UNIVERZA V LJUBLJANI

EKONOMSKA FAKULTETA

MAGISTRSKO DELO

PRIPRAVLJENOST ZDRAVSTVENEGA SEKTORJA NA UVEDBO ELEKTRONSKEGA POSLOVANJA

Ljubljana, marec 2009 ALEŠ ANŽUR

IZJAVA

Študent Aleš Anžur izjavljam, da sem avtor tega magistrskega dela, ki sem ga napisal pod mentorstvom prof. dr. Mira Gradišarja in skladno s 1. odstavkom 21. člena Zakona o avtorskih in sorodnih pravicah dovolim objavo magistrskega dela na fakultetnih spletnih straneh.

V Ljubljani, februar 2009 Podpis: _____

KAZALO VSEBINE

KAZALO SLIK, GRAFOV IN TABEL

UVOD

Problematika

V nekem obdobju svojega življenja vsi potrebujemo zdravniško pomoč, zato je vsak izmed nas zainteresiran za učinkovit zdravstveni sistem. Informatika v zdravstvu je področje, kjer je zdravstvenemu sistemu mogoče dati najvišjo dodano vrednost (Resolucija o nacionalnem planu zdravstvenega varstva 2008-2013 »Zadovoljni uporabniki in izvajalci zdravstvenih storitev«, Ur. l. RS, št. 72/2008, str.10046). Različni avtorji menijo, da lahko uporaba sodobnih informacijskih in komunikacijskih tehnologij pomembno poveča učinkovitost zdravstvenega sistema in kakovost storitev (Potts & Barr & Gregory & Wright & Patel, 2004, str.59-63 in Tamblyn et al., 2003, str. 549-556). Zdravstvo je informacijsko intenzivna dejavnost, ki potrebuje ustrezno informacijsko in komunikacijsko infrastrukturo (Stead & Brian Kelly & Kolodner, 2005). Bates (2002) navaja, da imajo zdravstvene organizacije še veliko možnosti za izboljšanje kakovosti z večjo uporabo informacijskih tehnologij, saj so njihovi sistemi relativno zastareli, pa tudi investicije so manjše od drugih informacijsko intenzivnih panog npr. bančništva ali letalstva. Tako vidi priložnosti za dvig učinkovitosti in kakovosti predvsem z računalniško podporo procesom dela in sprejemanju odločitev.

Znanje in odkritja, oziroma izboljšave se v zadnjem desetletju povečujejo eksponencialno predvsem zaradi razpoložljivih, hitro dostopnih informacij, kar omogočajo sodobna informacijska orodja in internet (Dimovski & Penger & Škerlavaj, 2002, str. 13-15). Prikaz informacijske opremljenosti izvajalcev zdravstvenih storitev je zato zelo zanimiv, saj lahko predvidimo nekatere ovire, na katere bomo naleteli pri privzemanju elektronskega poslovanja kot običajnega načina dela. Na Norveškem je že leta 2001 vsaj 72% bolnišničnih zdravnikov uporabljalo računalnik (Laerum & Ellingsen & Faxvaag, 2001). Kakšno pa je stanje v Sloveniji?

Mobilnost državljanov Evropske unije (EU) in možnost uveljavljanja zdravstvenega varstva kjerkoli v EU postavljata pred zdravstvene informacijske sisteme držav članic nove zahteve po povezanosti in interoperabilnosti zdravstvenih informacijskih sistemov. Strategija informatizacije slovenskega zdravstva, eZdravje2010, poudarja pomen informacijske infrastrukture kot predpogoja za izmenjavo podatkov (Kodele & Košir & Marušič & Sušelj, 2005, str. 6). Katerakoli sodobna aplikacija namreč temelji na izmenjavi podatkov. Med cilji EU, navedenimi v akcijskem načrtu so tudi omogočanje povezovanja nacionalnih zdravstvenih sistemov za zagotavljanje večje mobilnosti pacientov in stroke, (eHealth ERA report, 2007).

Trendi na področju informatike v zdravstvu potekajo v smeri elektronskega zdravstvenega zapisa, spletnih rešitev in varnosti podatkov (Meglič & Marušič & Anžur & Kodele,

2007c, str. 39). Informatika kot eno glavnih strateških orodij naj bi postala povezovalec kliničnega procesa in subjektov zdravstvenega sistema, kar bi zagotovilo lažje upravljanje in dolgoročno finančno vzdržnost celotnega zdravstvenega sistema. Z informatizacijo poslovanja se želi povečati transparentnost nad delovanjem celotnega zdravstvenega sistema, s tem ustvariti razmere, ki bodo izvajalce silile v primerjave (angl. *benchmarking*) in standardizacijo (angl. *best-practices*) in s tem učinkovitejše delovanje. Državljanu se želi ponuditi določene interakcije z zdravstvenim sistemom preko modernih spletnih aplikacij, ga osveščati o pomembnosti zdravega načina življenja in mu omogočili vpogled v svoje podatke. Tako naj bi se sistem razbremenil zamudnih administrativnih opravil in v središče postavil človeka in celovit pogled v njegovo zdravje. Vlada RS je 27.6.2007 sprejela Strategijo razvoja informacijske družbe v Republiki Sloveniji (Ministrstvo za visoko šolstvo, znanost in tehnologijo, 2007, str. 49), ki za področje zdravstva vsebuje naslednje strateške cilje:

- vzpostavitev osnovne informacijske infrastrukture, ter opredelitev osnovne zbirke zdravstvenih in socialnih podatkov za vzpostavitev in vodenje elektronskega zapisa zdravstvenih podatkov pacientov, pa tudi vzpostavitev osnov za elektronski zapis teh podatkov na državni ravni do konca leta 2007,

- postavitev varnostnih in tehnoloških standardov za varno komunikacijo, upravljanje in hrambo zdravstvenih podatkov,

- priprava izvedbenega načrta razvoja programov po merilih največjih strokovnih in stroškovnih učinkov,

- združitev zdravstvenih in socialnih informacijskih sistemov v celovit sistem na državni ravni s posebnim poudarkom na vzpostavitvi enotnega zdravstvenega informacijskega portala (krajše EZIP), ki bo vsem subjektom zdravstvenega sistema omogočil varno in zanesljivo izmenjavo podatkov, izvajanje elektronskih storitev ter enotno (standardizirano) in pregledno obveščanje in povezljivost s primerljivimi sistemi v EU do konca leta 2010,

- uveljavitev e-poslovanja kot običajnega načina dela v slovenskem zdravstvu do konca leta 2010.

V zdravstvenih sistemih predstavlja informacijsko komunikacijska tehnologija eno temeljnih orodij, ki lahko skupaj z organizacijskimi spremembami in razvojem novih veščin pripomorejo k učinkovitejšemu razvoju, večji učinkovitosti in produktivnosti, boljši dostopnosti in izboljševanju kakovosti. Informacijsko komunikacijska tehnologija mora zagotoviti državljanom boljše in lažje dostopne zdravstvene storitve, zdravstvenim strokovnjakom pa lažje delo, ter hitrejši dostop do potrebnih informacij. Eden od pogojev za uspešno načrtovanje projektov je poznavanje izhodiščnega stanja (COBIT 4.1, str 26-53).

Namen in cilj raziskave

V nalogi ugotavljam pripravljenost zdravstvenega sektorja za uvedbo elektronskega poslovanja predvsem iz stališča tehnološke opremljenosti izvajalcev. Iz tega stališča tudi postavljam hipotezo magistrske naloge: zdravstveni sektor v Sloveniji je pripravljen na elektronsko poslovanje.

Elektronsko poslovanje je v tesni povezavi s procesi, tehnologijo, kadri, njihovo organiziranostjo, ter pravno infrastrukturo, kar vse vpliva na prenovo poslovanja, ki jo načrtovani projekti eZdravja prinašajo.

Za načrtovanje in realizacijo informacijskih projektov je potrebno poznati obstoječe stanje, zato so cilji magistrskega dela:

- s študijem literature opredeliti ključna področja elektronskega poslovanja v zdravstvu,
- izvesti analizo ankete o informacijski opremljenosti izvajalcev zdravstvene dejavnosti,
- prikazati stanje in opozoriti na probleme.

Metodologija

Magistrska naloga je v osnovi pozitivistična študija, v kateri imam opravka s kvantitativnimi podatki, zbranimi s pomočjo ankete. Kot metodo za zbiranje primarnih podatkov uporabim anketo. V anketi je zajetih 1591 ustanov, ki spadajo v zdravstveni sektor glede na javno objavljene podatke (vir: www.zzzs.si, 15.7.2006). Anketiranje izvedem s pomočjo aplikacije za spletno anketiranje. Aplikacija omogoča, da anketirance povabim k sodelovanju preko elektronske pošte, ki vsebuje povezavo do ankete. Anketiranec se v aplikacijo prijavi z uporabniškim imenom in geslom, ki mu ga pošljem skupaj z vabilom. K sodelovanju so povabljeni vodje informatike oziroma odgovorne osebe za informatiko v ustanovi. Zbrani rezultati so prikazani grafično in tabelarično. Z aplikacijo za spletno anketiranje si olajšam združevanje podatkov in zmanjšam napake pri vnosu in seštevanju.

S časovnega vidika gre za presečno študijo, ki prikazuje stanje informacijske opremljenosti v obdobju izvajanja ankete. Tip raziskave je po namenu opisna raziskava, saj opisuje stanje

informacijske opremljenosti izvajalcev zdravstvene dejavnosti in njihovo pripravljenost na uvedbo elektronskega poslovanja.

Pripravljenost zdravstvenega sektorja na elektronsko poslovanje bom ocenjeval po posameznih kazalcih, ki bodo ali pa ne potrjevali postavljeno hipotezo. Če bo delež tistih, ki ne izpolnjujejo osnovnih pogojev, manjši od 5% glede na število zaposlenih v zdravstvenem sektorju, bom rekel, da je sistem kot celota pripravljen.

Omejitve raziskave in struktura

Elektronsko poslovanje zdravstvenih organizacij je zelo široko področje. Ker nam z naraščanjem števila anketnih vprašanj upada število prejetih odgovorov, sem se trudil najti kompromis. V anketi je zato zajet predvsem tehnološki del, ki omogoča elektronsko poslovanje. Ker so anketirane tudi manjše ustanove, ki nimajo zaposlenih informatikov, obstaja možnost, da bi na nekatera vprašanja težje odgovorili ali bi vprašanja narobe razumeli. V ta namen in za primer tehničnih problemov imajo pri dostopu do spletne ankete navedeno tudi kontaktno telefonsko številko in elektronski naslov.

Zaradi obsežnosti problematike opredelim samo tista področja, kjer je v ustanovah sorazmerno enostavno uvesti spremembe, so osnova za nadaljnje aktivnosti, so kritična za ustanovo in njeno delovanje in se tveganja, povezana z njimi, pojavljajo pogosteje. Seveda so pomembna tudi ostala področja, vendar presegajo obseg in namen naloge.

V prvem poglavju govorim na splošno o informatiki v zdravstvu, razložim nekatere pojme, ki se na obravnavanem področju najpogosteje pojavljajo in predstavim temeljni dokument razvoja informatike v zdravstvu Slovenije, strategijo eZdravje.

V drugem poglavju opredelim pojme elektronskega poslovanja in ključna področja, povem, kdaj poslujemo elektronsko in zakaj sploh uvajati elektronsko poslovanje v zdravstvo. Nato se v podpoglavjih podrobneje ukvarjam s posameznimi elementi, njihovim razvojem, možnostmi, dobrimi praksami, standardi in organizacijami, ki vplivajo na razvoj elektronskega poslovanja v zdravstvu. Predstavim tudi pravne podlage, ki jih je potrebno upoštevati.

V tretjem poglavju opredelim pripravljenost na elektronsko poslovanje, prikažem stanje, analiziram rezultate ankete in opozorim na probleme. V sklepnem poglavju povzamem ugotovitve raziskave.

1 SPLOŠNO O INFORMATIKI V ZDRAVSTVU

V angleški literaturi, ki opisuje uporabo informacijsko komunikacijskih tehnologij v zdravstvu, najpogosteje najdemo izraze:

- Health Care Informatics, ki ga prevajamo kot informatiko v zdravstvu,
- Medical informatics ali Health Informatics, ki ju prevajamo kot medicinsko informatiko,
- Electronic Health Record prevajamo kot elektronski zdravstveni zapis.

Najdemo seveda še mnogo drugih izrazov. Kako so ti izrazi med seboj povezani? Kaj je, kaj zajema in kakšen je cilj informatike v zdravstvu? Različni avtorji navajajo različne definicije, kaj določen izraz pomeni in katera področja zajema. Pogorelc (1999, str 1-13) meni, da izraz informatika v zdravstvu ni le sinonim za medicinsko informatiko, torej predvsem zdravniško klinično prakso, ampak predstavlja širši pojem. Englebardt in Nelson, (2002, str XVIII) navajata, da informatiko v zdravstvu sestavljajo področja informatike v zdravstveni negi, medicinske informatike, informatike na področju zobozdravstva in managementa informatike na področju zdravstva, ki pa se medsebojno prekrivajo. Spet drugi navajajo poleg navedenih področij še informatiko na področju javnega zdravja in posameznika, lekarn in farmacevtske industrije, ter biomedicine in bioinformatike. Da gre za pojme, ki se med seboj prepletajo in da področja niso jasno in ostro ločena, nam pokaže tudi naslednja definicija, če jo primerjamo s prejšnjo: »Informatika v zdravstveni negi je integracija zdravstvene nege in menedžmenta informacije s procesiranjem informacije in komunikacijskimi tehnologijami v smislu podpiranja zdravja ljudi po celem svetu.«(Kokol, 2003, str. 88).

Na spletni strani http://www.coiera.com/bk-intro.htm Coiera predstavi svojo knjigo Guide to Health Informatics in informatiko v zdravstvu slikovito opiše z besedami: »Če fiziologija dobesedno pomeni "logiko življenja", in patologija "logiko bolezni", potem je informatika v zdravstvu logika zdravstvenega varstva«.

Van Bemmel in Musen (1997) sta zapisala, da gre za znanost, ki proučuje nastanek podatkov, informacij in znanja, ter njihovo uporabo v medicini, zdravstvenem varstvu in javnem zdravju.

Lahko povzamemo, da gre za apliciranje računalništva in informatike na področju zdravstva v najširšem pomenu.

Primarni cilj informatike v zdravstvu je izboljšanje zdravstvenega sistema, tako izboljšanja izvajanja zdravstvenega varstva za odjemalce, kot izboljšanje pogojev za izvajalce in podpora institucijam zdravstvenega varstva (Englebardt & Nelson, 2002, str. XVII).

1.1 Strategija eZdravje

Ključni dokument na področju slovenske informatike v zdravstvu je strategija eZdravje. Strategija eZdravje se ne ukvarja s posameznim področjem informatike v zdravstvu, ampak zasleduje cilj vzpostavitve enovitega sistema, ki bo omogočal razvoj elektronskega poslovanja v zdravstvu kot običajnega načina dela. Seveda se nam pri tem porodi vprašanje, kakšna je pripravljenost zdravstvenega sektorja na uvedbo elektronskega poslovanja.

