Strokovni članek ■

Varnost osebnih podatkov v (tele)medicini

Jure Lihtenvalner, Uroš Flerin, Dejan Dinevski

Izvleček. Problematika varovanja osebnih podatkov v vsakdanjem življenju postaja vedno bolj pereča. V okviru medicine je ta problematika izrazito prisotna predvsem na področju varovanja bolnikovih osebnih podatkov, zaščite pred zlonamerno programsko opremo in zastojev procesa ob izpadu informacijskega sistema. Varovanje osebnih podatkov (v medicini) se v Sloveniji izvaja v skladu z Zakonom o varstvu osebnih podatkov, pri čemer je zagotavljanje sledljivosti vpogleda in spreminjanja osebnih ter zdravstvenih podatkov v informacijskih sistemih zdravstvenih ustanov zagotovo ena najpomembnejših kategorij varovanja. Razvoj medicine je ambivalenten: medtem ko mora nujno zagotavljati zasebnost in najvišje standarde za pacientovo varnost, je hkrati dolžan stremeti k čim bolj ekonomični in smotrni oskrbi pacientov.

Personal Data Protection in (Tele)Medicine

Abstract. Protection of personal data is becoming more and more problematic in everyday life. In medicine, it is especially important when it comes to the protection of patients' information and protection against malicious software and delays due to information system failures. Personal data protection (in medicine) is implemented in Slovenia in accordance with the Personal Data Protection Act, whereby the provision of tracing access and changes to personal and medical data in health care information systems is one of the key issues. Medicine must meet two often conflicting goals: ensuring privacy and the highest standard of patient safety, and developing more economical and efficient standard of care.

■ **Infor Med Slov**: 2014; 19(1-2): 29-43

Institucija avtorjev / Author's institution: Medicinska fakulteta, Univerza v Mariboru.

Kontaktna oseba / Contact person: Dejan Dinevski, Medicinska fakulteta, Univerza v Mariboru, Taborska ul. 8, 2000 Maribor. e-pošta / e-mail: dejan.dinevski@um.si.

Prejeto / Received: 12.05.2014. Sprejeto / Accepted: 25.10.2014.

Uvod

Telemedicino lahko definiramo kot zagotavljanje zdravstvenih storitev z uporabo informacijskih in telekomunikacijskih tehnologij v primerih, ko sta izvajalec zdravstvene storitve in pacient, oziroma dva izvajalca zdravstvene storitve, prostorsko ločena.[1,2] Z uveljavljanjem telemedicine postaja problematika varovanja osebnih podatkov, zaščita pred zlonamerno programsko opremo in preprečevanje zastoja procesa ob izpadu informacijskega sistema zelo pomembna. Trenutno je stanje varovanja informacij, ki se v zdravstvu zbirajo, hranijo in izmenjujejo, neustrezno glede na pomembnost tega vprašanja.

Ministrstvo za zdravje daje v strateškem dokumentu eZdravje 2010[1] močan poudarek zagotavljanju varovanja pacientovih podatkov. V Sloveniji načrtujemo uvedbo elektronske zdravstvene kartoteke pacienta ter elektronsko izmenjavo podatkov med zdravstvenimi organizacijami. Cilj je ustvariti povezan nacionalni informacijski zdravstveni sistem, ki bo omogočal varno izmenjavo osebnih podatkov med posameznimi zdravstvenimi organizacijami.[1]

Tudi Evropska komisija je sprejela e-Health Action Plan 2012-2020, ki v ospredje postavlja izboljšanje zdravstvenega sistema, večji vpliv pacientov na stroške zdravljenja in zmanjševanje stroškov.[3]

Eden od ciljev Evropske Unije je izmenjava podatkov na evropskem nivoju. Tudi Republika Slovenija bo tako morala izpopolniti zajemanje, hranjenje in posredovanje podatkov ter vse evropske varnostne zahteve.[1]

Tehnološki vidik

Prenos medicinskih podatkov preko računalniških omrežij je, tako kot po vseh računalniških omrežjih, izpostavljen računalniškim napadom ter programskim in strojnim napakam. Zaradi tega je ogrožena zasebnost, celovitost in razpoložljivost pacientovih podatkov v elektronski obliki. Pacientova elektronska kartoteka vsebuje občutljive podatke, zato ne sme biti dostopna nepooblaščenim osebam. Kljub temu pa mora biti vedno na voljo pooblaščenim osebam.[4]

Zaupnost je najosnovnejša funkcija varnosti, ki zagotavlja, da je informacija razkrita samo pooblaščenim posameznikom po ustrezni identifikaciji in avtentikaciji, ter da je posamezniku na voljo le tak obseg informacij, kot je potreben za njegovo delo.

Celovitost pomeni, da se točnost informacij ne sme izgubiti pri elektronskem prenosu in uporabi. Informacijski sistem mora preprečevati nepooblaščeno spreminjanje podatkov in zagotavljati evidentiranje vseh sprememb.

Razpoložljivost je zahteva po tem, da so pacientovi podatki na voljo vedno – tudi v izjemnih primerih, kot je na primer nenadni izpad električnega omrežja ali ob odpovedih strojne ali programske opreme.

Nevarnost napadov na prenos medicinskih podatkov preko računalniških omrežij

Zaradi občutljivosti podatkov v elektronskih kartotekah so pacienti zaskrbljeni za svojo zasebnost. Primer hude kršitve zasebnosti je bila npr. javna objava seznama bolnikov z aidsom, ki se je zgodila v ZDA. Po drugi strani pa je točnost in aktualnost pacientovih podatkov potrebna v mreži vseh zdravstvenih oddelkov in ustanov, da bi bila zagotovljena kar najustreznejša obravnava bolnika. Vsaka pomanjkljivost podatkov ima lahko resne posledice in ali celo povzroči smrt pacienta.

Z novimi trendi, ki olajšujejo dostop do podatkov (npr. brezžična omrežja), se problemi pri zagotavljanju varnosti samo še stopnjujejo. Zaradi tega je pri uporabi telemedicine ključnega pomena preverjanje stanja varnosti omrežij in analiza varnostnih tveganj.[4]

Kategorije groženj za varnost podatkov in zasebnost

Glede na to, kako napadi ovirajo normalen tok podatkov, jih lahko razvrstimo v štiri kategorije:[4]

- Prekinitev delovanja je napad na razpoložljivost informacij ali njihovo uničenje.
- Prestrezanje je napad na zasebnost, npr. če je nepooblaščena oseba dobila dostop do informacij.
- Spreminjanje je napad na celovitost (integriteto) informacije. Nepooblaščena oseba v tem primeru nima samo dostopa do informacij, ampak jih lahko tudi nepooblaščeno spreminja.
- Ponarejanje je napad na avtentičnost (verodostojnost) informacije. Nepooblaščena tretja oseba dodaja izmišljene informacije.

V okviru prenosa medicinskih podatkov preko računalniških omrežij poznamo aktivne in pasivne napade, ki ogrožajo varnost in zasebnost podatkov.

Aktivni napadi vključujejo spreminjanje in potvarjanje pacientovih podatkov ter onemogočanje dostopa do njih. Ločimo tri vrste teh napadov.

