since we were analysing opinions of employees in healthcare institutions from all over Slovenia, we could expect similar results elsewhere. However, the findings of this study are difficult to generalize to the entire population of Slovenian nurses. Besides, the identified problems indicate an alarming situation in the field of information security. So it would certainly be reasonable to examine this situation in detail in Slovenia and other countries as well. Information security in healthcare will certainly require special attention, since the competence of use of information and communication technologies is becoming more and more important for nurses. Consequently, it might be appropriate to create a document that would define the competences in the field of information and communication technologies with an emphasis on information security.

LITERATURA

1. Albarrak, A. (2012). Information security behavior among nurses in an academic hospital. HealthMED, 6, št. 7, str. 2349–2354.
2. American Nurses Association. (2008). Scope and standards of nursing informatics practice. 2nd ed. American Nurses Publishing.
3. Brezavšček, A. in Moškon, S. (2010). Vzpostavitev sistema za upravljanje informacijske varnosti v organizaciji. Uporabna informatika, 2, št. 18, str. 101–108.

4. Cartlidge, A., Hanna, A., Rudd, C., Macfarlane, I.and Windebank, J. (2007). An introductory overview of ITIL® V3. Norwich: The UK Chapter of the itSMF.
5. Chang, J., Poynton, M. R., Gassert, C. A. and Staggers, N. (2011). Nursing informatics competencies required of nurses in Taiwan. International journal of medical informatics, 80, št. 5, str. 332–340.
6. Dimitropoulos, L., Patel, V., Scheffler, S. A. and Posnack, S. (2011). Public attitudes toward health information exchange: perceived benefits and concerns. American Journal of Managed Care, 17, št. 12, Spec. No., str. 111–116.
7. Dixon, B. E. and Newlon, C. M. (2010). How do future nursing educators perceive informatics? Advancing the nursing informatics agenda through dialogue. Journal of Professional Nursing, 26, št. 2, str. 82–89.
8. Fetter, M. S. (2009). Baccalaureate nursing students' information technology competence — agency perspectives. J Prof Nurs 25, 42–49.
9. Glaser, J. and Aske, J. (2010). Healthcare IT trends raise bar for information security. Healthcare Financial Management, 64, št. 7, str. 40–44.
10. Gradišar, M. (2003). Uvod v informatiko. Ljubljana: Ekonomska fakulteta.
11. Green, M. D. and Rubin, A. D. (2011). A research roadmap for healthcare IT security inspired by the PCAST health information technology report. V: Proceedings of the 2nd USENIX Conference on Health Security and Privacy. USENIX Association, San Francisco, CA, str. 5–5.
12. Informacijski pooblaščenec Republike Slovenije, n. d. Evropske smernice za zdravstvene delavce o zaupnosti in zasebnosti v zdravstvu. Pridobljeno dne 10. 11. 2014 s svetovnega spleta: https://www.ip-rs.si/fileadmin/user_upload/Pdf/Evropske_smernice_za_zdravstvene.pdf.
13. ISO (n.d.). ISO/IEC 27000:2009 - Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary. Pridobljeno dne 12. 8. 2013 s svetovnega spleta: http://www.iso.org/iso/catalogue_detail?csnumber=41933.
14. IT Governance Institute (2007). COBIT. Rolling Meadows, IL: IT Governance Institute.
15. Ivanko, Š. (2007). Raziskovanje in pisanje del: metodologija in tehnologija raziskovanja in pisanja strokovnih in znanstvenih del. Kamnik: Cubus image.
16. Kodeks etike medicinskih sester in zdravstvenih tehnikov Slovenije – 2005 (2010). Uradni list Republike Slovenije, št. 40.
17. Lampe, R. (2004). Sistem pravice do zasebnosti. Ljubljana: Bonex.
18. McNeil, B. J., Elfrink, V. L., Pierce, S. T., Beyea, S. C., Bickford, C. J. and Averill, C. (2005). Nursing informatics knowledge and competencies: a national survey of nursing education programs in the United States. International Journal of Medical Informatics, 74, št. 11-12, str. 1021–1030.
19. Ministrstvo za zdravje, n. d. Sistem za upravljanje z informacijsko varnostjo - SUVI Pridobljeno dne 11. 12. 2014 s svetovnega spleta: http://www.ezdrav.si/?page_id=158.
20. Neame, R. (2008). Privacy and health information: health cards offer a workable solution. Informatics in Primarycare, 16, št. 4, str. 263–270.
21. Neuman, W. L. (2006). Social research methods: qualitative and quantitative approaches. Boston: Pearson.
22. Polito, J. M. (2012). Ethical considerations in internet use of electronic protected health information. Neurodiagnostic Journal, 52, št. 1, str. 34–41.
23. Prijatelj, V., Dornik, E., Rajkovič, U. in Žvanut, B. (2011). Razvoj informatike v zdravstveni negi v Sloveniji. Ljubljana: Slovensko društvo za medicinsko informatiko, Sekcija za informatiko v zdravstveni negi.
24. Staggers, N., Gassert, C.A. and Curran, C. (2002). A Delphi study to determine informatics competencies for nurses at four levels of practice. Nursing Research, 51, št. 6, str. 383–390.
25. Svetovna zdravstvena organizacija (2005). WHA58/2005/REC/1. Ženeva: Svetovna zdravstvena organizacija.
26. Štrakl, M. (2003). Varnostna politika informacijskega sistema. Pridobljeno dne 12. 12. 2014 s svetovnega spleta: http://lms.uni-mb.si/vitel/14delavnica/.
27. Thede, L.Q. and Sewel, J.P. (2010). Informatics and nursing: competencies & applications, 3rd ed. Philadelphia: Wolters Kluwer.

28. Trček, D., Trobec, R., Pavešić, N. and Tasič, J. F. (2007). Information systems security and human behaviour. Behaviour & Information Technology, 26, št. 1, str. 113–118.
29. Ustava Republike Slovenije (1991). Uradni list Republike Slovenije št. 33.
30. While, A. and Dewsbury, G. (2011). Nursing and information and communication technology (ICT): a discussion of trends and future directions. International Journal of Nursing Studies , 48, 1302–1310.
31. Yin, R. K. (2009). Case study research: design and methods. Los Angeles, CA: Sage Publications.
32. Zabukovec, M. in Bohinc, M. (2001). Mesto informacijskega sistema v zdravstveni negi. Obzornik zdravstvene nege, 35, št. 1/2, str. 56–65.
33. Zakon o pacientovih pravicah (2008). Uradni list Republike Slovenije, št. 15.
34. Zakon o varstvu osebnih podatkov (2004). Uradni list Republike Slovenije št. 86.
35. Železnik, D., Brložnik, M., Buček Hajdarević, I., Dolinšek, M., Filej, B., Istenič, B. in sod. (2008). Poklicne aktivnosti in kompetence v zdravstveni in babiški negi. Ljubljana: Zbornica zdravstvene in babiške nege – Zveza strokovnih društev medicinskih sester, babic in zdravstvenih tehnikov Slovenije.

Samanta Mikuletič, študentka 2. stopnje Fakultete za vede o zdravju, Univerze na Primorskem.
E-naslov: samanta.mikuletic@gmail.com

Mag. Tamara Štemberger Kolnik, višja predavateljica na Fakulteti za vede o zdravju, Univerza na Primorskem.
E-naslov: tamara.kolnik@fvz.upr.si

Dr. Boštjan Žvanut, docent na Fakulteti za vede o zdravju, Univerza na Primorskem.
E-naslov: bostjan.zvanut@fvz.upr.si