Ker prevajamo angleški izraz eHealth kot eZdravje, poglejmo najprej, kakšen je njegov pomen. Oh & Rizo & Enkin & Jadad (2005, str. 1) v sistematičnem pregledu preko 50 objavljenih definicij pojma eHealth do leta 2004 ugotavljajo, da gre za široko uporabljano in sprejeto novo besedo, ki je nastala kot posledica pomanjkanja primernega izraza. eHealth naj bi bil odgovor in rešitve, ki jih lahko ponudijo sodobne informacijsko komunikacijske tehnologije na izzive, s katerimi se srečuje zdravstvo (Alvarez, 2002). Zelo pogosto citirana je definicija: »eZdravje je področje, ki nastalo v presečišču medicinske informatike, javnega zdravja in poslovnih rešitev, ki se nanašajo na zdravstvene storitve in posredovanje informacij s pomočjo interneta in z njim povezanih tehnologij. V širšem smislu izraz označuje ne le tehnični razvoj, temveč tudi stanje duha, način razmišljanja, odnos in zavezo mreženju in globalnemu razmišljanju z namenom izboljšati zdravstveno varstvo lokalno, regionalno in širše z uporabo informacijsko in komunikacijskih tehnologij« (Eysenbach, 2001, str.1).

Ministrstvo za zdravje je decembra 2005 objavilo Strategijo informatizacije slovenskega zdravstvenega sistema e-Zdravje 2010 in jo kasneje vgradilo v Resolucijo o nacionalnih razvojnih projektih do leta 2023. S širšo uporabo informacijsko komunikacijskih sredstev se želi doseči učinkovitejši zdravstveni sistem. V ospredju so resnične koristi za državljane in bolnike, na drugem mestu so povečana učinkovitost in nadzor zdravstvenega sistema, šele na tretjem mestu pa tudi ekonomski učinki vlaganj (Marušič, 2007, str. 37). Strategija opredeljuje cilje, strateška področja in predlaga aktivnosti za doseganje omenjenih ciljev do leta 2010. V skladu z vizijo učinkovite, prožne in sodobne zdravstvene informatike opredeljuje naslednje strateške usmeritve: boljša informiranost, aktivnejša vloga državljana pri zdravljenju, hitrejši dostop do potrebnih informacij za zdravstvene strokovnjake in lažje upravljanje sistema zdravstvenega varstva. Prav tako opredeljuje zagonske naloge, kamor sodijo ustanovitev teles in organov za načrtovanje, koordinacijo, vodenje in nadzor razvoja ter uporabe informatike v zdravstvu, nadgradnja osnovne informacijske infrastrukture v zdravstvu, vzpostavitev infrastrukture javnih ključev, priprava operativnega načrta razvoja aplikacij, pravočasno urejanje zakonskih podlag za uvajanje eZdravja, ureditev financiranja, motivacijskih shem in pravnih okvirov, promocije in vključevanja v evropski prostor. Strategija se opira na rezultate projekta Razvoja upravljanja sistema zdravstvenega varstva. Ob sprejetju leta 2005 je prinesla pričakovanje sprememb in upanje, da bi z

usklajenim delom, ter finančno in politično podporo upravljavcev zdravstvenega sistema Slovenija naredila odločen korak naprej ter se spet pojavila na zemljevidu držav z razvito zdravstveno informatiko (Meglič & Marušič & Kodele & Anžur, 2007b). Nekateri od prepoznanih pritiskov, ki terjajo nove pristope pri zagotavljanju in organizaciji zdravstvenih storitev in delovanju zdravstvenega sistema, so: zahteve po izboljšanju kakovosti storitev, dolgoročna finančna vzdržnost, evropski razvojni cilji in zakonska ureditev. Cilj je povezava evropskih zdravstvenih informacijskih sistemov in vizija, da bi prebivalci uveljavljali pravice do zdravstvenega varstva kjer koli v Uniji. Evropska Unija v svoji strategiji eZdravja poudarja zahtevo po urejeni zdravstveni informatiki vsake države članice. Pri tem se lahko vprašamo, kako urediti zdravstveno informatiko neke države. Eden od zanesljivih načinov je, da se vsaj v osnovi držimo standardov, kot je na primer COBIT. Osnovni princip pri takšnem pristopu je poznavanje stanja, določitev ciljev, izvajanje ukrepov in ponovno preverjanje. S sistematičnim pristopom vzpostavimo sistem neprestanih izboljšav.

2 OPREDELITEV POJMOV ELEKTRONSKEGA POSLOVANJA

Preprosto lahko rečemo, da elektronsko poslovanje pomeni »poslovati elektronsko« (Gradišar, 2003, str. 21). Evropska komisija v svojem dokumentu (European Commision, 2006) navaja naslednjo definicijo: elektronsko poslovanje je avtomatiziran poslovni proces, tako znotraj, kot med subjekti preko računalniškega omrežja. Za elektronsko poslovanje v tehnološkem smislu potrebujemo računalnike, komunikacije in aplikacije. Tem sestavinam je potrebno dodati še organizacijo poslovanja, saj šele z njo osnovne tehnološke sestavine podpirajo cilje poslovnega sistema. Pomemben pogoj je tudi pravna infrastruktura. Udeleženci, ki želijo poslovati elektronsko, se morajo dogovoriti za standarde, ki jih bodo pri tem poslovanju upoštevali, če tega ne predpisuje že sama zakonodaja, ki daje poslovanju pravni okvir. V najširšem smislu elektronsko poslovanje vključuje uporabo vseh oblik informacijske in komunikacijske tehnologije v poslovnih odnosih. Poleg načina dela je potrebno določiti še vsebine elektronskega poslovanja, ter udeležence. Glede na interakcijo udeležencev elektronskega poslovanja ločimo elektronsko poslovanje:

- med podjetji (B2B, Business to Business),
- med podjetji in potrošniki (B2C, Business to Consumer),
- med potrošniki (C2C, Consumer to Consumer),

- med podjetji in javno oziroma državno upravo (B2G, Business to Government),
- med državljani in javno oziroma državno upravo (C2G, Consumer to Government),
- znotraj javne oziroma državne uprave (G2G Government to Government).

Gradišar (2003, str. 28) ugotavlja, da le redka slovenska podjetja elektronsko poslovanje uvajajo strateško, z jasno določenimi cilji in poslovno vizijo. Zaradi nerazumevanja problematike vodstva podjetij to nalogo pogosto prepustijo kar informatikom. Elektronsko poslovanje pomeni uvajanje novih načinov poslovanja in prinaša korenite spremembe v organizacijo, logistiko, učinkovitost in v vse segmente poslovnega in delovnega okolja. Proces uvajanja elektronskega poslovanja lahko razdelimo na štiri stopnje. Podjetje si najprej pridobi osnovne izkušnje komuniciranja preko interneta s postavitvijo spletnih strani. V naslednjem koraku se s povezavo interneta in intraneta poveže z »zunanjim svetom«. Sledi medsebojno povezovanje s poslovnimi partnerji, s čimer podjetje prične spreminjati svoj uveljavljeni tradicionalni način poslovanja. Zadnjo stopnjo elektronskega poslovanja podjetje doseže, ko celovito preoblikuje svoje poslovanje, organizacijsko strukturo, strategijo in poslovni model. Podjetja se morajo zavedati, da je uvajanje elektronskega poslovanja zanje tako rekoč edina alternativa. V anketi sem udeležence vprašal, ali imajo spletno stran in kakšne funkcionalnosti nudi.

2.1 Zakaj uvajati elektronsko poslovanje v zdravstvo?

Nekateri izzivi zdravstva, naj gre za neprofitno ali profitno dejavnost, so si podobni povsod po svetu ter so podobni izzivom podjetij, zato so tudi odgovori nanje lahko podobni. Kot pišejo Kovačič, Groznik in Ribič (2005), bi morale organizacije izboljšati uspešnost poslovanja z nižjimi stroški, krajšimi izvajalnimi časi in boljšo kakovostjo ter s prenovo poslovanja v smeri preoblikovanja, prestrukturiranja ali prenove poslovnih procesov ob uporabi sodobne informacijske tehnologije. Pri tem mora biti strategija razvoja informatike usklajena s poslovno strategijo in zajemati tehnologijo, kadre in procese. Evropska komisija meni, da informacijsko komunikacijske tehnologije lahko ponudijo ustrezen odgovor na te izzive (European Commission, 2006). Avtomatizacija obstoječih procesov vpliva na učinkovitost njihovega izvajanja, informatizacija, ki ima vpliv na uspešnost poslovanja, pa omogoča in pogojuje organizacijske in druge spremembe in drugačen način dela. Toth (2008) ugotavlja, da ni mogoče podati dokončnega odgovora na vprašanje, kje je meja, do katere je mogoče zagotavljati več sredstev za zdravstvene potrebe. Vse bolj pa je v ospredju zahteva po bolj učinkovitem sistemu zdravstvenega varstva. Osrednje vprašanje je, kako zagotavljati ekonomsko in fiskalno vzdržnost sistema. Bolnika neredko zdravi več zdravnikov, ki drug za drugega ne vedo in tudi ne vedo, kaj je kateri od njih

opravil pri bolniku, katera zdravila mu je predpisal itd. To vpliva na potek, čas, način in stroške obravnave in seveda na kakovost zdravljenja. Kot eno od možnosti vidi izboljšanje informacij in komunikacij med izvajalci zdravstvenih storitev, zlasti zdravniki. Meni, da se možnosti, ki jih nudi informacijsko komunikacijska tehnologija v zdravstveni službi, še vedno premalo uporabljajo. Zato sta slabši kakovost storitev in učinkovitost sistema, saj omogočata nepotrebno ponavljanje preiskav, neustrezno predpisovanje zdravil in druge neracionalnosti.

Informacijska tehnologija omogoča drugačno delo oziroma prenovo procesov. Zato morata, če želimo izrabiti njune potencialne možnosti, prenova in informatizacija poslovanja potekati hkrati. Uvedba elektronskega poslovanja (e-poslovanja) zahteva spremembo in preureditev tradicionalnega modela organiziranosti, poslovnih procesov, odnosov in načina, ki so bili prevladujoči do sedaj. E-poslovanje zahteva prilagoditev in sinhronizacijo strateške vizije in njenega praktičnega udejanjanja z možnostmi, ki jih pri tem ponuja sodobna informacijska tehnologija. Potrebno pa se je zavedati, da vpeljava elektronskega poslovanja poleg številnih prednosti povzroči številne in večplastne spremembe v organizaciji. Med najpomembnejše sodijo prenova poslovnih procesov, organizacijske spremembe, spremenjena poslovna kultura in nova znanja (Kovačič & Jaklič & Štemberger & Groznik, 2004, str. 272).

Vse do sedaj naštete prednosti in priložnosti elektronskega poslovanja v zdravstvu prinašajo tudi možne slabosti, ki so podobne in morebiti še bolj izražene kot v primeru e-uprave (Kovačič et al., 2005 str. 260):

- zmešnjava informacij, ki nas lahko zbega, če jih ne znamo urediti glede na naše potrebe,
- socialna izločenost, ki je lahko povezana s starostjo, posledico bolezni ali nizko računalniško pismenostjo, ki je v veliki meri tudi posledica pomanjkanja opreme in izobraževanja,
- elektronske zlorabe, ki se pojavljajo pri odpiranju sistemov navzven, zaradi pomot, napak, pri nezadostnem nadzoru, …
- razčlovečenje odnosov in neosebni pristop, na kar smo, ko gre za zdravje, še posebej občutljivi.

Potrebno se je zavedati, da je zdravstvo vseeno področje, kjer osebnega stika nikoli ne bo mogoče popolnoma nadomestiti.

2.2 Računalniki

Osnovno kar pričakujemo od informacijsko komunikacijskega sistema, je povezovanje uporabnikov in tehnologije v produktivno celoto. Človek oz. končni uporabnik je najpomembnejši element sistema. Informacijski sistem naj bi bil podatkovni model realnega sveta. Pri obravnavi informacijsko komunikacijskega sistema moramo izhajati iz uporabnikovih potreb, to je iz človeka, ki sedi pred zaslonom in si s tipkovnico ali miško prizadeva sistem kakorkoli produktivno izkoristiti. Pri tem uporablja različne storitve, ki mu jih sistem nudi, npr. prenos in delo z datotekami, elektronsko pošto, www, … Povezovanje delovnih mest v okviru tehnologije je osnovna naloga komunikacijskega dela sistema, aplikacije pa so bistveni element informacijskega dela našega sistema. Za neposredno povezovanje ljudi in tehnologije poskrbi s svojimi specializiranimi modeli informacijski del sistema, naloga komunikacijskega dela sistema pa je, da med seboj poveže tehnologijo. Računalnik (namizni ali prenosni), delovna postaja je, kot lahko že iz imena sklepamo, orodje, ki seveda oživi in je za uporabnika koristen šele z določenemu delovnemu mestu ustrezno aplikacijo. Že leta 2002 so vsi zdravniki na Finskem in Danskem pri svojem delu uporabljali računalnike (Taylor & Leitman, 2002).

Poleg tega, da so računalniki dostopni posameznemu profilu zdravstvenega osebja, potrebujejo za učinkovito delo še njihovemu delu primerne aplikacije in znanje za delo z njimi. Pomemben element, ki vpliva na privzemanje elektronskega poslovanja kot običajnega načina dela, pa je tudi motivacija. O dostopnosti lahko sklepamo iz števila računalnikov in števila ljudi, ki tak računalnik uporabljajo.

Pri ugotavljanju stanja nas zanima tudi tehnološka zastarelost oziroma sodobnost računalnikov. Načinov bi bilo seveda več, npr. z ugotavljanjem datuma nakupa, kar pa bi za anketirance predstavljalo velik napor. Druga možnost, mogoče celo bolj točna od prve, saj lahko nekdo kupi tehnološko že zastarel računalnik, je z ugotavljanjem zmogljivosti, ki je pri delovnih postajah določena vsaj z tipom oz. zmogljivostjo procesorja, velikostjo pomnilnika z naključnim dostopom (RAM – angl. *Random Access Memory*) in trdega diska. Tudi zbiranje takšnih odgovorov za anketirance, ki jim njihov sistem ne omogoča enostavnega izvajanja inventure, predstavlja precej dela. Zato sem se odločil, da anketirance povprašam samo po tipu oziroma generaciji procesorja. Ne zanima me tržni delež, na katerega bi lahko sklepal iz tipa procesorja, ampak generacija (rang), iz česar lahko sklepamo na približno starost in zmogljivost računalnika.

Podobno je s sistemsko programsko opremo delovnih postaj. Pri tem je poznavanje tržnega deleža zanimivo, v kolikor bi se država želela zgledovati po nekaterih delih sveta, kjer so se odločili za:

- uvedbo odprtokodnih sistemov,

- ali morebitno sklenitev »Enterprise agreement« licenčne pogodbe za sektor s prevladujočim ponudnikom.

Naslednje področje, ki ga lahko obravnavamo v tem poglavju, so strežniki. V primeru bolj heterogenih okolij so zahteve po potrebnih znanjih za zagotavljanje tehnične podpore večje.