- Maskiranje: tak napad lahko vpliva na zasebnost in celovitost informacije. V tem primeru se napadalec predstavlja sistemu kot nekdo drug.
- Spreminjanje sporočil: je primer, ko je del legitimnega sporočila spremenjen ali je sporočilo zadržano in reproducirano kasneje, s čimer je dosežen neavtoriziran učinek.
- Odpoved storitve: tak napad vpliva na razpoložljivost informacije. Napadalec preobremeni procesorske ali pomnilniške vire, tako da sistem prične zavračati legitimne zahteve in zavrača legitimne komunikacijske in upravljavske zmožnosti sistema.

Pasivni napadi vključujejo prestrezanje informacij (prisluškovanje, govornim in podatkovnim komunikacijam), ne pa njihovo spreminjanje. Pasivni napadi vodijo v razkrivanje informacij brez vednosti legitimnih uporabnikov. Pasivne napade delimo v dve kategoriji:

- Izdaja vsebine sporočila: možen je dostop do telefonskega pogovora, sporočila e-pošte ali prenos pacientovih podatkov brez vpliva na samo sporočilo.
- Analiza informacijskega prometa: nepooblaščena oseba spremlja dohodni in odhodni podatkovni promet v medicinsko omrežje z namenom ugotavljanja narave komunikacije.

Ukrepi za zagotavljanje varnosti ob prenosu medicinskih podatkov preko računalniških omrežij

Varnost podatkov zagotavljamo z mnogo ukrepi. Mednje sodijo:

- redno shranjevanje podatkov in izdelava varnostnih kopij,
- decentralizirano hranjenje podatkov,
- varovani podatkovni centri,
- jasno definirane kategorije dostopov (medicinska sestra, zdravnik, upravljalec omrežja in sistemov ipd.),
- izobraževanja za zaposlene,
- restriktivne sistemske nastavitve na požarni pregradi med zunanjim in notranjim omrežjem,
- vzpostavljeni sistemi za zaznavanje vdorov v omrežje,
- vzpostavljen sistem za nadzor podatkovne infrastrukture,

- ažurna protivirusna zaščita,
- učinkovita uporaba varnostnih ključev,
- predpisana kompleksnost in veljavnost gesel,
- beleženje prijav na sistem in nadzorovanje le-teh,
- varovanje pred fizičnim dostopom do opreme,
- negovanje varnostne kulture med zaposlenimi.

Ker je sistem varen le toliko, kot je varen njegov najšibkejši člen, je potrebno periodično preverjati ranljivost omrežja in redno izdelati varnostno oceno. Občasne varnostne presoje je potrebno izvajati po vseh oddelkih zdravstvenih organizacij. Izvajajo jih odgovorni za varnost (notranje presoje) in tudi neodvisne zunanje institucije.[4]

Računalništvo v oblaku

Temelj računalništva v oblaku je virtualizacija računalniške strojne opreme, to je oblikovanje navideznih računalnikov. Tehnologija navideznih računalnikov (ang. *virtual machine*) omogoča, da definiramo računalnik poljubne kapacitete in zmogljivosti neodvisno od dejanske stojne (strežniške) opreme. Na ta način je mogoče fizični računalniški strežnik razdeliti na več manjših, med seboj neodvisnih navideznih računalnikov ali več fizičnih strežnikov združiti v en sam, super-zmogljiv računalnik. Virtualni računalnik lahko sproti prilagajamo (dodajamo/odvzemamo pomnilnik, procesorsko moč, prostor na trdem disku, mrežne vmesnike ipd.) trenutnim potrebam glede aplikativne programske opreme, kot je npr. program za podporo procesom v zdravstvu.[5,6]

Prednosti take tehnologije se izrazito pokažejo šele, če računalniško opremo skoncentriramo na enem mestu – v podatkovnem centru. Več strežnikov zagotavlja večjo elastičnost pri oblikovanju navideznih računalnikov in podvojeno, visoko-razpoložljivo delovanje. Investicija v spremljajočo opremo, kot je podvojeno električno napajanje, podvojena klimatska naprava, sistem za samodejno gašenje ter rezervni deli, je bolj optimalna. Relativno manjši so tudi stroški vzdrževalnega osebja, ki izvaja postopke izdelave varnostnih kopij podatkov, posodobitve programske opreme, odpravo napak ter dežurstva in fizično varovanje. Podatkovni centri so lahko razdeljeni na dve ali več geografskih lokacij, s čimer se zagotavlja visoko razpoložljivo delovanje storitev v primeru naravnih katastrof.[5]

Abstrakcija infrastrukture, platforme in storitev v računalniškem oblaku omogoča različne oblike poslovnega sodelovanja med ponudnikom računalniškega oblaka in uporabnikom oziroma organizacijo. V računalniškem oblaku so podprte naslednje storitve:[5]

- Infrastruktura kot storitev (angl. *Infrastructure as a Service - IaaS*) je oddaja prostora v podatkovnem centru, kapacitet omrežja in fizičnih strežnikov. Pri takšnem modelu bi npr. zdravstvena ustanova pri ponudniku oblaka najela opremo v podatkovnem centru, kamor bi namestila lastno programsko opremo.
- Platforma kot storitev (angl. *Platform as a Service – PaaS*) je oddaja platformske programske opreme in računalniških kapacitet, ki zagotavljajo okolje za razvoj aplikativne programske opreme. Pri tem modelu bi zdravstvena ustanova za razvoj lastne programske opreme uporabila najeto platformo v zunanjem podatkovnem centru.
- Programska opremo kot storitev (angl. *Software as a Service – SaaS*) je oddaja aplikativne programske opreme. V tem primeru zdravstvena ustanova ne bi investirala v lastno programsko opremo, ampak bi jo najemala kot storitev. Glede na unikatnost procesov in pripadajoče aplikativne programske opreme je v zdravstvu to malo verjeten scenarij.

Poleg tehnoloških možnosti in možnosti za različne poslovne modele (različno razmerje med najemom in lastništvom) pa je potrebno upoštevati tudi zakonske obveze o varovanju zasebnih podatkov in poslovnih informacij.

Informacijski pooblaščenec v splošnem glede storitev računalništva v oblaku meni, da:[7]

- morajo biti vloženi nadaljnji napori v raziskave, standardizacijske in certifikacijske sheme in prilagoditve zakonodajnega in regulativnega okvira za dvig stopnje zaupanja v storitve računalništva v oblaku;
- morajo upravljavci osebnih podatkov pred uporabo storitev računalništva v oblaku izvajati potrebne analize tveganja in presoje vplivov na zasebnost, po potrebi s pomočjo zaupanja vrednih tretjih strank;
- morajo ponudniki storitev računalništva v oblaku zagotoviti večjo transparentnost svojih praks, predvsem pa zagotovil s področja informacijske varnosti;
- morajo nadzorni organi na področju varstva osebnih podatkov in zasebnosti nadaljevati z oblikovanjem smernic in nudenjem strokovne pomoči deležnikom glede vprašanj varstva osebnih podatkov in zasebnosti.