Računalniški sistem je informacijska infrastruktura delovnega mesta. Osnovni cilj povezovanja računalniških sistemov je povezovanje uporabnikov z viri računalniških sistemov. Problem, ki ga je treba rešiti, je združljivost virov, kar pomeni, da moramo zagotoviti produktivno sodelovanje na nivoju uporabnikov, kompatibilnost aplikacij, ki potekajo v različnih računalnikih, kompatibilnost operacijskih sistemov ter končno združljivost aparaturne opreme različnih računalnikov oziroma delovnih mest. Če želimo začeti izvajati aktivnosti za združljivost virov je dobro, da poznamo stanje, saj si bomo le tako lahko začrtali pot. Razpršenost virov informacijsko komunikacijskega sistema je naravna posledica razvoja in je danes jedro problemov, ki jih je potrebno rešiti.

2.3 Komunikacije

V tem poglavju prikažem razvoj storitev, ki jih nudijo sodobna omrežja. Iz stanja, ki ga bomo ugotovili s pomočjo ankete in možnosti, ki jih nudijo sodobna omrežja, bomo lahko sklepali na pripravljenost za uvedbo sodobnih storitev, smer razvoja in ovire, ki jih lahko pričakujemo.

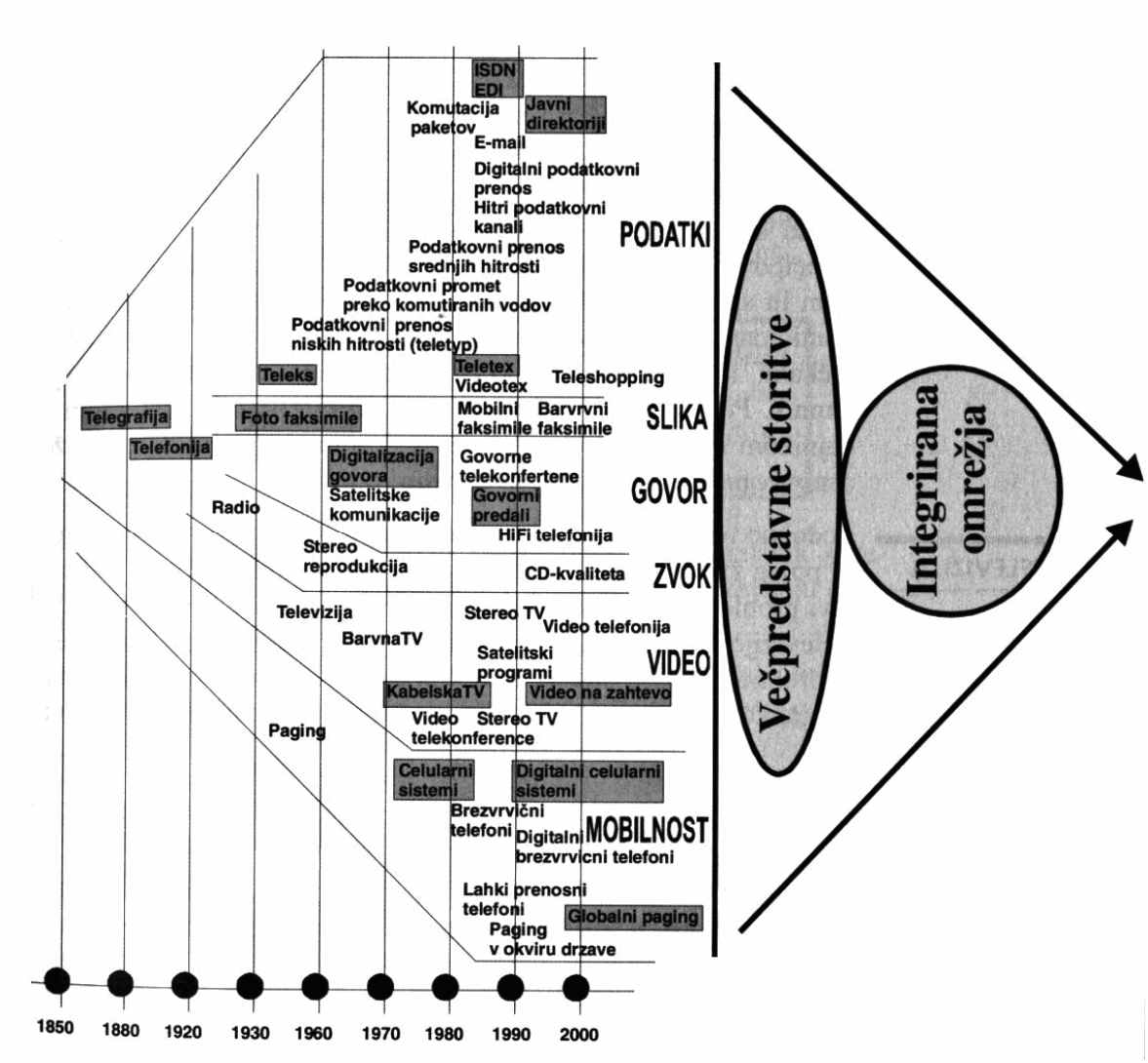
Cilji EU so tudi omogočanje povezovanja nacionalnih zdravstvenih sistemov za zagotavljanje večje mobilnosti pacientov in zdravstvenih strokovnjakov (Commission of the European Communities, 2004). Nadaljnji koraki članic EU morajo biti v smeri povezovanja zdravstvenih informacijskih sistemov in zagotavljanja interoperabilnosti (eHealth ERA report, 2007). Polovica držav EU (eHealth ERA report, 2007, str. 12) dela na nacionalni infrastrukturi, ki bo povezovala vse deležnike zdravstvenega sektorja, primarni, sekundarni nivo, lekarne in domačo oskrbo.

Zdravstvena industrija je močno odvisna od informacij. Zahteva sodelovanje številnih strani, zato lahko omrežna tehnologija izboljša kakovost, zmanjša stroške in podpre aplikacije, ki izboljšujejo oskrbo pacientov. Omrežna tehnologija, ki pomeni povezovanje podatkovnih, video in avdio vsebin, je način za izboljševanje učinkovitosti in kakovostne oskrbe.

2.3.1. Razvoj komunikacij

Informacijski sistem podatke obdeluje in posredno omogoča njihovo interpretacijo, medtem ko telekomunikacijski sistem omogoča komuniciranje (izmenjavo podatkov) med točkami informacijskega sistema (Vidmar, 2002). Telekomunikacijski sistemi povezujejo različna informacijska okolja in omogočajo njihovo medsebojno komunikacijo. Uporabnost telekomunikacijskega sistema se izkaže šele takrat, ko se preneseni podatki v informacijskem okolju sprejemnika interpretirajo. V uporabi so zelo raznolike storitve, ki so se v času razvijale kot kaže Slika 1: Razvoj storitev. Integrirana omrežja združujejo prenos podatkov, zvoka, govora, slik in uporabniku omogočajo mobilnost. Za začetek razvoja lahko štejemo izum telegrafije v 19. stoletju, kateremu so sledili različni tehnološki izumi, npr. digitalno omrežje z integriranimi storitvami - ISDN (angl. *Integrated Services Digital Network*), računalniško izmenjevanje podatkov - EDI (angl. *Electronic Data Interchange*) in drugi.

Slika 1: Razvoj storitev



Vir: Vidmar, Informacijsko-komunikacijski sistem, 2002, str.55

Z integracijo naraščajo možnosti informacijsko komunikacijskih tehnologij (IKT) in njihove zahteve po zmogljivosti prenosnih sistemov. Prenos podatkov, ki so potrebni za besedilo, sliko in računalniške aplikacije v klasičnem smislu, nima ostrih zahtev glede hitrosti in zakasnitev ga je načeloma mogoče realizirati s poljubno hitrim (počasnim) prenosnim kanalom. Govorimo o podatkovnih storitvah. Storitve v realnem času (telefonija) pa zahtevajo minimalno kapaciteto (širino) prenosnega kanala v celotnem času komunikacije. Ker je trend integracije storitev v tako imenovane večpredstavne storitve, ter razvoj omrežij v t.i. integrirana omrežja, ki so primerna za prenos podatkov za kakršnokoli storitev, pričakujem, da bodo tudi nacionalni projekti v zdravstvu imeli to smer.

V okviru IKT sistema se »srečujejo« različne tehnologije, različni operacijski sistemi (OS), aplikacije in pristopi k varnosti, skratka govorimo o različnih tehnoloških platformah. Ker pa je sistem dober, če delujejo vse komponente in ker moramo za to imeti podatke o vsaki komponenti, če si želimo uspešnega upravljanja, je bilo nujno, da so bili sprejeti standardi, ki omogočajo enovit način komuniciranja v smislu nadzora, upravljanja in zbiranja podatkov v standardizirano podatkovno bazo. Zato imamo SNMP (angl. *Simple Network Management Protocol*) v internetnem okolju in SMAE (angl. *System Management Application Entity*) v okolju OSI (angl. *Open Systems Interconnection*). Protokola bolj ali manj podrobno sistematizirata osnovne funkcije nadzora in upravljanja in kot taka sta standardizirano jedro nadzorno upravnega centra. Funkcije nadzora so se standardizirale v okviru aplikacijske plasti kot tipične standardne storitve: odkrivanje napak, ugotavljanje zmogljivosti, nadzor storitev posameznih plasti, vodenje imenskega prostora, implementacija varnostnih funkcij, zaračunavanje storitev, …

Arhitekturo informacijsko komunikacijskega sistema delimo na informacijske – zgornje plasti in komunikacijski podsistem – spodnje plasti. Osnovni tehnološki in infrastrukturni del transportne plasti je omrežje, katerega najopaznejša lastnost je topologija, definirana z vozlišči in povezavami med njimi. Osnovna storitev transportnega sistema je zagotavljanje povezljivosti med informacijskimi sistemi. Povezljivost pomeni, da se povežeta dva računalnika na nivoju podatkov oziroma aplikacijskih procesov. Za zagotovitev povezljivosti morata transportna plast in omrežna plast vzpostaviti t.i. končno povezavo, ki zagotavlja fizično komunikacijo med dvema informacijskima sistemoma. Arhitektura sistema opredeljuje plasti, njihova mesta v hierarhiji, logične povezave in funkcionalno vsebino posamezne plasti. Arhitektura se ukvarja z logičnimi odnosi med elementi sistema. Za izvedbo katerekoli logične povezave potrebujemo tudi vzpostavitev ustreznih fizičnih povezav. Prenosni sistem po modelu OSI sestavljata povezavna in fizična plast, medtem ko model TCP/IP opredeljuje le – prenosno plast. Prenosni kanal je naprava, ki lahko prenese paket (okvir) prek prenosnega medija med dvema ali več točkami. Standardne hitrosti v bitih na sekundo so: 2400, 4800, 9600, 19.2K, 28.8K, 33.3K, 57.6K, 64K, 128K, 256K, 512K, 1024K, 2M, 10M, 100M, 1G (Vidmar, 2002).

Pri informacijsko komunikacijskem sistemu se problem tehnologije razširi s problematiko standardizacije, komunikacijskih protokolov, posebnosti strukture sistema in krajevne razpršenosti opreme. Arhitekturo oziroma funkcionalnost informacijsko komunikacijskega sistema je treba obravnavati v okviru osnovnih domen (tehnološka, nadzorna, administrativna, upravna in varnostna), opredeljenih za sistem. Infrastrukturo lahko kategoriziramo takole:

- podatkovni sistemi (brezizgubna omrežja):
  - telegraf (besedilo), teleks (besedilo);
  - faks (slika);
  - klasični informacijski podatki (interaktivne storitve za prenos besedila).
- sistemi v realnem času (izgubna omrežja):
  - telefon (govor), radio (zvok);
  - televizija (video);
  - večpredstavne storitve (kombinacija in sinhronizacija vseh tipov podatkov).

Širokopasovnost je termin, ki najpogosteje opisuje hitre povezave uporabnikov v skupno omrežje. Povezave so izvedene z uporabo različnih tehnologij, kot so DSL (angl. *Digital Subscriber Line*), kabelsko omrežje, LAN (angl. *Local Area Network*), optične povezave,… Širokopasovnost omogoča hitro dostavljanje podatkov, avdia in videa na zahtevo - to je t.i. »triple play«. Storitve, ki jih širokopasovnost zagotavlja, se izvajajo na napravah, kot so osebni računalnik, video komunikator (angl. *Set-Top-Box*), telefon in ročne naprave. Širokopasovne rešitve predstavljajo zlivanje več neodvisnih omrežij v, iz perspektive uporabnika, združeno širokopasovno omrežje. Največkrat se širokopasovni dostop uporablja v povezavi z IP (Internet Protokol) omrežjem, ki združuje strežnike, omrežja in odjemalce v integriran sistem in omogoča komunikacijske rešitve, ki so preprostejše in cenovno bolj ugodne tako za implementacijo kot tudi za upravljanje. IP si lahko predstavljamo kot protokol današnjega in jutrišnjega (IPV6, Internet Protokol verzija 6) dne, ki bo podpiral »triple play« storitve.

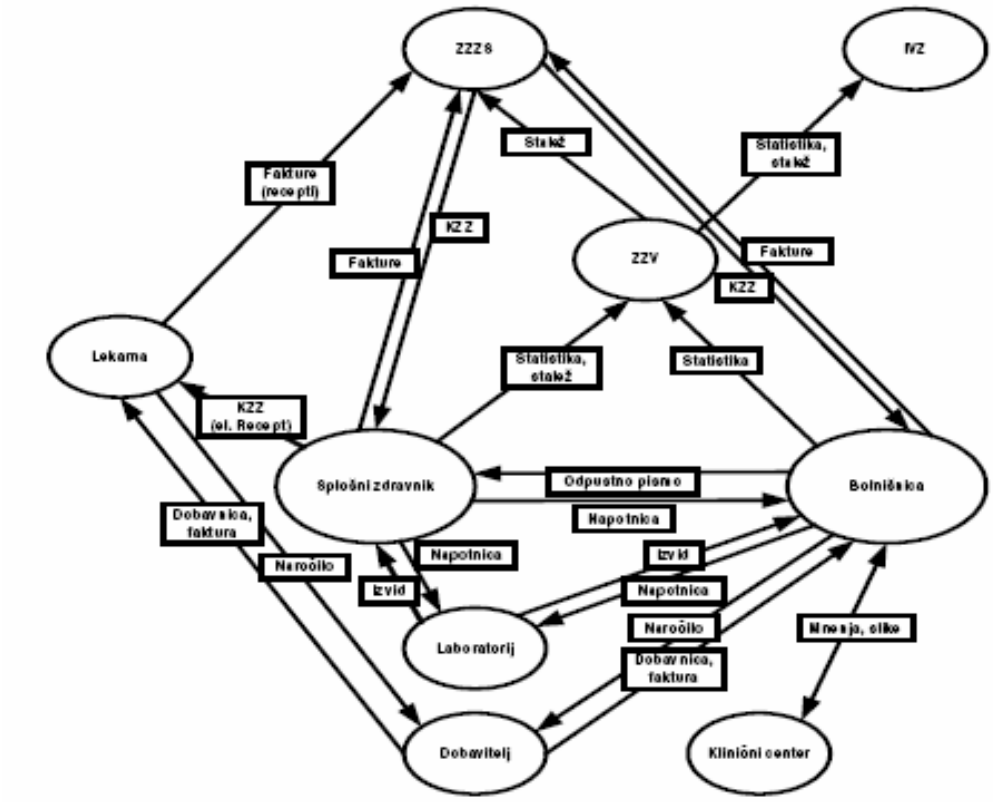
Povezovanje različnih virov ima dva vidika: sintaktičnega in semantičnega. Sintaktična združljivost pomeni, da je format podatkov tak, da ga sprejemnik razume, semantična združljivost pa pomeni, da podatki po vsebini ustrezajo namenu aplikacije in s tem uporabnika. Povezujemo uporabnike, uporabnike in računalnike ter računalnike med seboj. Sama povezava računalnika z računalnikom je le droben tehničen detajl, ki je orodje za

izpolnitev osnovnega cilja, to je povezovanja ljudi z računalniki in med seboj. Povezava med uporabniki je implementirana z množico informacijskih funkcij, ki omogočajo podatke zbirati, hraniti in do njih dostopati, ter množico funkcij komunikacijskega sistema, ki omogočajo podatke prenašati med različnimi informacijskimi okolji. Uporabnik je človek, ki komunicira oziroma je povezan z računalniškim informacijskim sistemom prek različnih vhodno-izhodnih enot. Komunikacijske storitve so specializirana oblika aplikacij, ki jih uporabnik dosega posredno prek informacijskega okolja. Na področju komunikacij je trend, ki zasleduje končni cilj - mobilnost, ki naj omogoči prave podatke ob pravem času na pravem mestu.

2.3.2. Komunikacije v zdravstvu

V zdravstvu potekajo komunikacije, tako znotraj same ustanove, med ustanovo in državljanom, drugo zdravstveno ustanovo, z dobavitelji, upravljavcem sistema in ustanovo, s katero se komunicira za namene poročanja (npr. IVZ – Inštitut za varovanje zdravja) in plačil (npr. ZZZS – Zavod za zdravstveno zavarovanje Slovenije). Primer komunikacij v zdravstvu prikazuje Slika 2: Del komunikacij v zdravstvu.

Slika 2: Del komunikacij v zdravstvu



Vir:Planinc & Šorli & Kralj & Fuart &Slavec, Elektronski zapis podatkov o pacientu – pridobitve in dileme, 2004, str. 219.

Subjekti/uporabniki zdravstveno informacijskega sistema (Popovič et al., 2007):

- izvajalci storitev (bolnice, zdravstveni domovi, zdravstveno osebje, lekarne, dobavitelji medicinsko tehničnih pripomočkov, ...),
- zavarovalnice (ZZZS, Adriatic, Vzajemna, Triglav, ...),
- vladne in nevladne organizacije (Ministrstvo za zdravje, IVZ, ...),
- zavarovanec/uporabnik storitev.

Opazovanje posameznih segmentov komunikacij znotraj ustanov, med ustanovami in z drugimi organizacijami ali posamezniki nam lahko poda informacije o ozkih grlih, nevarnostih in priložnostih za izboljšave.

Infrastruktura predstavlja le potreben, ne pa zadostnega pogoja za delovanje informacijske družbe. Nedvomno je bistvo informacijske družbe v »znati koristno uporabljati«, ne samo v »imeti tehnologijo«. Drugo zelo kritično področje pa so vsebine. Vlade naprednih držav se vse bolj zavedajo pomena telekomunikacij za družbeni in gospodarski razvoj družbe. Slovenska informacijska infrastruktura določa evolucijo sedanjih omrežij v smeri vzajemno delujočih omrežij za vse storitve. Zagotoviti mora uporabo telekomunikacijskih storitev, temelječih na odprtih aplikacijah, ki posredujejo in obdelujejo vse vrste informacij kjerkoli in kadarkoli. Bistven pomen in smisel vsej infrastrukturi pa bodo dale storitve, aplikacije in vsebine. Usmeritev temelji na povezovanju obstoječih omrežij in optimizirani uporabi vsakega izmed njih. Dostop bo zaradi ekonomskih, geografskih in tržnih razlogov ter različnih potreb uporabnikov izveden z različnimi tehnologijami. Za delovanje vseh komponent informacijske infrastrukture je potrebno upravljanje in nadzor sistema ter storitev. Poleg vlaganj v opremo je treba vlagati tudi v razvoj aplikacij, storitev in vsebin. Glede na to, da se poudarek v komunikacijah iz infrastrukture in sistemov seli na aplikacije in vsebine, je odsotnost le-teh v okviru komunikacijskega sistema nedopustna (Bešter & Kos, 2001).

2.3.3. Lokalna računalniška omrežja

Lokalna omrežja povezujejo naprave in uporabnike, ki so si krajevno blizu (stavba ali več stavb) in medsebojno paketno komunicirajo. Njihov pomen je ključen za učinkovitost delovanja ustanove, saj omogoča skupno rabo naprav, aplikacij, podatkovnih baz, komunikacijo med uporabniki, racionalno rabo komunikacij navzven in še bi lahko naštevali. Tehnološka zmogljivost in arhitektura lokalnih omrežij je pomembna iz več vidikov. Z naraščanjem števila uporabnikov in aplikacij narašča promet v omrežju, zato

lahko to postane ozko grlo v komunikaciji. Glede na to ali lokalno omrežje fizično povezuje koaksialni vodnik, parica, optični vodnik ali je brezžično, nastopajo drugačna varnostna tveganja, možnosti in zmogljivosti.

V anketi sem ustanove povprašal:

- kolikšno hitrost omogoča njihovo lokalno računalniško omrežje,
- koliko računalnikov v ustanovi je priključenih v lokalno računalniško omrežje,
- koliko računalnikov v ustanovi ima dostop do interneta,
- katero tehnologijo uporabljajo za dostop do interneta,
- kakšna je hitrost internetne povezave (sprejem podatkov - angl. *Download*),
- kakšna je hitrost internetne povezave (pošiljanje podatkov - angl. *Upload*),
- na koliko lokacijah delujejo,
- kako so lokacije med seboj povezane,
- ali obstoječa oprema omogoča oddaljen dostop?

Na promet v omrežju in njegovo prepustnost lahko sklepamo iz števila računalnikov, ki so priključena v lokalno računalniško omrežje in uporabljene tehnologije. Iz števila računalnikov, ki ima dostop do interneta in hitrosti internetne povezave, lahko izračunamo povprečno hitrost, ki je na voljo posameznemu računalniku pri dostopu do interneta. Glede na to, kakšno tehnologijo ustanova uporablja za dostop do interneta, lahko sklepamo na možnosti širitev oziroma omejitev, s katerimi se bodo ustanove srečevale.

Poleg nekoč najpomembnejšega parametra hitrosti internetne povezave, sprejema podatkov pa z aplikacijami, ki zahtevajo simetrično komunikacijo (npr. videokonference), postaja čedalje pomembnejši podatek tudi hitrost internetne povezave za pošiljanje podatkov.

Ustanove, ki imajo dislocirane enote, so z njimi lahko povezane ali pa tudi ne. V kolikor imajo ustanove enote med seboj povezane, gre lahko za povezave in tehnologije v smislu lokalnega omrežja ali pa gre za povezave preko interneta. Vsak način prinaša s seboj nekoliko drugačne tehnologije in organizacijo dela, pa tudi vprašanja, povezana z varnostjo.

2.3.4. Komunikacije med izvajalci zdravstvenih storitev

V Sloveniji do danes formalno ni vzpostavljenega elektronskega sistema komunikacije, enotne vstopne točke in določenih standardov za izmenjavo podatkov med ustanovami. Kljub temu, da sta Odbor za zdravstveno informacijske standarde in Svet za informatiko ustanovljena že dve leti, rezultatov žal še nista pokazala.

Menim, da za tehnološko izvedbo ni ovir, kar kažejo primeri dobrih praks Danske, Finske, Nizozemske in nekaterih drugih držav (Popovič et al., 2007). Torej je lahko problem predvsem v volji, ki vodi do reorganizacije procesov. Kako zadeve potekajo sedaj in kakšne so priložnosti? Za primer si poglejmo problem pomanjkanja kadrov na področju radiologije (Kondža, 2008). Digitalizacija in teleradiologija ponujata z ustrezno organizacijo in motivacijo vključenih rešitev za pridobitev drugega mnenja, rešitev problema pomanjkanja radiologov specialistov, zniževanje stroškov dela, boljšo izkoriščenost strokovnega kadra in večjo dostopnost strokovnjakov tudi geografsko bolj oddaljenim ustanovam (Kadivec, 2007).

Seveda ne bom mogel prikazati vseh priložnosti izboljšav, ki jih v procese dela lahko prinese informacijska tehnologija, niti to ni namen naloge. Nekatere države npr. Danska preko svojega portala www.sundhed.dk zdravstvenim strokovnjakom nudijo:

- komuniciranje s pacienti,
- dostop do EZZ lastne in drugih ustanov,
- dostop do laboratorijskih rezultatov,
- vpogled v pacientovo farmakoterapijo in kompatibilnost zdravil,
- predstavitev lastne enote, prakse,
- informacije o zdravstvenih strokovnjakih,
- nacionalna klinična vodila,
- podporo kliničnim potem,
- ponudbo prostih delovnih mest.

Gotovo se bodo s povečanjem komunikacij med izvajalci zdravstvenih storitev povečala tveganja kraje in razkritja zdravstvenih podatkov. Rešitev iščejo države v graditvi zdravstvenih omrežij npr. Švedska Sjunet (Larson & Malmqvist, 2003). Razlogi pa so tudi v standardizaciji in stroškovni učinkovitosti. Zato sem anketirane ustanove povprašal tudi, ali bi jih vključitev v nacionalno zdravstveno informacijsko omrežje zanimala.

Uporaba Danskega zdravstveno podatkovnega omrežja, kamor so povezane ustanove preko VPN (angl. *Virtual Private Network*) povezav z MedCom, je zelo visoka: 97% splošnih zdravnikov, 74% specialistov, 100% bolnišnic in lekarn, 44% lokalnih avtoritet. Preko omrežja se trenutno izvajajo naslednje storitve eZdravja: izmenjava napotnic in odpustnih pisem, pošiljanje receptov, teleradiologija – teledermatološka storitev, vpogled v laboratorijske izvide preko Nacionalnega zdravstvenega portala (Popovič et al., 2007).

2.3.5. Komunikacije za namene poročanja, upravljanja in fakturiranja

Pravočasne in natančne informacije so za uspešno upravljanje zdravstvenega sistema vse bolj pomembne. Zato narašča pomen komunikacij ustanov z vladnimi in nevladnimi organizacijami (MZ, IVZ RS, ...). Trenutno komunikacija Ministrstva za zdravje (MZ) z zdravstvenimi ustanovami poleg papirne, telefonske in osebne komunikacije, poteka z uporabo elektronske pošte ter spletne strani. Inštitut za varovanje zdravje RS (IVZ RS) zbira podatke na zelo različne načine, odvisno od posamezne zbirke. Tehnološko najsodobneje zasnovana aplikacija je eSPP, namenjena zbiranju podatkov skupin primerljivih primerov (SPP). Sistem SPP je način razvrščanja bolnikov, za katere porabimo podobno količino virov, podlaga za razvrščanje bolnikov pa so statistične analize kliničnih podatkov in podatkov o porabi virov velikih vzorcev bolnikov. V anketo sem zajel tudi IVZ RS, saj je pošiljanje statističnih podatkov ustanov na Inštitut za varovanje zdravja RS, za fakturiranjem, drugo najpogostejše pošiljanje podatkov. Izmenjava podatkov med zdravstvom in državno upravo poteka precej pogosto. Podatki vsakega od nas se izmenjajo najmanj ob rojstvu in ob smrti (Gaspari & Anžur & Kravanja, 2006).

Poleg uporabe elektronske pošte največ ustanov izmenjuje podatke v elektronski obliki za namene fakturiranja z Zavodom za zdravstveno zavarovanje Slovenije (ZZZS). Ker ima ZZZS vzpostavljen svoj komunikacijski sistem, zavarovalnic nisem vključil v anketo.

2.3.6. Komunikacije zdravstvenih ustanov s posamezniki

V zadnjih desetletjih je bil napredek medicinske znanosti in medicinske tehnologije zelo hiter, po zaslugi razvoja informacijske tehnologije pa so podatki o tem dostopni ne le izvajalcem zdravstvene dejavnosti temveč tudi uporabnikom - državljanom. Ljudje so vse bolj zdravstveno osveščeni; aktivno iščejo informacije, kako bi ohranjali in krepili zdravje in še zlasti, kakšne možnosti jim v primeru bolezni nudijo medicina in spremljajoče

znanosti. Z uporabo možnosti, ki jih nudijo sodobne informacijsko komunikacijske tehnologije, lahko z vključevanjem zainteresirane javnosti poiščemo odgovore na nekatere izzive, s katerimi se srečuje zdravstvo. Na primer odgovor na izzive starajočega prebivalstva in pomanjkanja zdravnikov lahko ponudijo nekatere storitve, ki jih ponuja telemedicina in teleoskrba. Telemedicina je nudenje medicinske oskrbe, kjer je premagovanje razdalje prevladujoč faktor. Področje telemedicine se nanaša na povezavo med bolnikom in zdravstvenim osebjem s pomočjo informacijsko komunikacijske tehnologije. Wilson in soavtorja (2004) poudarjajo pomen komunikacij in uporabe sodobnih informacijskih orodij in storitev za opolnomočenje posameznikov. Pogoj za uporabo teh storitev so primerna stopnja razvitosti elektronskega poslovanja zdravstvenih ustanov in razširjenost uporabe interneta med posamezniki. Po raziskavi RIS 2007 Uporaba interneta je v Sloveniji v populaciji od 10 do 75 let 63% uporabnikov interneta oziroma 1.057.893 prebivalcev. V raziskavi navajajo, da je bil v letu 2006 po podatkih Eurostata delež slovenskih tedenskih uporabnikov enak povprečnemu deležu tedenskih uporabnikov EU25 (47%). V letu 2007 je Slovenija z 49% tedenskih uporabnikov ponovno zaostala za povprečjem EU25 (53%) v populaciji 16 do 74 let, še bolj pa zaostaja za EU15 (55%), (Vehovar & Brečko, 2007). Menim, da je kljub navedenim zaostankom v primerjavi s povprečji EU ozko grlo stopnja razvitosti elektronskega poslovanja zdravstvenih ustanov.

Z anketnimi vprašanji sem poizkušal ugotoviti, koliko ustanov ima svojo spletno stran in katere funkcionalnosti obiskovalcu nudijo. Nekatere države, npr. Danska, preko svojega portala www.sundhed.dk državljanom z digitalnim spletnim potrdilom nudijo naslednje storitve:

- osebna zdravstvena spletna stran,
- komunikacija z zdravstvenim sistemom,
- naročanje na obisk pri osebnem zdravniku,
- naročanje zdravil pri apotekah,
- ponovni recept,
- informacija o kompatibilnosti zdravil,
- informacija o določenem zdravilu,
- vpogled v naročenost za zdravstvene storitve,
- opominjanje na termine naročenosti,
- iskanje specifičnega, relevantnega strokovnjaka,

- preverjanje najkrajšega čakalnega časa za operacije,
- varno pošiljanje e-sporočil zdravstvenim institucijam,
- vpogled v obravnave in diagnoze lastnega EZZ,
- registracija donatorja organov,
- vpogled v predstavitve zdravstvenih izvajalcev,
- zdravstveno relevantne informacije.