Pomembno nevarnost uporabe storitev v oblaku predstavlja preveliko zaupanje ponudniku oblaka. Tudi profesionalno usposobljeno osebje včasih ni doraslo kompleksnosti infrastrukture, zaradi česar lahko pride do napake, ki vodi do trajne izgube podatkov.[5]

Do izpada sistema lahko pride zaradi povsem nepredvidenih okoliščin. Ob izpadu Amazonovega podatkovnega centra aprila 2011 v ZDA je bilo ohromljeno delovanje številnih storitev (Reddit, Foursquare, Quora, Friendfeed). Navkljub podvojenemu sistemu in varnostnim kopijam so nekateri uporabniki trajno izgubili večjo količino podatkov.[5,8]

Pri trenutnem stanju zrelosti tehnologije in stopnji zakonske regulacije storitev v računalniškem oblaku je najrealnejša možnost postavitev lastnega (privatnega) oblaka za vse zdravstvene ustanove v Sloveniji. Večji kot je oblak, več prednosti oblačnih tehnologij se izrazi tudi v privatnem oblaku, obenem pa organizacija v primeru lastnega (privatnega) oblaka obdrži popoln nadzor nad opremo, vzdrževalnimi postopki in osebjem ter seveda zavarovanjem in nespornim izvajanjem lastništva podatkov.[5]

Problemi varovanja informacij

V zdravstvenih organizacijah nastaja velika količina zaupnih osebnih podatkov, ki so vezani na telesno in duševno zdravje ljudi. Zato je razumljivo, da so zahteve glede varnosti pri beleženju, hranjenju in posredovanju teh podatkov v organizacijah velike in raznolike. Zdravstvene delavce veže k varovanju podatkov in informacij že etični kodeks, poleg tega pa tudi zakoni in predpisi s področja zdravstvenega varstva in zdravstvene dejavnosti, varstva osebnih podatkov in zbirk podatkov, ki so podrobneje predstavljeni v nadaljevanju. Te dokumente dopolnjujejo interni pravilniki zdravstvenih organizacij. Tako so npr. v kliničnem centru v Ljubljani na podlagi 13. in 14. člena Zakona o varstvu osebnih podatkov ter 82. člena Statuta zavoda kliničnega centra že v letu 2000 sprejeli Pravilnik o varovanju osebnih in drugih zaupnih podatkov ter dokumentiranega gradiva, ki določa, kako so zdravstveni delavci dolžni varovati informacije povezane z zdravjem pacienta in kdaj ter komu jih lahko posredujejo.[9]

Posredovanje podatkov

Za osebne podatke se bolj ali manj upravičeno zanimajo bolnik, njegovi svojci, vodstvo organizacije ter drugi zdravstveni delavci, zavarovalnice, delodajalci, raziskovalci, organi pregona in pravosodni organi. Ostali nimajo nobene pravice do vpogleda v občutljive osebne podatke bolnikov in vsaj v tem primeru je

zdravniška molčečnost lahko povsem izražena. Ob novinarskem interesu za določen dogodek zdravnik ali drugi zdravstveni delavec nikoli ne sme posredovati nobenih informacij o dogodku, temveč mora zainteresirane napotiti do osebe v organizaciji, ki je odgovorna za stike z javnostjo.

Osebni podatki se na podlagi določil Direktive Evropske komisije in Zakona o varovanju osebnih podatkov posredujejo tretjim osebam le izjemoma:[10,11]

- ob izrecni in prostovoljni privolitvi lastnika osebnih podatkov;
- pri uporabi podatkov s strani drugih zdravstvenih delavcev pod vnaprej opredeljenimi pogoji;
- zaradi izrazitega javnega interesa, ko je ta opredeljen v drugih zakonih;
- če je obdelava nujno potrebna za varovanje življenja ali telesa posameznika, na katerega se osebni podatki nanašajo.

Zakon lastniku nosilcev podatkov nalaga, da mora le-ta za vsako posredovanje osebnih podatkov (zdravstvene dokumentacije) zagotoviti možnost naknadnega ugotavljanja, kateri podatki so bili posredovani, komu in v kakšne namene. Zdravnik je tako dolžan voditi posebno evidenco komu, kdaj, kako in katere bolnikove podatke je posredoval.[10,12]

Posredovanje podatkov bolniku

Bolnik je lastnik lastnih medicinskih podatkov, zato jih ima pravico dobiti/zahtevati kadarkoli v postopku diagnostike ali zdravljenja. Po Zakonu o varstvu osebnih podatkov[12] je zdravnik dolžan, tudi proti plačilu stroškov posredovanja, posredovati osebne podatke iz zdravstvene dokumentacije lastnikom podatkov. Bolnik lahko uveljavlja pravico do vpogleda v zdravstveno dokumentacijo, dovoljeni pa so tudi prepisi izvirnikov ali drugačen prenos izvirne vsebine podatkov (ni pa upravičen do izvirnih nosilcev podatkov). Upravičencu (bolniku) ni potrebno utemeljevati želenega vpogleda v podatke, zahteve po prepisu ali prenosu vsebine, hkrati pa upravljavec (organizacija) ne sme z ničemer pogojevati teh zahtev.

Zadeva se zaplete pri načinu oziroma obliki posredovanja. Bolnik nikakor ne sme sam odnesti nosilcev podatkov izven varovanih prostorov z namenom prepisa, fotokopiranja ali skeniranja, saj bi se lahko dokumentacija izgubila, poškodovala ali uničila. Posledica je lahko izguba arhiva bolnikovih bolezenskih stanj. Bolnik si lahko prepiše želene podatke v varovanih prostorih v prisotnosti pooblaščene osebe, ki skrbi, da ne pride do odtujitve, poškodovanja ali spreminjanja občutljivih podatkov. Bolnik lahko pisno zaprosi tudi za računalniške izpise ali fotokopije svoje zdravstvene dokumentacije. Po navadi se v ta namen pripravi poseben obrazec, tako da ima organizacija na ta način arhivirano sledljivost vpogledov v zdravstveno dokumentacijo.[10,12]

Posredovanje podatkov svojcem

Bolnikovim svojcem brez privolitve ne smemo posredovati njegovih podatkov. Težave lahko nastopijo v zvezi z zdravstveno dokumentacijo tudi po bolnikovi smrti. Zdravnika namreč veže poklicna molčečnost tudi po bolnikovi smrti. Le redki bolniki v Sloveniji v svoji oporoki razrešijo zdravnike poklicne molčečnosti oziroma svojce pooblastijo za vpogled v zdravstveno dokumentacijo po smrti ali pa svojcem prepovedo vpogled v zdravstveno dokumentacijo. Mnogi načelno nasprotujejo pravici svojcev do vpogleda v zdravstveno dokumentacijo po bolnikovi smrti, saj zdravstvena dokumentacija ni predmet dedovanja.[10,13]

Svojci prvega dednega reda lahko izkažejo pravni interes vpogleda v zdravstveno dokumentacijo umrlega. Zdravnik oziroma zdravstvena organizacija nimata možnosti sama preveriti mnenja vseh svojcev glede vpogleda v zdravstveno dokumentacijo umrlega, zato morata zahtevati od sorodnika, ki želi vpogled, da predloži pisne izjave

vseh dedičev prvega reda, da se z vpogledom strinjajo. Zdravnik izvirne dokumentacije svojcem ne sme dati, zato dobi svojec v podpis tudi omenjeni zahtevek za fotokopije zdravstvene dokumentacije, ki jasno opredeljuje čas, v katerem mu bodo fotokopije ali računalniški izpisi posredovani, in kolikšen bo strošek te storitve. Podoben postopek sledi tudi v primeru, če bi dokumentacijo zahteval odvetnik enega od svojcev.[10,12]

Posredovanje podatkov vodstvu organizacije

Direktor organizacije je odgovoren za kakovost in strokovnost dela, pri čemer za del nalog strokovnega nadzora pooblasti strokovnega vodjo in vodje enot ali služb. Omenjene osebe oziroma organi morajo izvajati strokovni nadzor nad delom zaposlenih, zato imajo pri svojem delu tudi vpogled v občutljive bolnikove podatke. Če pride do pritožbe bolnika, le-ta s pritožbo hkrati dovoljuje vpogled v lastno zdravstveno dokumentacijo osebam, ki bodo izvajale nadzor, saj drugače ni mogoče priti do ustreznih sklepov glede spornega ukrepanja. Bolj problematičen je vpogled v zdravstveno dokumentacijo ob rednih nadzorih. V teh primerih bi potrebovali bolnikovo privolitev. Ker gre pri rednih nadzorih za aktivnosti, ki so namenjene bolj kakovostni oskrbi bolnikov na splošno, morajo pravilniki o varovanju podatkov in notranjem nadzoru to področje ustrezno opredeliti, da ne bi prihajalo do sporov.

Podobno tudi za nadzor, ki ga izvajajo Zdravniška zbornica Slovenije, Ministrstvo za zdravje in Zavod za zdravstveno zavarovanje Slovenije (ZZZS) velja, da nimajo pravice vpogleda v občutljive osebne podatke bolnikov brez njihove izrecne privolitve.[10,12]

Posredovanje podatkov drugim zdravstvenim delavcem

Ob zamenjavi zdravnika posredujemo izvirno zdravstveno dokumentacijo, računalniški zapis ali izpis ali fotokopije izvirne zdravstvene dokumentacije novemu zdravniku v zaprti ovojnici s kurirsko službo ali s priporočeno poštno pošiljko.

Posredovanje zdravstvene dokumentacije drugim zdravstvenim delavcem je upravičeno v primeru, kadar gre za zdravljenje bolnika, ne pa tudi za kakršnokoli izvedensko delo. Podatke torej upravičeno posredujemo zdravnikom, ki bodo bolnika zdravili, ne pa tudi zdravnikom izvedencem, ki bodo bolniku zgolj izdali zdravniško spričevalo (za delo ali upravljanje motornih vozil, oceno telesne okvare, oceno upravičenosti do dodatka za pomoč in postrežbo drugega, oceno invalidnosti ali oceno začasne sposobnosti za delo). V teh primerih potrebujemo izrecno privolitev bolnika za posredovanje občutljivih podatkov tretjim osebam. Tipična primera te prakse sta predloga za oceno telesne okvare in dodatka za pomoč in postrežbo drugega. Značilen primer posredovanja dokumentacije je prav tako ocena stopnje invalidnosti na podlagi sklenjenih pogodb med izvajalci in ZZZS, kjer je plačnik storitev ZZZS.[10,11,14]

Posredovanje podatkov v raziskovalne in učne namene

Bolniki morajo biti seznanjeni s posredovanjem lastnih osebnih podatkov v raziskovalne namene in morajo se pisno strinjati s takšnim zbiranjem podatkov. Če iz posredovanih zbranih podatkov ni mogoče razbrati identitete posameznika, privolitev bolnikov ni potrebna.

Številni dijaki, študenti ter specializanti pridejo med praktičnim delom v bolnišnicah dnevno v stik z zdravstveno dokumentacijo bolnikov. Bolniki morajo biti seznanjeni z možnostjo, da lahko odklonijo prisotnost študentov med preiskavami ter tudi njihov vpogled v zdravstveno dokumentacijo. Če tega ne storijo, vpogled študenta v konkretno dokumentacijo v okviru učnega procesa ni sporen.[10,12]

Posredovanje podatkov zavarovalnicam

Zavarovalnice imajo pravico do vpogleda v zdravstveno dokumentacijo bolnika izključno na podlagi pisne privolitve svojega zavarovanca. K temu dodajmo, da si kljub bolnikovemu privoljenju njihovo dokumentacijo lahko ogleda le zavarovalniški cenzor, ki je po poklicu zdravnik. Kadar zavarovalnica zahteva vpogled v bolnikovo zdravstveno dokumentacijo, mora priložiti fotokopijo dokumenta, s katerim jo zavarovanec pooblašča za vpogled v tisti del dokumentacije, ki se nanaša na obravnavani (npr. škodni) primer. Praviloma se cenzorju posredujejo fotokopije dela zdravstvene dokumentacije – izvirnih dokumentov praviloma ne pošiljamo.[10,11,14]

Posredovanje podatkov delodajalcem

Zdravniška organizacija se na tem področju predvsem ukvarja z zbiranjem podatkov o zdravniško upravičeni odsotnosti z dela in vzroki zanjo. Aktualno odsotnost bolnika z delovnega mesta je zdravnik dolžan evidentirati z datumom začetka, datumom predvidene kontrole, če odsotnost še ni zaključena, vzrokom odsotnosti (bolezen, poškodba, poškodba pri delu, poklicna bolezen) in na koncu še z datumom zadnjega dne odsotnosti. To so tudi podatki, ki jih lahko zdravniška organizacija posreduje delodajalcu, če bi se le-ta pozanimal glede odsotnosti svojega zaposlenega. Vse druge podatke lahko delodajalec pridobi le od delavca, nikakor pa ne od zdravniške organizacije.[10,12]

Posredovanje podatkov organom pregona in pravosodnim organom

Zdravnik se mora ravnati v skladu z Zakonom o kazenskem postopku, kadar je pri svojem delu ugotovil, da gre za poškodbo, sum poškodbe po tretji osebi ali za sum zlorabe, kadar je potrebno državnemu tožilcu ali najbližji postaji policije oziroma pristojnemu centru za socialno delo posredovati podatke o poškodovani ali zlorabljeni osebi (prijavna dolžnost). To se nanaša na zdravnika, ki se je prvi službeno srečal s poškodovancem.[10,15,16]

Na podlagi veljavne sodne odločbe o zaplembi medicinske dokumentacije (zdravstvenega kartona) ima sodišče pravico do vpogleda v zdravstveno dokumentacijo. V vseh drugih postopkih imajo organi pregona pravico do podatkov, v primeru, da imajo pisno potrdilo strinjanja stranke, na katero se osebni ali občutljivi podatki nanašajo.[10,17]

Pravne podlage za uporabo storitev prenosa medicinskih podatkov preko računalniških omrežij