2.4 Procesi in aplikacije

Uporaba sodobnih informacijskih in komunikacijskih tehnologij (IKT) lahko pomembno poveča učinkovitost zdravstvenega sistema in kakovost storitev (Kaushal & Shojania & Bates, 2003). Da bi uporabnik lahko uporabljal dobrobiti IKT, mu mora biti na voljo dobro opredeljena aplikacija, ki ga prijazno vodi k cilju. Potrebno je zagotoviti, da bo sistem za uporabnika obvladljiv in da ga bo znal izkoriščati brez pretiranega specialističnega znanja. Če želimo, da bo privzemanje sodobnih IKT s strani izvajalcev zdravstvenega varstva in zdravstvenih delavcev potekalo hitro, je zanj potrebno zagotoviti orodja, znanje in veščine, motivacijo ter prilagojeno organizacijo procesov (Meglič et al., 2007a). Na privzemanje IKT vplivajo tudi drugi dejavniki. Za primarno zdravstveno varstvo jih je že leta 1994 opisal (Dixon & Dixon, str 631-635). Zdravstvenemu osebju morajo biti na voljo orodja za delo s podatki (vnos, obdelava, prikaz), izmenjavo podatkov in komunikacijo znotraj posameznega izvajalca (med oddelki, z laboratorijem ipd.), med izvajalci (npr. recepti, napotitve, slikovno in drugo gradivo), med izvajalci in uporabniki zdravstvenih storitev (naročanje, odpustna pisma, telemedicina ipd.). Zdravstveno osebje mora hkrati posedovati znanje in spretnosti za uporabo obstoječih orodij, da lahko izrabi polno funkcionalnost orodij. Velik pomen ima tudi motivacija uporabnikov.

S strani upravljavca sistema lahko na motivacijo vplivamo s spodbudami, na primer z nagradami, prisilo ali moralnimi obvezami. Spodbude lahko delimo na neposredne in posredne. Z neposrednimi spodbudami upravljavec sistema vpliva neposredno na izvajalce. Delimo jih lahko naprej na nagrajevalne in prisilne. Nagrajevalne (običajno finančne) spodbude lahko neposredno vežemo na uporabo IKT. V splošnem so te spodbude učinkovite, lahko pa si predstavljamo, da obstaja pomembna razlika med učinkovitostjo spodbude, če se nagrajujejo izvajalci ali osebje neposredno, kar je bolj zahtevno. Primer dobre prakse s področja neposrednih finančnih spodbud je uvedba nacionalnega

elektronskega zdravstvenega kartona IZIP na Češkem (www.izip.cz), kjer je finančno nagrajevanje pomembno prispevalo k začetni uvedbi rešitve. Zdravnik namreč za vsak vnos podatkov v IZIP prejme plačilo, sredstva pa posredno zagotavlja zdravstvena zavarovalnica. Naslednja kategorija so t.i. prisilne spodbude, ki so običajno pravne narave. Primer je lahko obvezna uporaba elektronskega zdravstvenega kartona za vodenje bolnikove dokumentacije. Te spodbude so zelo učinkovite, vendar morajo biti prej zagotovljeni pogoji za izpolnjevanje zahtev. Tak primer sta Madžarska in Slovenija, kjer je elektronsko poročanje zavarovalnici predpisano s pravilnikom kot pogoj za plačilo storitev. Posredne spodbude pa izvajalci občutijo zaradi drugih dejavnikov, na katere upravljavec sistema ne more neposredno vplivati. Primer je zadovoljstvo uporabnikov in njihova pričakovanja do izvajalcev zdravstvenih storitev. Posredne spodbude delimo na organizacijske vzpodbude in zahteve s strani uporabnikov. Organizacijske spodbude imajo podoben končni učinek kot nagrajevalne, saj z IKT podprta prenovljena organizacija dela omogoča zdravnikom manj napak in stresa pri delu ter večjo učinkovitost. Upravljavci sistema lahko posredno vplivajo na privzemanje IKT s sofinanciranjem ali brezplačnim ponujanjem tovrstnih rešitev, vendar mora na strani izvajalcev in osebja obstajati interes po povečanju učinkovitosti dela. Tudi zahteve s strani uporabnikov zdravstvenega sistema so učinkovita in stroškovno sprejemljiva metoda spodbujanja, kjer ločimo dva vidika: na eni strani osveščanje uporabnikov zdravstvenega sistema o prednostih IKT ustvari pritisk na zdravnike s strani posameznih uporabnikov, na drugi strani pa opolnomočenje uporabnikov omogoča nadzorovanje poteka njihove lastne oskrbe v zdravstvenem sistemu v primerjavi z normativno oskrbo (Wilson & Leitner & Moussalli, 2004). Tehnologija brez ustrezne organiziranosti ljudi in opolnomočenja delavcev lahko proces dela tudi zavre in pri odjemalcih povzroči več slabega kot dobrega. Obstajajo še druge spodbude, kot je masovni učinek izvajalcev ali zaposlenih, ki uporabljajo določeno tehnologijo, ki postane prevladujoča in nadomesti prejšnjo.

Pri anketnih vprašanjih sem spraševal po zaposlenih po posameznih profilih in zaposlenih, ki pri svojem delu uporabljajo računalnik po posameznih profilih. Na ta način sem želel ugotoviti, koliko zaposlenih po posameznih profilih pri svojem delu uporablja računalnik. Ta kazalec lahko vsaj približno primerjamo z nekaterimi tujimi raziskavami.

Elektronski zdravstveni zapis je mogoče res najpomembnejši element zdravstvenega informacijskega sistema, ne moremo pa reči, da je edini. Nekateri »nezdravstveni« profili, kot npr. zaposleni v računovodstvu, ga tudi nikoli ne bodo uporabljali, vendar lahko tudi njim sodobne informacijske tehnologije omogočijo učinkovitejše delo.

Procesi dela se razlikujejo tako ali gre za primarno, sekundarno ali terciarno raven kot tudi glede na posamezno specialnost. Lahko poskusimo oblikovati nek splošen proces, iz katerega lahko sklepamo na aplikacije, ki jih ima ali jih bo nekoč želela imeti vsaka ustanova.

Ko posameznik potrebuje obisk v zdravstveni ustanovi, se želi naročiti na obisk. Pri naročanju nastajajo čakalne vrste. Ob obravnavi pacienta se v njegovo kartoteko zapisujejo ali iz nje berejo določeni podatki. Pri postavljanju diagnoze in spremljanju poteka zdravljenja se pacienta napoti na različne teste in slikanja. Po potrebi se opravijo tudi napotitve k različnim specialistom. Slike (rentgen - RTG, EKG, CT,...) si izvajalci storitev izmenjujejo in se o njih posvetujejo ali se o postavljeni diagnozi pridobi tudi drugo mnenje. Izvajalci med seboj komunicirajo s pomočjo različnih komunikacijskih naprav. Po zdravljenju pacient dobi odpustno pismo, plačniku se pošlje faktura, na ustanove, ki zbirajo podatke za statistične in druge namene pa kot določeno redna poročila.

Glede na tip, vrsto ustanove in uporabe računalnikov po posameznem profilu lahko pridemo do zanimivih odgovorov na vprašanja:

- ali je računalnik bolj dostopen posameznemu profilu v javnem ali zasebnem sektorju? Je zato različna učinkovitost?
- se stopnja uporabe med posameznimi profili razlikuje?

Zaradi obsega ankete bom z vprašanji poskusil ugotoviti, katere aplikacije ustanove uporabljajo in s tem izmenjujejo podatke, ter katere nameravajo začeti uporabljati. Sprašujem predvsem po aplikacijah, katerih funkcionalnosti večina uporablja oziroma potrebuje:

- naročilo laboratorijskih testov,
- napotnice,
- odpustna pisma,
- fakturiranje,
- statistika (npr z IVZ, SURS,...),
- elektronski karton pacienta,
- izmenjava digitalnih RTG slik,
- posvetovanja/ videokonference (zvok in slika),
- izmenjava kardioloških slik, EKG, ...
- VoIP - uporaba informacijskega omrežja za prenos zvoka, telefonske storitve, ...
- naročanje pacientov preko spleta in čakalne liste.

Ker je področje zdravstva zelo široko, je tudi aplikacij ogromno. V nadaljevanju bom nekoliko podrobneje predstavil elektronski zdravstveni zapis in uporabo elektronske pošte za posvet z zdravstvenim osebjem.

2.4.1. Elektronski zdravstveni zapis

Med medicinske zapise lahko prištejemo (Ilijaž, 2005): vse rokopise in papirnate zapiske, računalniške zapise, zdravniške izvide in odpustna pisma, izvide laboratorijskih in drugih preiskav, rentgenske in slike ultrazvoka in vse ostale slikovne medicinske zapise, fotografije, zvokovne in videoposnetke, ter različne izpiske medicinske opreme (EKG, …). Eden najpogostejših izrazov, ki pokriva najpomembnejši element zdravstvenega sistema – pacienta, je elektronski zdravstveni zapis. Elektronski zdravstveni zapis - EZZ je po definiciji tehničnega komiteja (TC) 215 pri mednarodni organizaciji za standardizacijo, ISO/TC 215 (www.prorec.si): repozitorij informacij v zvezi z zdravjem subjekta zdravstvene oskrbe v računalniško berljivi obliki. Trenutno imajo bolnice implementirane nepopolne elektronske zdravstvene zapise. Razvoj se je začel v šestdesetih letih prejšnjega stoletja z željo po izboljšanju interne komunikacije in zajemu stroškov. Od tedaj je nastalo precej definicij, ki naj bi opredeljevale nekaj, kar lahko imenujemo podatki o pacientu (angl. *Patient data file*). Četudi vse zajemajo podatke o pacientu in zdravstveno administrativne podatke, pa se razlikujejo glede na to ali zajemajo podatke samo ene institucije, izbranih institucij ali ciklusa zapisa s podatki iz vseh vpletenih institucij. Zato so si pogosto nasprotujoče, zavajajoče in nejasne. Evropska komisija v svojem poročilu predstavi pet nivojev računalniške podprtosti zdravstvenih informacijskih sistemov od najmanj do bolj sofisticiranega (European Commission, 2008, str.25-27):

- avtomatizirani medicinski zapis (angl. *Automated Medical Records*, AMR),
- računalniško podprt medicinski zapis (angl. *Computerized Medical Records* CMR),
- elektronski medicinski zapis (angl. *Electronic Medical Records*, EMR),
- elektronski zapis o pacientu (angl. *Electronic Patient Records*, EPR),
- elektronski zdravstveni zapis (angl. *Electronic Health Records*, EHR).

Teh pet nivojev lahko združimo v elektronsko datoteko pacienta, nivoji od 1-3 in v elektronski zdravstveni zapis, nivoja 4-5, predvsem glede interoperabilnosti (Tabela 1: Razvoj elektronskega zdravstvenega zapisa).

Tabela 1: Razvoj elektronskega zdravstvenega zapisa

Elektronska datoteka pacienta	Nivo 1	Avtomatizirani medicinski zapis	Večina današnjih sistemov sodi v to kategorijo. Informacije o pacientu so še vedno pretežno v papirnati obliki. Na njem temeljijo nekatere računalniško podprte funkcije: - sprejem, odpust, premestitev, - obračun stroškov zdravljenja, - laboratorijski inform. sistemi, …
	Nivo 2	Računalniško podprt medicinski zapis	Informacije nastajajo v papirnati obliki. Digitalizacija medicinskih zapisov poteka s pomočjo skeniranja papirne dokumentacije in uvoza digitalnih datotek. Struktura in izgled sta podobna papirnim kartotekam, ni uporabe prepoznavanja pisav (OCR), temveč samo slike. Dokument je potrebno poskenirati kot eno sliko skupaj z datumi in podpisi.
	Nivo 3	Elektronski medicinski zapis	Je nadgradnja prejšnjega tipa zapisa. Podatki se neposredno vnašajo v računalnik v obliki, ki je primerna za raznovrstno poznejšo uporabo. Digitalni medicinski zapis je že vključen v organizacijo in procese, ki so podprti z informacijsko tehnologijo. Omogočena je podpora odločanju in menedžment podatkov. Uspešna uporaba temelji na naslednjih pogojih: - prijaznost do uporabnika, - sprejemanje pri uporabnikih, - zasnova sistema in funkcionalnost.
Elektronski zdravstveni zapis	Nivo 4	Elektronski zapis o pacientu	Vsebuje vse za bolezensko stanje pacienta relevantne podatke, ne glede na ustanovo v regiji. Obstoji možnost telemedicine in sistema raziskovalnih omrežij. Možen je dostop do vseh podatkov o pacientu v organizaciji. Zaščita in varnost podatkov se vrši s kontrolo dostopa in elektronskim podpisom. Možna je integracija z ekspertnimi programi: - elektronski priročniki, - diagnostični programi, - pomoč pri izbiri in doziranju zdravil.
	Nivo 5	Elektronski zdravstveni zapis	Združuje zdravstvene informacije, ki izhajajo iz različnih organizacij in se nanašajo na eno osebo. Z uporabo spletnih tehnologij so podatki vedno dostopni ne glede na lokacijo v svetu. Pri nastajanju zapisa posamezniki sodelujejo. Vsebuje širšo množico podatkov, kot elektronski medicinski zapis, tudi podatke, ki niso neposredno povezani z zdravljenjem kot npr. ali oseba kadi, ali se ukvarja s športom, … Na podlagi zbranih in urejenih podatkov omogočeno merjenje stroškovne učinkovitosti, prepoznavanje dobre prakse, vodenje raznih indikatorjev kakovosti, varnosti in učinkovitosti, (Englebardt & Nelson, 2002).

Vir: *European Commission, 2008, str. 25*

Elektronska datoteka pacienta običajno vsebuje medicinske podatke o enem pacientu v eni ustanovi. V tem primeru o uporabi standardov za interoperabilnost ne moremo govoriti. Dokumenti elektronskega zdravstvenega zapisa ustrezajo zahtevam interoperabilnosti in niso omejeni na eno ustanovo. To pomeni, da izraz elektronski zdravstveni zapis zajema datoteko, ki ni omejena na eno ustanovo in zajema vse relevantne podatke. Bolj kot množica izrazov je pomemben cilj, ki ga želimo doseči, ki ga predstavljata peti nivo in pravo elektronsko poslovanje.

2.4.2. Elektronska pošta

Poleg uporabe interneta je elektronska pošta gotovo najbolj razširjena storitev med uporabniki informacijsko komunikacijskih tehnologij. Ravno zaradi velike razširjenosti je zanimivo, kako je z njeno primernostjo za posvet z zdravstvenim osebjem. Nekatere prednosti in slabosti prikazuje Tabela 2: Nekatere prednosti in slabosti elektronskega posveta. Več različnih možnosti za posvet z zdravnikom in zdravstvenim osebjem povečuje dostopnost zdravstvene oskrbe. Elektronska pošta med uporabnikom zdravstvene storitve in izvajalcem je opredeljena kot komuniciranje preko računalnika ob v naprej opredeljenih pogojih, pri čemer ponudnik elektronske zdravstvene storitve prevzame določeno odgovornost za ustreznost tovrstne zdravstvene oskrbe (Kane & Sandz, 1998). Izmenjava podatkov po elektronski pošti ne sodi le med zdravstvene storitve, temveč tudi med storitve informacijske družbe (Ilijaž, 2007, str. 28). Zdravnik bi moral posebno pozornost posvetiti ugotavljanju ali je takšna obravnava primerna pri konkretnem problemu. Elektronska komunikacija je namreč primerna samo za nenujna stanja, nezapletene zdravstvene težave in za zdravstveno vzgojo in preventivo. Kadarkoli bi bil zdravnik v dvomih, bi moral uporabniku takšne zdravstvene storitve svetovati tudi ambulantni posvet.