Lastništvo podatkov

Lastnik podatkov je bolnik. Lastnik nosilcev podatkov pa je javni zavod ali zasebnik (v nadaljevanju organizacija), kjer hranimo našo medicinsko dokumentacijo. Ta organizacija mora tudi poskrbeti za ustrezno varovanje podatkov. Vsi zdravstveni delavci so se dolžni držati etičnih načel in predpisov o varovanju osebnih podatkov. Za izvajanje pravilnika in s tem za varovanje bolnikovih podatkov je neposredno odgovoren bolnikov osebni zdravnik, ki hrani bolnikovo zdravstveno dokumentacijo.[10,12]

Vsaka organizacija mora imeti tudi notranji pravilnik o varovanju osebnih podatkov, v katerem so podrobno opredeljeni pogoji zbiranja in hranjenja podatkov, vodenja evidenc, določitev varovalnih prostorov ter vstopnega režima vanje, dostop do podatkov, pogoji in način uničenja podatkov ter režim posredovanja podatkov drugim upravičencem. Vsi zaposleni in zunanji sodelavci, ki pri svojem delu obdelujejo in uporabljajo osebne podatke, morajo biti seznanjeni z Zakonom o varstvu osebnih podatkov, z drugo zdravstveno zakonodajo ter z vsebino pravilnika svoje organizacije o varovanju podatkov.[10,12]

Varovanje občutljivih podatkov

Lastništvo nosilcev podatkov je povezano z odgovornostjo varovanja le-teh. Vsaka organizacija mora določiti t. i. varovalne prostore. V teh prostorih se nahajajo nosilci osebnih podatkov, strojna in programska oprema. Praviloma so to ambulantni in upravni prostori, le redko tudi hodniki, čakalnice ter skupni prostori, kjer se nahajajo kartotečne omare z občutljivimi podatki. V tem primeru morajo biti ti prostori posebej varovani. Za varovanje podatkov je odgovoren direktor takšne organizacije ter od njega pisno pooblaščene osebe.[10,12]

Splošna načela zavarovanja občutljivih podatkov so:[10,12]

1. Varovani prostori morajo biti varovani z organizacijskimi ter fizičnimi in/ali tehničnimi ukrepi, ki nepooblaščenim osebam onemogočajo dostop do podatkov. Prostore morajo ves čas nadzorovati pooblaščene osebe, ko se v njih zadržujejo stranke. Če pooblaščene osebe ni v prostoru, morajo biti nosilci podatkov zaklenjeni.

2. Dostop do varovanih prostorov je mogoč izključno med delovnim časom, izven njega pa le na podlagi dovoljenja, ki ga lahko izda direktor.

3. Ključe varovanih prostorov ima direktor ter pooblaščene osebe.

4. Ključev ne smemo puščati v ključavnicah vrat varovanih prostorov.

5. Varovani prostori ne smejo ostajati nenadzorovani.

6. Izven delovnega časa morajo biti omare in pisalne mize z nosilci osebnih podatkov zaklenjene, računalniki in druga strojna oprema pa izklopljeni oziroma fizično ali programsko zaklenjeni.

7. Nosilci osebnih podatkov (kartotečne omare), hranjeni izven varovanih prostorov (hodniki, skupni prostori ipd.), morajo biti stalno zaklenjeni. Dostop do programske opreme mora biti varovan tako, da dovoljuje dostop samo za to v naprej določenim zaposlenim ali pravnim/fizičnim osebam, ki v skladu s pogodbo opravljajo dogovorjene storitve. Pristop do podatkov preko uporabne (aplikativne) programske opreme se varuje s sistemom gesel na nivoju operacijskega sistema, omrežja in uporabne programske opreme za avtorizacijo ter identifikacijo uporabnikov, programov in podatkov. Vsa gesla in postopki, ki se uporabljajo za vstop in administriranje mreže osebnih računalnikov (supervizorska oz. nadzorna gesla), administriranje elektronske pošte in administriranje uporabnih programov, hranita samo direktor in ena dodatna oseba.

8. Občutljivi osebni podatki se ne smejo hraniti izven varovanih prostorov.

9. Za potrebe obnavljanja računalniškega sistema ob okvarah in ob drugih izjemnih okoliščinah se zagotavlja redna izdelava kopij vsebine mrežnega strežnika in lokalnih postaj, če se podatki nahajajo tam. Te kopije se hranijo na posebej določenih mestih, ki morajo biti varna pred požarom, zavarovana proti poplavam in elektromagnetnim motnjam, v okviru predpisanih klimatskih pogojev ter zaklenjena.

10. Zaposleni ne smejo nenadzorovano puščati nosilcev osebnih podatkov na mizah ali jih kako drugače izpostavljati nevarnosti vpogleda nepooblaščenim osebam.

11. V prostorih, ki so namenjeni poslovanju s strankami, morajo biti nosilci podatkov in računalniški prikazovalniki nameščeni tako, da stranke nimajo vpogleda vanje.

12. Zaposleni vzdrževalci, čistilke, varnostniki idr. se izven delovnega časa lahko gibljejo v varovanih prostorih, ne da bi pri tem bila prisotna pooblaščena oseba ali direktor,

vendar jim mora biti onemogočen vpogled v osebne podatke. Nosilci podatkov so shranjeni v zaklenjenih omarah in pisalnih mizah, računalniki in druga strojna oprema so izklopljeni ali kako drugače fizično ali programsko zaklenjeni.

13. Vzdrževalci prostorov in druge opreme, poslovni partnerji in drugi obiskovalci imajo dostop do varovanih prostorih le v prisotnosti direktorja ali pooblaščene osebe.

14. Vzdrževanje in popravila strojne opreme, s katero se obdelujejo osebni podatki, so dovoljena samo, če je z njimi seznanjena pooblaščena oseba. Izvajalci morajo spremembe in dopolnitve programske opreme ustrezno dokumentirati. V času vzdrževalnih del mora biti ves čas prisotna pooblaščena oseba. Ta skrbi, da ne pride do nedopustnega ravnanja z osebnimi podatki.

Hraniti moramo izvirnike zdravstvene dokumentacije, bolnik pa si lahko priskrbi fotokopije ali dvojnike, na katerih lahko označimo, da so skladni z izvirnikom. Zdravstvene podatke moramo hraniti predpisano dobo, ki je za različne podatke različno dolga. Osebni podatki se lahko shranjujejo le toliko časa, dokler je to potrebno za dosego namena, zaradi katerega so se zbirali ali nadalje obdelovali.[10,13] Zbirke podatkov, ki vsebujejo bolnikove osebne podatke, kot tudi njegovo osnovno zdravstveno dokumentacijo, mora upravljavec hraniti 15 let. Bolnikovo zdravstveno izkaznico/karton (ime, priimek, EMŠO, številko zdravstvenega zavarovanja, naslov stalnega bivališča, telefon, izobrazba, poklic, osebni zdravnik, obiski pri zdravniku, diagnoza, terapija, predpisana zdravila itd.) ter popis bolezni mora upravljavec hraniti še 10 let po smrti bolnika. Izjema je zobozdravstveni karton, ki ga mora upravljavec hraniti trajno.[11] Po izpolnitvi namena obdelave se osebni podatki zbrišejo, uničijo, blokirajo ali anonimizirajo, če niso na podlagi zakona, ki ureja arhivsko gradivo in arhive, opredeljeni kot arhivsko gradivo, oziroma če zakon za posamezne vrste osebnih podatkov ne določa drugače.[12]

Pravna ureditev v Evropski uniji

Pravna podlaga za uporabo storitev prenosa medicinskih podatkov preko računalniških omrežij v državah Evropske unije je opredeljena že v Pogodbi o ustanovitvi Evropske skupnosti, kjer je prenos medicinskih podatkov preko računalniških omrežij opredeljen kot zdravstvena storitev in storitev informacijske družbe in tako spada tudi v področje sekundarne zakonodaje Evropske unije oziroma med direktive. Direktiva 95/46/ES določa zahteve v zvezi z zaupnostjo in varnostjo, ki jih morajo za zaščito pravic posameznikov izpolnjevati interaktivne spletne storitve. Direktiva 98/34/ES, ki je bila spremenjena z Direktivo 98/48/ES, predvideva postopek, ki državo članico obvezuje, da Evropski komisiji in ostalim državam članicam pred nacionalnim sprejetjem sporoči vsak osnutek tehničnega predpisa o proizvodih in storitvah informacijske družbe, vključno s prenosom medicinskih podatkov preko računalniških omrežij. Leta 2000 je bila sprejeta Direktiva 2000/31/ES, t. i. direktiva o elektronskem poslovanju, ki ureja zdravstvene storitve in storitve informacijske družbe, med katere sodi tudi prenos medicinskih podatkov preko računalniških omrežij. Direktiva 2002/58/ES določa za ponudnike storitev elektronskih komunikacij prek javnih komunikacijskih omrežij posebne zahteve, ki zagotavljajo zaupnost komunikacije in varnost njihovih omrežij. Leta 2008 sta Evropski parlament in Svet Evropske unije sprejela Direktivo o uveljavljanju pravic pacientov na področju čezmejnega zdravstvenega varstva, v kateri je obravnavana čezmejna mobilnost pacientov in njihove možnosti za dostop do čezmejnih storitev. Na podlagi sprejete direktive mora Evropska komisija sprejeti ukrepe, s katerimi bo zagotovila interoperabilnost sredstev, potrebnih za nudenje e-zdravstvenih storitev, vključno s prenosom medicinskih podatkov preko računalniških omrežij.

Kljub vsemu vloženemu trudu, da bi poenotili in poenostavili pravno ureditev za učinkovitejše izvajanje prenosa medicinskih podatkov preko računalniških omrežij v državah članicah EU, pa le peščica držav članic obstoječi zakonodaji Evropske

unije dosledno sledi.[18] Večina držav Evropske unije je začela uvajati storitve prenosa medicinskih podatkov preko računalniških omrežij, vendar skoraj nobena nima omenjenih zdravstvenih storitev vključenih v svoj zdravstveni sistem sistematično in pravno priznano, kar bi omogočalo njihovo rutinsko uporabo. Razlog za pomanjkanje pravne jasnosti so predvsem številna nerazjasnjena pravna in etična vprašanja, ki se porajajo ob uporabi prenosa podatkov.[18]

Iz navedb v evropskem poročilu o napredku na področju eZdravja v posameznih državah Evropske unije[19] je razvidno, da je na pravnem področju zdravja na daljavo (telehealth) manj nacionalnih regulativnih dokumentov, kot jih je na voljo za področje elektronskega zdravstvenega zapisa. Prav tako nekatere države (Belgija, Češka, Grčija, Nizozemska) menijo, da ni pravnih ovir za uporabo tovrstnih storitev, čeprav ne obstaja posebna zakonodaja, ki bi urejala to področje. Druge države (Avstrija, Madžarska, Ciper) navajajo, da je ravno pomanjkanje ustrezne pravne ureditve eden od razlogov za širšo uporabo teh storitev.

Pravna ureditev v Republiki Sloveniji

Evropska komisija navaja,[19] da trenutno v Sloveniji ni posebne zakonodaje, ki bi opredeljevala izvajanje storitev eZdravja, vendar pa bi se naj v Sloveniji pripravljal nov zakon o zbirkah podatkov s področja zdravstvenega varstva, čigar usoda še ni znana.

Kljub temu je potrebno pri izvajanju storitev prenosa medicinskih podatkov preko računalniških omrežij upoštevati obstoječo slovensko zakonodajo, zlasti

- Zakon o pacientovih pravicah (ZPacP),[20]
- Zakon o zdravstveni dejavnosti (ZZDej),[21]
- Zakon o zdravstvenem varstvu in zdravstvenem zavarovanju (ZZVZZ-UPB3),[22]
- Zakon o zbirkah podatkov s področja zdravstvenega varstva (ZZPPZ),[23]
- Zakon o varstvu osebnih podatkov (ZVOP-1-UPB1),[12]
- Zakon o zdravniški službi (ZZdrS-UPB3),[24]
- Zakon o elektronskem poslovanju na trgu (ZEPT),[25] ter
- Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP).[26]

ZPacP[20] govori v 44. členu o varstvu osebnih podatkov, v 45. členu pa o varovanju poklicne skrivnosti oziroma o razrešitvi obveze. Oba člena torej naslavljata varovanje osebnih podatkov. Zaradi pomembnosti navajamo oba člena v celoti.

44. člen (varstvo osebnih podatkov)

(1) Pacient ima pravico do zaupnosti osebnih podatkov, vključno s podatki o obisku pri zdravniku in drugih podrobnostih o svojem zdravljenju.

(2) S pacientovimi zdravstvenimi in drugimi osebnimi podatki morajo zdravstveni delavci in zdravstveni sodelavci ravnati v skladu z načelom zaupnosti in predpisi, ki urejajo varstvo osebnih podatkov.

(3) Uporaba in druga obdelava pacientovih zdravstvenih in drugih osebnih podatkov je za potrebe zdravljenja dopustna tudi na podlagi pacientove privolitve ali privolitve oseb, ki imajo pravico do privolitve v medicinski poseg ali zdravstveno oskrbo, če pacient ni sposoben odločanja o sebi.

(4) Uporaba in druga obdelava pacientovih zdravstvenih in drugih osebnih podatkov izven postopkov zdravstvene oskrbe je dovoljena le z njegovo privolitvijo ali privolitvijo oseb, ki imajo pravico do privolitve v medicinski poseg ali zdravstveno oskrbo, če pacient ni sposoben odločanja o sebi. Po pacientovi smrti lahko dajo privolitev njegovi ožji družinski člani, razen če je pacient to pisno prepovedal.

(5) Ne glede na določbo prejšnjega odstavka lahko uporabo pacientovih zdravstvenih in drugih osebnih podatkov izven postopkov zdravstvene oskrbe določa zakon.