Glede na prednosti in slabosti ter dejstvo, da je elektronska komunikacija primerna predvsem za nenujna stanja, izobraževanje in podobno, je razumljiv razmah forumov z zdravstveno vsebino, kot je na primer www.med.over.net. Večji razmah elektronskih posvetovanj lahko pričakujemo, ko bo širokim množicam dosegljiva oprema za videokonference in jo bodo znali uporabljati. Pri videokonferencah odpadejo nekatere slabosti, zdravnik pa pridobi dodatne informacije preko zvoka in slike. Potrebno pa bo rešiti tudi problem plačevanja takšne storitve.

Tabela 2: Nekatere prednosti in slabosti elektronskega posveta

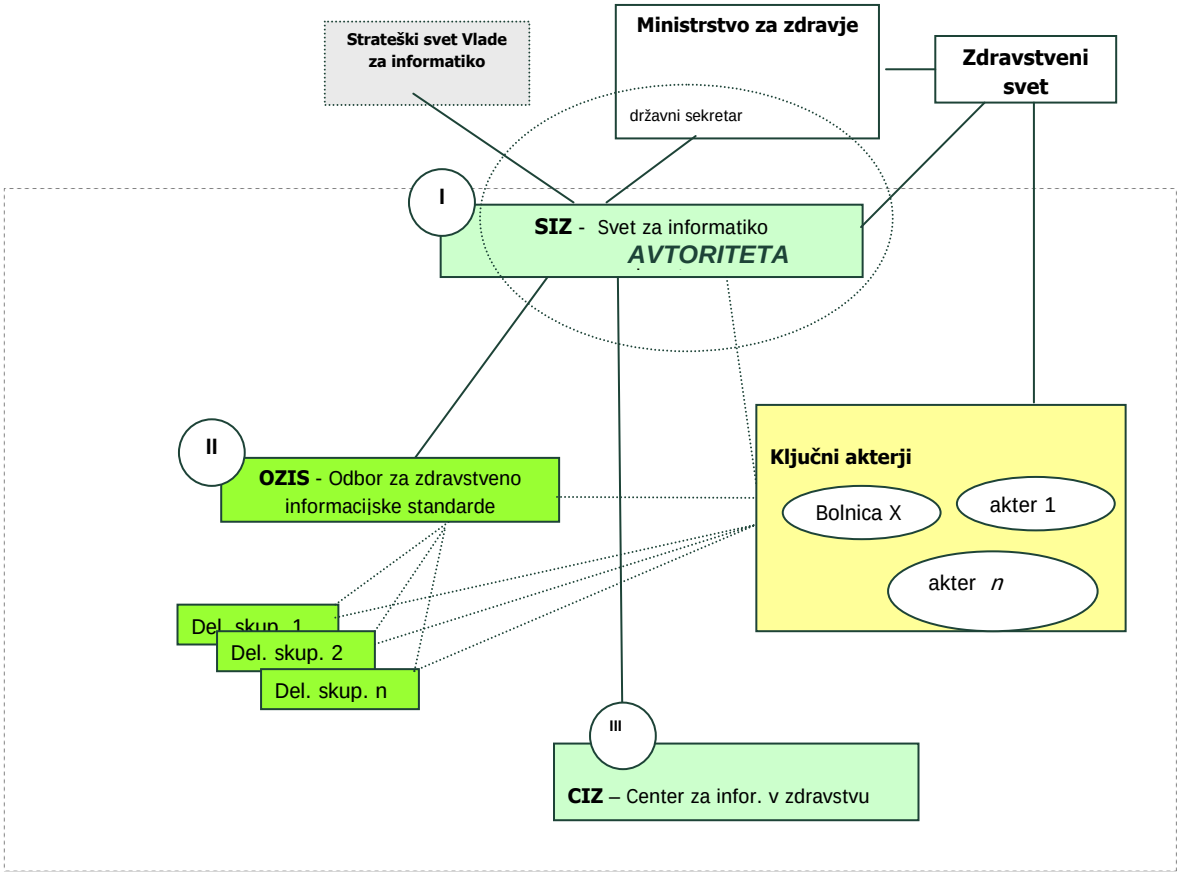
Pridobitve	Slabosti in nevarnosti
Udobnost - zmanjšanje potrebe po neposrednem stiku, - časovna in krajevna neomejenost.	- tehnološka zahtevnost in visoki varnostni standardi.
Dostopnost - ni nezadovoljstva zaradi številnih neuspešnih telefonskih klicev.	- nevarnost socialne diskriminacije.
Informiranje - večja možnost za hitro obveščanje, - bolniku pomembnih informacij ni potrebno zapisovati (npr. navodila za jemanje zdravila, naslovi, navodila pred operacijo,...).	- nevarnost nepooblaščenga dostopa in poseganja v bolnikovo zasebnost.
Zadovoljstvo uporabnika - hitrejši dostop do zdravnika, - možnost anonimnega posveta, - komunikacija brez tradicionalnih predsodkov (starost, spol,..).	- nevarnost preobremenitve zdravnika s številom in obsegom e-pošte.
Kakovost oskrbe - elektronski posvet predstavlja koristen dodatek k opravljenemu ambulantnemu pregledu, - predvsem za spremljanje in dodatna pojasnila, - odgovori, ki jih zapišemo v e-pošti so bolj pretehtani.	- ne omogoča pregleda bolnika, - ne omogoča empatične komunikacije (barva glasu, pogled, dotik), - otežena je emotivna podpora bolniku, - povišano tveganje za diagnostične in terapevtske spodrsljaje.
Učinkovitost - možnost zniževanja stroškov oskrbe, - možnost posredovanja obvestil več bolnikom hkrati (npr. o odsotnosti, ...).	- nevarnost prepočasnega odgovora na potencialno nujna stanja.

Vir: Car & Sheikh, 2004

2.6 Nacionalne entitete in načrti

Aktivnosti Ministrstva za zdravje glede realizacije strateških ciljev zadanih v Strategiji eZdravje 2010 se kažejo v vzpostavitvi entitet, ki bodo skrbele za trajnostni razvoj informatike v zdravstvu v Sloveniji. Svet za informatiko v zdravstvu (v nadaljevanju SIZ ali Svet) je ključna komponenta nacionalne informacijske strukture zdravstvenega sektorja poleg Centra za informatiko v zdravstvu (v nadaljevanju CIZ) in Odbora za zdravstveno informacijske standarde (v nadaljevanju OZIS). CIZ (oz. do njegove vzpostavitve Projektna enota za CIZ) je center, ki vodi in koordinira večino strokovnih nalog oziroma dela na področju informatike, potrebnega za podporo slovenskemu zdravstvenemu sistemu na nacionalni ravni. Povezave med entitetami informatike v zdravstvu Slovenije prikazuje Slika 3: Povezave med entitetami.

Slika 3: Povezave med entitetami



Vir: Kodele et al. ,2005, str 29.

Ministrstvo za zdravje v letnem načrtu razvoja nacionalne zdravstvene informatike za obdobje julij 2008 do december 2009 predvideva:

- aktivnosti na vzorčnih rešitvah za projekt eZdravje:
  - pripravljalne aktivnosti za uporabo omrežja HKOM;
  - vzorčna rešitev 1: Izmenjava digitalne dokumentacije;
  - vzorčna rešitev 2: Čakalne vrste – kvalitetno upravljanje lokalnih čakalnih vrst in usklajeno poročanje;
  - vzorčna rešitev 3: e-naročanje;
  - vzorčna rešitev 4: zdravstveni portal.
- aktivnosti za realizacijo celovitega projekta eZdravje,
- aktivnosti spremljanja projektov v teku (Projekt prenove KZZ in Online).

Menim, da ima Slovenija s svojo majhnostjo prednost pred velikimi državami, saj lahko določene projekte namesto dolgotrajnih pilotnih faz izvede na celotnem področju države v precej krajšem časovnem obdobju. Evropska komisija vidi prednost v centralizirani vlogi, ki jo je pri razvoju informatike v zdravstvu imela ZZZS in to stanje primerja z NHS (National Health Service) v Angliji (European Commission, 2004).

2.7 Svet za informatiko v zdravstvu

Iz Temeljne listine za ustanovitev Sveta za informatiko v zdravstvu in Poslovnika Sveta za informatiko v zdravstvu lahko povzamemo, da je Svet za informatiko v zdravstvu (SIZ) pooblaščen za oblikovanje usmeritev in določanje prioritetnih nacionalnih aktivnosti v zvezi z zdravstveno informatiko, vključno z nalogami Odbora za zdravstveno informacijske standarde (OZIS) in Centra za informatiko v zdravstvu (CIZ). Področje dela Sveta obsega vse aktivnosti na področju zdravstvene informatike na nacionalni ravni, ki so skupne vsem službam in ustanovam v okviru zdravstvenega sistema. Področje dela Sveta ne vključuje tistih aktivnosti s področja zdravstvene informatike, ki so lastne zgolj posamezni službi oz. ustanovi. Svet ima 14 članov, ki zastopajo različne akterje v sistemu. Svet najmanj enkrat letno posreduje ministru za zdravje predlog za izvedbo projektov eZdravja. Izvedbo projektov eZdravja odobri minister za zdravje na predlog SIZ s sklepom. Svet se sestane najmanj 4 krat letno oziroma takrat, kadar je potrebno opredeliti usmeritve nacionalnih dejavnosti na področju informatike, proučiti predloge, povezane s področjem informatike ali oceniti napredek glede na sprejete načrte.

2.8 Odbor za zdravstveno informacijske standarde

Na spletni strani Ministrstva za zdravje najdemo različne dokumente iz katerih o OZIS dobimo naslednje informacije. Odbor je organ, odgovoren za postopek oblikovanja in obvladovanja informacijskih standardov oziroma drugih normativnih dokumentov, potrebnih v slovenskem zdravstvenem sistemu. Odbor je krovno strokovno telo na področju standardov v zdravstveni informatiki, ki Svetu podaja priporočila glede standardizacije zdravstvene informatike. Sestavlja ga 11 članov in deluje na sejah, ki so praviloma enkrat vsaka 2 meseca oziroma takrat, kadar je potrebno opredeliti usmeritve dejavnosti na področju nacionalnih informacijskih normativnih dokumentov, proučiti predloge za informacijske normativne dokumente ali oceniti z normativnimi dokumenti

povezane dejavnosti. Njegova naloga je, da zagotavlja razvoj in obvladovanje tistih zdravstveno informacijskih normativnih dokumentov, ki so pomembni za vse sodelujoče v zdravstvenem sistemu z naslednjih vidikov:

- sistemsko-vsebinski vidik (opredeljevanje in sprejemanje zdravstvenih konceptov, informacijskih modelov, normativnih dokumentov s področja metapodatkovnih registrov, klasifikacij, šifrantov ipd.),
- vidik zaščite, varnosti in kakovosti (opredeljevanje in sprejemanje priporočil, normativnih dokumentov in navodil za zaščito, varnost in kakovost informacijsko komunikacijske tehnologije in zdravstvene informatike v slovenskem zdravstvu),
- komunikacijski vidik (opredeljevanje in sprejemanje priporočil, normativnih dokumentov in vodil za učinkovito izmenjavanje sporočil, dokumentov in podatkov v nacionalnem zdravstvu – delo na funkcionalni in semantični povezljivosti),
- tehnološki vidik (opredeljevanje pomena in priprava priporočil za uporabo novih informacijsko komunikacijskih tehnologij v slovenskem zdravstvu).

Končni cilj sodobnega sistema je globalna mobilnost za vsako storitev – besedilo, sliko, zvok, govor, video. Ker je stanje v slovenskem zdravstvu zelo heterogeno, je cilj aktivnosti OZIS, da s standardizacijo elementov nacionalnih projektov postopoma dosega vse bolj enovit sistem. Če želimo doseči svetovno kompatibilnost storitev, je standardizacija bistvenega pomena.

2.9 Standardi

Celovitost informacijskega sistema, k čemur stremi tudi strategija eZdravje, je možno doseči samo s standardizacijo. Zdravstvena informatika povezuje kompleksno in občutljivo področje zdravstva s hitro razvijajočim in spreminjajočim se področjem informacijsko komunikacijskih tehnologij. Standardizacija na področju zdravstvene informatike je eno izmed orodij, ki omogoča in zagotavlja skladnost in medsebojno povezljivost zdravstvenih informacijskih sistemov z opredelitvijo zahtev za zdravstveno informacijske strukture v podporo kliničnih in administrativnih postopkov, zahtev za tehnične metode v podporo medsebojno povezljivih sistemov in opredelitvijo varnostnih in kvalitativnih zahtev.

Standardi so zapisani sporazumi, ki temeljijo na priznanih rezultatih znanosti, tehnike in izkušenj. Slovenski institut za standardizacijo (SIST) je nacionalni organ za standarde, ki pripravlja in sprejema slovenske nacionalne standarde in standardizacijske dokumente, ter zastopa slovenske interese v mednarodnih, evropskih in drugih nacionalnih organizacijah za standardizacijo. SIST med drugim redno privzema harmonizirane standarde EU v sistem slovenske standardizacije, zato so skoraj vsi harmonizirani evropski standardi tudi slovenski standardi z oznako SIST. Za področje informatike je zlasti zanimiv SISTov tehnični odbor za Informacijsko tehnologijo (SIST/TC ITC), za zdravstvo pa odbor Varovanje zdravja (SIST/TC VAZ). Nekatere zanimive standarde s tega področja obvladuje strokovni svet SIST za elektrotehniko, informacijske tehnologije in telekomunikacije (SIST/TC SET). V katalogu slovenskih standardov pod imeni zdravstvena informatika, medicinska informatika ali informatika zdravstvenega varstva najdemo vrsto standardov, predstandardov oz. osnutkov, tehničnih poročil in specifikacij. Trenutno število standardov na svetu za področje IKT v zdravstvenem sektorju ni znano (European Commission, 2008, str. 15). Trenutni problemi na področju standardov v EU (European Commission, 2008, str. 5 in str. 16-21):

Nasprotujoči standardi, različice in izvedbe. Na eni strani obstaja množica standardov, na drugi pa pomanjkanje standardov, ki bi se široko uporabljali, kar pogosto vodi do težav z interoperabilnostjo. Obstajajo tudi različne verzije, ki so si v navzkrižju (primer HL7 (angl. *High Level*) verzija 2 in verzija 3, ki žal ni nazaj kompatibilna) ali različne in neustrezne implementacije istega standarda, kar tudi vodi do problemov z interoperabilnostjo. Visoka kompleksnost standardov in lastniški standardi z nerazkritimi specifikacijami.

Pomanjkanje pravih standardov za posebna področja. Kljub velikemu številu standardov obstaja veliko področij, kjer ni nobenega standarda.

Politične ovire. Različni zdravstveni sistemi z nizko podporo standardizaciji. Veliko nacionalnih in regionalnih zdravstvenih sistemov na eni strani in majhna politična podpora standardizaciji na drugi strani.

Organizacije, ki se ukvarjajo z razvojem standardov, pričakujejo povračilo vloženih sredstev v razvoj in glede na to usmerjajo svoje aktivnosti. Ker narašča število standardov in stroški njihovega razvoja, si organizacije, ki se ukvarjajo z razvojem, ne prizadevajo za harmonizacijo standardov, saj je to dolgotrajen in drag postopek, temveč poizkušajo z trženjem svojih izdelkov dobiti povrnjen vložen denar.

Ustanove pričakujejo povračilo stroškov standardizacije. Ključni problem interoperabilnosti ni strojna ampak programska oprema. Velike korporacije so zainteresirane za standardizacijo z njihovimi lastniškimi standardi. Obstaja tudi interes podjetij, ki se ukvarjajo s sistemsko integracijo in služijo z vmesniki, ki nekompatibilnim sistemom zagotavljajo interoperabilnost. Za manjša podjetja in ustanove je strošek

implementacije standardov velik finančni zalogaj, zato si poizkušajo pomagati z uporabo cenejših nestandardnih rešitev.

Uporabniki. Ustanovam je lastna učinkovitost običajno pomembnejša kot uporaba splošnih standardov. Lahko se zgodi, da uporabnikom dostopni standardi ne ustrezajo ali jih tudi ne želijo uporabljati. Pri tem managerji ne pomislijo na finančne učinke, ki jih lahko prinese interoperabilnost.

Vse ovire v osnovi izvirajo z pričakovanih donosov v in iz standardizacije organizacij, ki se ukvarjajo z razvojem, industrije in uporabnikov. Če se želi spremeniti trenutno stanje, je potreben interes vseh vključenih. Tudi Englebardt in Nelson (2002, str. 362) menita, da je glavna prepreka pri široki uporabi elektronskega zdravstvenega zapisa in povezanega zdravstveno informacijskega sistema v pomanjkanju široko uporabljanih standardov.

S standardizacijo na področju informatike v zdravstvu se želi zagotoviti interoperabilnost in kompatibilnost med neodvisnimi sistemi ter z uporabo klasifikacij primerljivost podatkov za statistične namene. Standarde v zdravstvu lahko razdelimo tudi na tiste, ki pokrivajo tehnična področja npr. komunikacij, varnosti, programske opreme,… in na tiste, ki so namenjeni strokovnemu delu zdravstvenega osebja (npr za področje zdravstvene nege, …). Standarde pripravljajo različne delovne skupine, ki delujejo pod okriljem mednarodnih organizacij kot je npr tehnični komite TC215 (angl. *Technical Commetee* 215) pri mednarodni organizaciji za standardizacijo ISO (angl. *International Organization for Standardization*), ki ima naslednje delovne skupine (WG):

- TC 215/CAG 1 – izvršni svet, ki skrbi za usklajevanje aktivnosti,
- TC 215/WG 1 – podatkovne strukture,
- TC 215/WG 2 – izmenjava podatkov,
- TC 215/WG 3 – semantična vsebina,
- TC 215/WG 4 – varnost,
- TC 215/WG 5 – zdravstvene kartice,
- TC 215/WG 6 – poslovanje farmacevtov in zdravstva,
- TC 215/WG 7 – naprave,
- TC 215/WG 8 – poslovne zahteve za elektronski zdravstveni zapis,
- TC 215/WG 9 - skrbi za usklajevanje z drugimi organizacijami, ki razvijajo standarde.

Rezultat njihovega dela je viden v 52 standardih iz obravnavanih področij.

Pri CEN (Comite Europeen de Normalisation) skrbi za standarde s področja informatike v zdravstvu tehnični komite TC 251, ki je razdeljen v štiri delovne skupine. V Tabela 3: Najpomembnejše standardizacijske organizacije za področje IKT v zdravstvu, vidimo za vsako od naštetih organizacij tudi oznako organizacije, področje na katerem deluje in njihov najpomembnejši standard.

Tabela 3: Najpomembnejše standardizacijske organizacije za področje IKT v zdravstvu

Ime organizacije	**Oznaka**	**Področje**	**Njihov najpomembnejši standard**
International Standardisation Organisation	ISO	Razvoj splošnih standardov	ISO/TR 18307
European Committee for Standardisation	CEN	Razvoj splošnih standardov	ENV 13606 (parts 1-5), HISA - Health Care Information System Architecture
International Health Terminology Standards Development Organisation	IHTSDO	Terminologija	SNOMED, Systematized Nomenclature of Medicine
Health Level 7	HL7	Komunikacije in arhitektura	HL7 v2.x, HL7 v3.0, CDA, RIM, CCOW
Digital Imaging and Communications in Medicine	DICOM	Slike	DICOM
openEHR	openEHR	Arhitektura EZZ	openEHR
Integrating the Healthcare Enterprise	IHE	Standardi okvirov	Integracijski profili

Vir: European Commission, 2008, str. 29

2.9.1. Uporaba standardov na primeru elektronskega zdravstvenega zapisa

Za uspešno implementacijo elektronskega zdravstvenega zapisa potrebujemo standarde, ki bi omogočali pravilno identifikacijo, zbiranje, kodiranje, klasificiranje in izmenjavo kliničnih in administrativnih podatkov. Proces standardizacije mora zajeti področja arhitekture, terminologije, komunikacij in varnosti. Organizacijska struktura povezuje porazdeljene neodvisne enote, zdravstvene domove, bolnišnice, specialistične ambulante in druge. Primerna arhitektura elektronskega zdravstvenega zapisa je zato porazdeljena

(Belochi, 2003, str 379). Da bi se zagotovil nemoten pretok informacij med lokalnimi informacijskimi sistemi, je potrebno poskrbeti za integracijo številnih obstoječih aplikacij. To je težavna naloga, saj se zdravstveni in tehnični strokovnjaki še niso dogovorili o standardu in njegovi uporabi v primeru elektronskega zdravstvenega zapisa.

Arhitektura

Začetke arhitekture in vsebine elektronskega zdravstvenega zapisa lahko iščemo v predstandardu pr-ENV12265 (Evropean Pre-Standard of Electronic Healthcare Record Architecture, EHCRA) iz leta 1996. Naslednji korak je bil storjen 1997 z predstandardom prENV12967-1 (Health Care Information System Architecture, HISA). Sedaj to področje pokriva standard v treh delih:

- EN 12967-1:2008 (Zdravstvena informatika - Arhitektura storitve - 1. del: Vidik podjetja - Health informatics - Service architecture - Part 1: Enterprise viewpoint),
- EN 12967-2:2008 (Zdravstvena informatika - Arhitektura storitve - 2. del: Informacijski vidik - Health informatics - Service architecture - Part 2: Information viewpoint),
- EN 12967-3:2008 (Zdravstvena informatika - Arhitektura storitve - 3. del: Vidik obdelave informacij - Health informatics - Service architecture - Part 3: Computational viewpoint).

Naslednji standard s področja arhitekture je v petih delih:

- prEN 13606-1:2005 - Zdravstvena informatika – Komunikacija z elektronskimi zapisi na področju zdravstva – 1. del: Referenčni model - Health informatics - Electronic health record communication - Part 1: Reference model,
- prEN 13606-2:2006 - Zdravstvena informatika – Komunikacija z elektronskimi zapisi v zdravstvenem varstvu – 2. del: Arhetipi - Health informatics - Electronic health record communication - Part 2: Archetypes,
- prEN 13606-3:2006 - Zdravstvena informatika - Komunikacija z elektronskimi zapisi v zdravstvenem varstvu - 3. del: Referenčni arhetipi in seznami izrazov - Health informatics - Electronic health record communication - Part 3: Reference archetypes and term lists,
- prEN 13606-4:2006 - Zdravstvena informatika – Komunikacija z elektronskimi zapisi na področju zdravstva – 4. del: Varnostne zahteve in pravila za razdeljevanje - Health Informatics - Electronic health record communication - Part 4: Security requirements and distribution rules,

- prEN ISO 13606-5:2008 - Zdravstvena informatika - Komunikacija z elektronskimi zapisi na področju zdravstva - 5. del: Specifikacija vmesnika (ISO/DIS 13606-5:2008) - Health Informatics - Electronic Health Record Communication - Part 5: Interface specification (ISO/DIS 13606-5:2008).

Terminologija

Določena skupna terminologija za kodiranje in klasifikacije je tako kot format sporočila potrebna, če želimo učinkovito izmenjavati podatke. Na tem področju je uveljavljen SNOMED (Systematized Nomenclature of Medicine). Gre za numerično kodifikacijo, ki je mednarodno uveljavljena in uporabljena v kliničnih zapisih, patologiji, laboratorijih, skladiščenju podatkov in sistemih za podporo odločanju. Drugo tako orodje je mednarodna klasifikacija bolezni ICD (International Classification of Diseases) pod pokroviteljstvom svetovne zdravstvene organizacije WHO. Za to področje zdravstvene informatike v EU skrbi druga delovna skupina tehničnega komiteja CEN-TC251. Druge organizacije, ki delujejo na tem področju so še ANSI-HISB (American National Standard Institute), CPRI (Computer Patients Record Institute), MRI (Medical Records Institute) in NMDS (Clinical Nursing Minimum Data Set).

Komunikacije

Na področju komunikacij so predvsem pomembna sporočila in terminalne naprave. Sporočila so končni produkt UN/EDIFACT procesa, ki zasleduje hierarhično strukturirana sintaktična pravila. Najpogostejši EDI standard:

- laboratorijska sporočila (MEDREQ),
- za področje patologije in imunologije (MEDRPT),
- medicinski odpust pacienta (MEDIS),
- premestitve pacientov (MEDREF),
- recepti (MEDPRE in PRESCRIPTION).

Norme sporočil za ta področja so vključena v naslednje standarde:

- ENV 13607:2003 - Zdravstvena informatika – Sporočila za izmenjevanje informacij o medicinskih receptih - Health informatics - Messages for the exchange of information on medicine prescriptions,
- EN 13609-1:2005 - Zdravstvena informatika – Sporočila za vzdrževanje informacijske podpore pri sistemih zdravstvenega varstva – 1. del: Obnavljanje kodirnih shem - Health informatics – Messages for maintenance of supporting information in healthcare systems – Part 1: Updating of coding schemes,

- ENV 13609-2:2003 - Zdravstvena informatika – Sporočila za vzdrževanje informacijske podpore pri sistemih zdravstvenega varstva – 2. del: Obnavljanje medicinskih laboratorijskih informacij - Health informatics - Messages for maintenance of supporting information in healthcare systems - Part 2: Updating of medical laboratory-specific information.

Varnost

V skladu z direktivo EU 95/46/EC o varovanju obdelave in prostega pretoka osebnih podatkov mora upravljanje s podatki izpolnjevati tri temeljna načela: zaupnost, celovitost in razpoložljivost. Direktiva poudarja potrebo po pravni varnosti in celovitosti podatkov skupaj z varnostjo sistemov, celovitostjo in zanesljivostjo. Zahteva tudi soglasje pacienta, šifriranje podatkov in elektronski podpis pri izmenjavi podatkov med zdravstvenimi ustanovami. Pri CEN TC251 je tretja delovna skupina zadolžena tudi za področje varnosti. Veljavni standardi tega področja so:

- prEN 13608-1:2006 - Zdravstvena informatika – Varnost komuniciranja v zdravstvenem varstvu – 1. del: Koncepti in izrazje - Health informatics - Security for healthcare communication - Part 1: Concepts and terminology,

- prEN 13608-2:2006 - Zdravstvena informatika – Varnost komuniciranja v zdravstvenem varstvu – 2. del: Varni podatkovni objekti - Health informatics - Security for healthcare communication - Part 2: Secure data objects,

- prEN 13608-3:2006 - Zdravstvena informatika – Varnost komuniciranja v zdravstvenem varstvu – 3. del: Varni podatkovni kanali - Health informatics - Security for healthcare communication - Part 3: Secure data channels,

- EN 12251:2005 - Zdravstvena informatika – Varna identifikacija uporabnikov v zdravstvenem varstvu – Upravljanje in varnost avtentikacije z gesli - Health informatics - Secure User Identification for Health Care - Management and Security of Authentication by Passwords,

- ENV 13729:2003 - Zdravstvena informatika – Varna identifikacija uporabnikov – Močna avtentikacija z mikroprocesorskimi karticami - Health informatics - Secure user identification - Strong authentication using microprocessor cards.

Nekatere primere standardov po posameznih področjih s kratkimi opisi področij vidimo v Tabela 4: Poglavitni standardi s področja informatike v zdravstvu.

Tabela 4: Poglavitni standardi s področja informatike v zdravstvu

Področje	Opis	Primeri
Standardi za področje arhitekture (v tem primeru za EZZ).	Standardi splošne strukture ali načrti zdravstveno informacijskega sistema, s komponentami in njihovimi povezavami in razmerji. Posebna vrsta standardov arhitekture je za področje elektronskega zdravstvenega zapisa.	- CEN EN 13606 - CEN EN 12967 Service Architecture (HISA), - HL7 v3, - openEHR
Standardi za področje modelov.	Standardi za načine načrtovanja in definiranja arhitekture zdravstveno informacijskih sistemov.	- SIST-TP CEN/TR 15300:2006 - Zdravstvena informatika - Okvir za formalno oblikovanje varnostne politike v zdravstvenem varstvu - Health informatics - Framework for formal modelling of healthcare security policies - ISO 10746 ODP
Standardi za področje komunikacije	Dvosmerna izmenjava informacij med dvema entitetama zdravstvenega sistema.	- CEN EN 13606 EHR Communication, - CEN EN 13609-1:2005 Messages for maintenance of supporting information in healthcare systems, Part 1: Updating of coding scheme, - DICOM, - HL7 v2.x, HL7 v3, - ISO 11073 Point of Care Medical Device Communications
Standardi za področje infrastrukture	Standardi za skupino komunikacijskih protokolov, ki zagotavljajo podporo za distribucijo informacij znotraj zdravstvenega omrežja, na primer strojev in institucij.	- CEN ENV 13729 Secure User Identification, Strong Authentication using microprocessor cards, - ETSI TS 101733 Electronic Signature Formats, - HL7 Service-oriented architecture, - ISO 17090 Public Key Infrastructure
Standardi za področje varnosti podatkov	Standardi za zaščito bolnikov podatkov s pomočjo npr. šifriranja podatkov in elektronskega podpisa, da se prepreči izguba in tatvine.	- DICOM, - ISO DTS 25237 Pseudo-anonymisation, - ISO 22600 Privilege Management and Access Control,
Varnostni standardi	Standardi v zdravstvenem varstvu s poudarkom na podpori poročanju, analizi in preprečevanju zdravniških napak in neželenih zdravstvenih dogodkov.	- CEN TR 13694 Safety and Security Related Software Quality Standards for Healthcare
Standardi za področje terminologije in ontologije	Standardi za specifično izrazoslovje zdravstvenega sektorja za opis konceptov in njihovih medsebojnih povezav.	- CEN EN 13940 System of Concepts to Support Continuity of Care, - ISO/CD 17115 Vocabulary on Terminological Systems, - LOINC in SNOMED

Vir. European Commission, 2008, str.15

2.10 Varnost

Na področju zdravstvenega varstva so zaupnost, varnost in integriteta ključnega pomena in zahtevajo odlično načrtovanje, zasnovo in implementacijo (Englebardt & Nelson, 2002, str. 419). Vse elemente elektronskega poslovanja povezuje proces in organizacija dela. Z organizacijo in tehnologijo pa je neločljivo povezana varnost in z njo povezana vprašanja. To je tudi razlog, da se v nadaljevanju dotaknem področja informacijske varnosti in nekaj vprašanj tudi vključim v anketo.