(6) Privolitev za uporabo in drugo obdelavo osebnih podatkov po tretjem in četrtem odstavku tega člena ni potrebna:

- *če za namene epidemioloških in drugih raziskav, izobraževanja, medicinskih objav ali druge namene pacientova istovetnost ni ugotovljiva,*
- *če za namene spremljanja kakovosti in varnosti zdravstvene oskrbe pacientova istovetnost ni ugotovljiva,*
- *kadar prijavo zdravstvenega stanja zahteva zakon,*
- *kadar se zaradi potreb zdravljenja podatki posredujejo drugemu izvajalcu zdravstvenih storitev,*
- *kadar to določa drug zakon.*

(7) Osebni podatki, ki se obdelujejo v skladu s tretjim, četrtim in petim odstavkom tega člena, morajo biti ustrezni in po obsegu primerni glede na namene, za katere se zbirajo in nadalje obdelujejo.

(8) Pacient ima pravico določiti osebe, ki se lahko seznanijo z njegovo zdravstveno dokumentacijo, in osebe, katerim seznanitev z njegovo zdravstveno dokumentacijo prepoveduje, če to ni v nasprotju z zakonom. Pravica iz tega odstavka se uresničuje na način in pod pogoji, ki jih določa 45. člen tega zakona.

45. člen (varovanje poklicne skrivnosti)

(1) Zdravstveni delavci in zdravstveni sodelavci ter osebe, ki so jim zaradi narave njihovega dela podatki dosegljivi, so dolžni kot poklicno skrivnost varovati vse, kar pri opravljanju svojega poklica ali dela zvedo o pacientu, zlasti informacije o njegovem zdravstvenem stanju, njegovih osebnih, družinskih in socialnih razmerah ter informacije v zvezi z ugotavljanjem, zdravljenjem in spremljanjem bolezni ali poškodb (v nadaljnjem besedilu: informacije o zdravstvenem stanju).

(2) Dolžnosti varovanja informacij o zdravstvenem stanju pacienta lahko zdravstvenega delavca oziroma zdravstvenega sodelavca ali drugo osebo, ki so ji ti podatki dosegljivi zaradi narave njihovega dela, razreši:

- *pacient,*
- *starši oziroma skrbnik za otroka pred dopolnjenim 15. letom starosti,*
- *starši oziroma skrbnik za otroka po dopolnjenem 15. letu starosti, če so informacije potrebne za izvrševanje roditeljske pravice oziroma skrbništva, otrok pa sporočanja ni prepovedal,*
- *oseba, ki je imela pravico do privolitve v medicinski poseg oziroma zdravstveno oskrbo, če pacient ni bil sposoben odločanja o sebi, vendar samo glede informacij o zdravstvenem stanju, ki so vezane na medicinski poseg oziroma zdravstveno oskrbo, v katero je privolila,*
- *sodišče,*
- *druge osebe, kadar tako določa zakon.*

(3) Zdravnik lahko sporoči informacije o zdravstvenem stanju pacienta, če je to nujno potrebno za varovanje življenja ali preprečitev hudega poslabšanja zdravja drugih oseb.

Iz določil 2. alineje 44. člena ZPacP[20] izhaja, da morajo zdravstveni delavci in zdravstveni sodelavci ravnati s pacientovimi zdravstvenimi in drugimi osebnimi podatki v skladu z načelom zaupnosti in predpisi, ki urejajo varstvo osebnih podatkov, to pa je z določili ZVOP-1.[12]

Po 6. alineji 44. člena ZPacP[20] privolitev bolnika za uporabo in drugo obdelavo osebnih podatkov ni potrebna, kadar se zaradi potreb zdravljenja podatki posredujejo drugemu izvajalcu zdravstvenih storitev, kar je primer pri izmenjavi digitalne dokumentacije za izvedbo laboratorijskih preiskav.

Zavarovanje osebnih podatkov je urejeno v 24. členu ZVOP-1-UPB1,[20] ki določa:

(1) Zavarovanje osebnih podatkov obsega organizacijske, tehnične in logično ali namerno nepooblaščeno uničevanje podatkov, njihova sprememba ali izguba ter nepooblaščena obdelava teh podatkov tako, da se: 1. varujejo prostori, oprema in sistemsko programska oprema, vključno z vhodno-izhodnimi enotami; 2. varuje aplikativna programska oprema, s katero se obdelujejo osebni podatki; 3. preprečuje nepooblaščen dostop do osebnih podatkov pri njihovem prenosu, vključno s prenosom po telekomunikacijskih sredstvih in omrežjih; 4. zagotavlja učinkovit način blokiranja, uničenja, izbrisa ali anonimiziranja osebnih podatkov; 5. omogoča poznejše ugotavljanje, kdaj so bili posamezni osebni podatki vneseni v zbirko osebnih podatkov, uporabljeni ali drugače obdelani in kdo je to storil, in sicer za obdobje, ko je mogoče zakonsko varstvo pravice posameznika zaradi nedopustnega posredovanja ali obdelave osebnih podatkov.

(2) V primeru obdelave osebnih podatkov, ki so dostopni preko telekomunikacijskega sredstva ali omrežja, morajo strojna, sistemska in aplikativno programska oprema zagotavljati, da je obdelava osebnih podatkov v zbirkah osebnih podatkov v mejah pooblastil uporabnika osebnih podatkov.

(3) Postopki in ukrepi za zavarovanje osebnih podatkov morajo biti ustrezni glede na tveganje, ki ga predstavlja obdelava in narava določenih osebnih podatkov, ki se obdelujejo.

(4) Funkcionarji, zaposleni in drugi posamezniki, ki opravljajo dela ali naloge pri osebah, ki obdelujejo osebne podatke, so dolžni varovati tajnost osebnih podatkov, s katerimi se seznanijo pri opravljanju njihovih funkcij, del in nalog. Dolžnost varovanja tajnosti osebnih podatkov jih obvezuje tudi po prenehanju funkcije, zaposlitve, opravljanja del ali nalog ali opravljanja storitev pogodbene obdelave.

Zavarovanje občutljivih osebnih podatkov je posebej urejeno v 14. členu ZVOP-1-UPB1, ki določa:

(1) Občutljivi osebni podatki morajo biti pri obdelavi posebej označeni in zavarovani tako, da se nepooblaščenim osebam onemogoči dostop do njih, razen v primeru iz 5. točke 13. člena tega zakona.

(2) Pri prenosu občutljivih osebnih podatkov preko telekomunikacijskih omrežij se šteje, da so podatki ustrezno zavarovani, če se posredujejo z uporabo kriptografskih metod in elektronskega podpisa tako, da je zagotovljena njihova nečitljivost oziroma neprepoznavnost med prenosom.

Izzivi ob prenosu medicinskih podatkov preko računalniških omrežij

Navkljub svoji uporabnosti in razvitosti po svetu in v Evropi prenos medicinskih podatkov preko računalniških omrežij v vsakdanji medicinski praksi premalokrat uporabljamo. Razlog za to bi lahko bil v številnih nerešenih pravnih in etičnih vprašanjih, ki se pogosto porajajo v zvezi s tem. Uporabniki telemedicine moramo dobiti odgovore na naslednja vprašanja:

- Ali je ustrezno varovana zasebnost pacienta?
- Kako zagotavljamo zaupnost informacij?
- Ali spoštujemo in upoštevamo pacientovo avtonomnost?
- Ali so jasni pravni okviri zdravljenja?

Spoštovanje avtonomije posameznika naj bi bilo osnovno etično načelo družbe. Iz tega izhajata tudi pravica do zasebnosti in pravica do varovanja osebnih podatkov, ki sta temeljni človekovi pravici. Nemalokrat se zgodi, da sta omenjeni pravici pri uporabi prenosa medicinskih podatkov preko računalniških omrežij zlorabljeni. Takšen primer predstavlja razkritje bolnikovega

zdravstvenega stanja ali diagnoze, kar lahko ima posledično močan vpliv na bolnikovo zasebno in poklicno življenje.[18]

Zaključek

Pri zajemanju, obdelavi, hrambi in posredovanju pacientovih podatkov je potrebno upoštevati obstoječo zakonodajo Republike Slovenije, direktive EU in spoštovati pacientove pravice ter delovati z veliko mero skrbnosti in odgovornosti. Varnost osebnih podatkov je torej ključna, da dosežemo zaupanje pacientov v prenos medicinskih podatkov preko računalniških omrežij, s tem zmanjšamo stroške v zdravstvu in hkrati dvignemo raven zdravstvenih storitev ter tako izboljšamo kakovost življenja pacientov.

Literatura

1. Ministrstvo za zdravje Republike Slovenije: e-Zdravje 2010 – Strategija informatizacije slovenskega zdravstvenega sistema 2005-2010. Ljubljana 2010: Ministrstvo za zdravje. http://www.ris.org/uploadi/editor/1130935067OsnutekeZdravje2010-01.pdf
2. Rudel D, Gašperšič J, Breskvar M, Vidjen TS: *Izhodišča za pripravo nacionalne strategije zdravja na daljavo (delovni osnutek)*. Ljubljana 2012: SDMI. https://zdrzz.si/files/Izhodisca%20za%20strategijo%20ZND_V21_2012-07-05.pdf
3. European Commission: eHealth Action Plan 2012-2020 – Innovative healthcare for the 21st century. Brussels 2012: European Commission. https://ec.europa.eu/digital-agenda/en/news/ehealth-action-plan-2012-2020-innovative-healthcare-21st-century
4. Das S, Mukhopadhyay A: Security and Privacy Challenges in Telemedicine. *CSI Communications* 2011; 35(8): 20-23.
5. Sedlar U, Bešter J, Kos A: Računalništvo v oblaku v telekomunikacijah in primeri uporabe. V: Mlinar T, Caf D, Robnik A, *et al.* (ur.), *Komunikacije in računalništvo v oblaku: zbornik referatov (26. VITEL)*. Ljubljana 2011: Elektrotehniška zveza Slovenije;: 3-6. http://www.ltfe.org/wp-content/uploads/2011/11/2-Urban-Sedlar-Janez-Bester-Andrej-Kos-VITELnov2011.pdf
6. Mell P, Grance T: *The NIST Definition of Cloud Computing (NIST Special Publication 800-145)*. Gaithersburg 2011: National Institute of Standards and Technology. http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf
7. Pirc Musar N: *Uporaba storitev računalništva v oblaku (mnenje)*. Ljubljana 2011: Informacijski pooblaščenec. http://bit.ly/JFyIH6
8. Fogarty K: Amazon crash reveals 'cloud' computing actually based on data centers. *IT World* 2011. http://www.itworld.com/article/2743887/cloud-computing/amazon-crash-reveals--cloud--computing-actually-based-on-data-centers.html
9. Klemenc D, Milić, Požun P. Varovanje bolnikovih osebnih podatkov in podatkov o njegovem zdravstvenem stanju v Kliničnem centru Ljubljana. *Inform Med Slov* 2004; 9(1-2): 24-30.
10. Kersnik J, Tušek-Bunc K. Zdravnik kot lastnik in posrednik zdravstvene dokumentacije. *Medic razgl* 2007; 47(S1): 155-162.
11. European Commission: Directive 95/46/EC (TheDataProtectionDirective). *Official Journal* 1995; L 281: 31-50. http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:31995L0046
12. *Zakon o varstvu osebnih podatkov (uradno prečiščeno besedilo) (ZVOP-1-UPB1)*. Uradni list RS 94/2007. http://www.uradni-list.si/1/objava.jsp?urlid=200794&stevilka=4690
13. Zupančič K. Dedovanje, Zbirka predpisov z uvodnimi pojasnili. [ZP Uradni list RS, Ljubljana 1992].
14. Beyleveld D, Townend D, Rouille-Mirza S, et al. The data protection Directive and Medical Research Across Europe. Burlington, ZDA: Ashgate Publishing, Ltd.; 2004.
15. Zdravniška zbornica Slovenije: *Kodeks medicinske deontologije Slovenije*. Ljubljana 1997: Zdravniška zbornica Slovenije. http://www.zdravniskazbornica.si/zzs.asp?FolderId=386
16. *Kazenski zakonik (KZ-UPB1) (uradno prečiščeno besedilo)*. Uradni list RS 95/2004. http://www.uradni-list.si/1/content?id=51064
17. *Zakon o kazenskem postopku (uradno prečiščeno besedilo) (ZKP-UPB4)*. Uradni list RS 32/2007. http://www.uradni-list.si/1/objava.jsp?urlid=200732&stevilka=1700
18. Prijatelj V, Hudernik Preskar A, Krstov L: Pravna in etična vprašanja ob uporabi zdravstvenih storitev na daljavo. *Inf Med Slov* 2010; 15(1): 26-29.

19. empirica: *eHStrategies – News*. http://www.ehealth-strategies.eu/news/new.html
20. *Zakon o pacientovih pravicah (ZPacP)*. Uradni list RS 15/2008. http://www.uradni-list.si/1/objava.jsp?stevilka=455&urlid=200815
21. *Zakon o zdravstveni dejavnosti (ZZDej)*. Uradni list RS 36/2004. http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO214
22. Zakon o zdravstvenem varstvu in zdravstvenem zavarovanju (uradno prečiščeno besedilo) (ZZVZZ-UPB3). Uradni list RS 72/2006. http://www.uradni-list.si/1/objava.jsp?urlid=200672&stevilka=3075
23. *Zakon o zbirkah podatkov s področja zdravstvenega varstva (ZZPPZ)*. Uradni list RS 65/2000. http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO1419
24. *Zakon o zdravniški službi (uradno prečiščeno besedilo) (ZZdrS-UPB3)*. Uradni list RS 72/2006. http://www.uradni-list.si/1/objava.jsp?urlurid=20063076
25. *Zakon o elektronskem poslovanju na trgu (ZEPT)*. Uradni list RS 61/2006. http://www.uradni-list.si/1/objava.jsp?urlid=200661&stevilka=2566
26. *Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP-UPB1)* (uradno prečiščeno besedilo). Uradni list RS 98/2004. http://www.uradni-list.si/1/objava.jsp?urlid=200498&stevilka=4284