Pospešena digitalizacija zdravstvenih organizacij, rastoča kompleksnost informacijskih tehnologij in sofisticiranost kriminalnih združb povečuje tveganja vdorov v informacijske sisteme, krajo in zlorabo podatkov. Grožnja varnosti v zdravstvu pomeni grožnjo poslanstvu, poslovnim ciljem in poslovnemu uspehu, delovanju zdravstvene institucije in posredno zdravju pacientov (Rudel, 2005).

Informacijska varnost (angl. *Information security*) pomeni zaščito informacij pred nepooblaščenim razkritjem, prenosom, spreminjanjem ali uničenjem, ne glede na to, ali je dogodek naključen ali nameren (Kovacic & Halibozek, 2003, str. 361). Namen informacijske varnosti je zagotoviti neprekinjeno poslovanje in zmanjšati škodo s preprečevanjem in zmanjšanjem posledic varnostnih incidentov (Šinigoj, 2008, str 14). V zdravstvu naj bi varnosti posvečali še posebno pozornost, saj gre za dejavnost, ki tudi rešuje življenja in v svoji podatkovnih bazah hrani občutljive osebne podatke. Če želimo nekaj varovati, moramo najprej vedeti, kaj želimo varovati in koliko je za nas to vredno. Torej glede na pomen opredelimo vire, ki jih bomo varovali. V zdravstvenih organizacijah je vrednost podatkov težko oceniti, saj imajo poleg objektivne tudi veliko subjektivno vrednost. Nato poizkušamo ugotoviti, kakšnim tveganjem so viri lahko izpostavljeni. Na podlagi ugotovitev izdelamo varnostno politiko, ki nam bo osnova pri oblikovanju in izvajanju tehničnih in organizacijskih ukrepov. Tehnične rešitve po oceni lahko zagotovijo samo 30% varnosti zdravstvenih informacij (Englebardt & Nelson 2002, str.445). Vsi strokovnjaki se strinjajo, da popolne varnosti ni. Vodja informatike v Gorenju trdi, da so vsi informacijski sistemi glede varnosti ranljivi. Razlika je le v tem, da se ena podjetja tega bolj zavedajo, druga pa manj (Kotnik, 2006, str. 21). Ker stroški s povečevanjem varnosti naraščajo eksponentno, ne gre za to, da dosežemo največjo možno varnost, ampak da postavimo najbolj smiseln nivo varnosti. Da bi lahko govorili o nivoju, ki ga želimo doseči, pa moramo vedeti, kje sploh smo. Kako je z zavedanjem in nivojem varnosti v slovenskem zdravstvu?

Pri vprašanju varnosti je pomembno, da smo sistematični. Zato si pomagamo s standardi. V ZDA od zdravstvenih ustanov zahtevajo skladnost s HIPAA (Health Insurance Portability and Accountability Act). HIPAA zagotavlja prenosljivost in nepretrganost zdravstvenega zavarovanja, preprečuje zlorabe zdravstvenega zavarovanja in koriščenja zdravstvenih storitev, promovira sisteme varčevanja za zdravstvene storitve, izboljšuje dostopnost do

dolgotrajne zdravstvene obravnave in poenostavlja administrativne zadeve v zvezi z uveljavljanjem zdravstvenega zavarovanja (http://cms.hhs.gov/hipaa/). V Sloveniji je SIST 1.11.2008 sprejel standard SIST EN ISO 27799:2008 – Zdravstvena informatika - Upravljanje informacijske varnosti v zdravstvu z uporabo standarda ISO/UEC 27002. Med pogosteje uporabljenima standardoma pa sta standard za upravljanje z informacijsko varnostjo ISO/IEC 27001:2006 in kodeks za upravljanje varovanja informacij ISO/IEC 17799:2005. ISO/IEC 17799:2005 ima kontrole razdeljene v 11 področij:

- varnostna politika,
- informacijska varnost organizacije,
- upravljanje sredstev,
- človeški viri,
- fizična zaščita in zaščita okolja,
- upravljanje s komunikacijami in s produkcijo,
- nadzor dostopa,
- nabava, razvoj in vzdrževanje informacijskih sistemov,
- upravljanje incidentov pri varovanju informacij,
- neprekinjeno poslovanje,
- združljivost.

Standard BS17799 v ustanovi pomeni; neoporečnost, razpoložljivost in zaupnost in je vodilo za vse aktivnosti zagotavljanja varnosti pri posredovanju in hrambi informacij. Je orodje stalnega izboljševanja poslovnega procesa v smislu upravljanja informacij. Sestavljen je iz dveh delov. Prvi del predstavlja najboljšo prakso pri zadovoljevanju zahtev standarda in razlaga, kaj naj bi organizacija imela. Drugi del je specifikacija z napotki za uporabo in razlaga, kaj mora organizacija imeti, če želimo biti skladni s standardom in se po njem certificirati.

Standard 27001:2006 določa tri stebre informacijske varnosti:

- zaupnost, ki pomeni zaščito informacij pred nepooblaščenim razkritjem,
- celovitost, ki pomeni zaščito informacij pred nepooblaščenimi spremembami in zagotovitev, da so informacije pravilne in popolne,

- razpoložljivost, ki pomeni zagotavljanje, da so informacije na voljo, kadar jih potrebujemo.

Zagotavljanje varnosti informacijskega sistema je stalen proces, ki naj prispeva k zmanjševanju motenj v delovanju informacijskega sistema organizacije ter možnosti odpovedi delovanja. Ena od dejavnosti službe za informatiko je tudi skrb za varnost informacijskih sistemov.

Informacijska varnost obsega varovanje in zaščito vseh kritičnih, poslovno občutljivih, tajnih, osebnih in drugače občutljivih podatkov ter sistemov, ki so namenjeni obdelavi teh podatkov. Ustanove dnevno prejmejo, ustvarijo, dopolnijo in spremenijo podatke v različnih oblikah. Če se ti podatki uničijo, poškodujejo ali so odtujeni, lahko pride do velikanske škode ali celo do nepopravljivih posledic. Za ugotovitev in oceno s tem povezanih tveganj, pripravo in izvajanje ukrepov za zmanjševanje teh tveganj, ter nadzor nad izvajanjem ukrepov, mora vsaka ustanova opraviti podrobno oceno tveganj ter zatem pripraviti dokument z jasnimi pravili in navodili glede informacijske varnosti, ki mu rečemo tudi informacijska varnostna politika. V njej so natančno določeni odzivi in postopki pri posamičnih, v naprej opredeljenih težavah, varnostnih kršitvah, naravnih nezgodah, itd. Aktivnosti na področju varnosti morajo omogočati poslovanje, ne pa ga zavirati. V anketnih vprašanjih sem zastavil po eno vprašanje iz naslednjih področij:

- varovanje ključne informacijsko komunikacijske opreme,
- zaščita podatkov, ki se izmenjujejo,
- varovanje dostopa do podatkov,
- izdelava varnostnih kopij,
- varnost pred zlonamerno kodo,
- varnostna politika,
- oskrba z energijo.

2.10.1. Tveganja

Informacijske vire sestavljajo strojna in programska oprema, podatki in ljudje. Vsak od teh virov pa je lahko vzrok nedelovanju sistema oziroma ključno področje pri varovanju informacijskih sistemov. Naloga odgovornih za varnost je določiti tveganja, ki jim je informacijski sistem izpostavljen. Tveganjem se ne moremo v celoti izogniti, lahko pa jih

poizkušamo zmanjšati na najmanjšo možno mero. Pri tem bomo najuspešnejši, če bomo sistematični. Vzpostavljanje informacijske varnosti je v začetku projekt nato pa proces, ki ga je potrebno stalno vzdrževati. Vzroki za nedelovanje oziroma napačno delovanje informacijske opreme so lahko (Gradišar & Jaklič & Turk, 2007):

- napačno ravnaje človeka (neznanje, …),
- strojne okvare (diski, napajanje, spomin,…),
- napake v programih,
- napake v podatkih,
- poškodbe računalniške opreme,
- neprimerne tehnične karakteristike,
- neodgovornost,
- zlonamerna programska koda (črv, virus, trojanski konj, …).

Za največ varnostnih težav so krivi prav zaposleni v organizaciji, pri čemer več kot polovico teh groženj predstavljajo uporabniki, ki škode ne povzročajo namenoma (Praprotnik, 2006, str. 24-27). Vzroki notranjih incidentov so različni, od neznanja do želje po maščevanju ali samodokazovanju. Nekdo znotraj bolje pozna sistem in varovala in tako lažje povzroči škodo. Izdelane varnostne politike in vpeljane procedure za njeno izvajanje močno zmanjšujejo tovrstna tveganja. Naslednje tveganje je kraja podatkov, ki se lahko izvaja na različne načine oziroma z uporabo različnih metod:

- kraje z goljufivimi podatki,
- kraje s spremembo programa,
- kraje podatkov s pomočjo programa (vohljač – angl. *Sniffer*, vohunsko programje – angl. *Spyware*, opazovalci tipkovnice – angl. *Keylogger*).

Največja nevarnost pa je zagotovo nepravilno konfigurirana, nenadzorovana ali slabo vzdrževana oprema, saj poleg nevarnosti povzroča tudi lažen občutek varnosti (Bratuša, 2006, str 322).

V anketi sem ustanove povprašal, kako zagotavljajo varovanje pred virusi. Izraz virusi, namesto zlonamerna koda, je uporabljen namenoma zaradi večje razširjenosti.

2.10.2. Varnost fizičnega nivoja

Vključuje fizično okolje, vključno z lokacijo kritične opreme in računalniško sobo kot tudi varovanjem strežnikov in namiznih računalnikov v celotni ustanovi. Kontrole, ki pokrivajo to področje po standardu ISO/IEC 17799:2005, najdemo v poglavju Fizična in okoljska varnost. Za sistem varovanja informacij je jasno, da so tehnične varnostne kontrole premalo oziroma, da so neučinkovite, v kolikor niso podprte z organizacijskimi ukrepi. Eden takšnih organizacijskih ukrepov je Načrt varovanja, v katerem opredelimo različne postopke in ukrepe pri zagotavljanju varovanja, predvsem pa opredelimo odgovornost in odgovorne osebe (Loborec, 2006, str. 16-17).

V anketi sem ustanove povprašal, kako zagotavljajo varovanje ključne IKT opreme (npr. strežnika).

2.10.3. Varnost omrežja

Omrežje je definirano kot dve ali več naprav, ki sta povezani z namenom pošiljanja, sprejemanja in izmenjave podatkov (Vidmar, 2002). V kolikor izmenjava podatkov v omrežju poteka brez zaščite, na primer uporabe virtualnih privatnih omrežij – VPN, obstaja večja možnost kraje podatkov. Varnostni problemi so večji v mobilnih, brezžičnih okoljih, saj gre za medij, ki ga je težje nadzorovati, zato je pomen enkripcije večji. Brezžična omrežja po mnenju nekaterih še niso primerna, ko gre za omrežja, ki zahtevajo visoko zaupnost, zanesljivost in razpoložljivost (Rolih, 2006, str.9-10). Varnost informacijskih sistemov zagotavlja mnogo dejavnikov, kot so na primer antivirusni programi, protivohunsko programje, požarni zidovi, sistemi za zaznavanje in preprečevanje vdorov ter drugo. Požarni zidovi in sistemi za zaznavanje in preprečevanje vdorov se dopolnjujejo, saj prvi določajo, kateri promet se lahko odvija v omrežju oz. kateri se zavrže, medtem ko drugi dodatno preverjajo dovoljeni promet, ki je usmerjen v omrežje, hkrati pa nadzorujejo tudi dogajanje znotraj sistema in s tem preprečujejo zlorabe od znotraj (Šavnik, 2006, str. 28-30). Klasifikacija sistemov in programov za odkrivanje vdorov (Bratuša, 2006, str 381):

- sistemi za odkrivanje vdorov v omrežje NIDS (Network Intrusion Detection Systems),
- sistemi za odkrivanje vdorov v strežnik HIDS (Host Intrusion Detection Systems),
- sistemi za preprečevanje vdorov v strežnike HIPS (Host Intrusion Prevention Systems),

- muholovci (HoneyPots),
- programi za zaznavanje vdorov v brezžična omrežja (Wireless IDS's),
- programi za preverjanje integritete datotek,
- sistemi za omejevanje napadov,
- priključki omrežnih sistemov za zaznavanje in preprečevanje vdorov.

Da bi ugotovili, v kakšnem stanju je omrežje in kako izvajamo navodila varnostne politike, je priporočljivo izvajati testiranje in na podlagi rezultatov izvajati korekcije politike in nastavitev. Redno preverjanje varovanja informacijskega sistema, ki ga opravi nekdo, ki je neodvisen, nikakor pa ne tisti, ki so načrtovali varnostno politiko ali jo izvajajo, pripomore k bolj realni oceni varnostne slike. S pomočjo testiranja pridobimo informacije o osnovnih karakteristikah delovanja omrežja in posnamemo promet med testiranji. Z njim pregledamo različne segmente omrežja. Testiranje zunanjega dela poteka preko interneta. Izvajalec varnostnega preizkusa se postavi v vlogo zunanjega napadalca in s pomočjo različnih orodij in tehnik pridobiva čim več informacij o omrežju, predvsem pa pomanjkljivosti, ki bi pravemu napadalcu lahko omogočile vstop v informacijsko infrastrukturo naročnika. Predmet notranjega testiranja so elementi notranjega omrežja (računalniški sistemi in omrežna infrastruktura). Testiranje notranjega omrežja sestavljata dve fazi. V prvi se postavimo v vlogo napadalca, kjer s pomočjo različnih orodij in tehnik poskušamo odkriti varnostne slabosti omrežja in računalniških sistemov. V okviru varnostnega testiranja notranjega omrežja preverjamo vse varnostno občutljive elemente omrežja, strežnike in vzorčne delovne postaje. V okviru testiranja zunanjega omrežja testiramo vse sisteme, ki so namenjeni povezavi z javnim internet omrežjem in povezavi s partnerji ter sisteme, ki so namenjeni za posredovanje javnih informacij (požarne pregrade, spletne strežnike, usmerjevalnike, namenjene povezavi z internetom in drugo).

V anketi sem ustanove povprašal, kako zagotavljajo varnost pred zunanjimi vdori.

2.10.4. Varnost aplikacij

Aplikacije in sistemska programska oprema so čedalje bolj kompleksni, zato pogosto vsebujejo tudi napake. Napake, ki omogočajo vdor in zlorabe, nepridipravi izkoriščajo za svoje delovanje. Takšne ranljivosti poizkušajo proizvajalci odpraviti s popravki (angl. *Patches*). Ustanove, ki skrbijo za področje informacijske varnosti, kot na primer CERT ali National Vulnerability Database (http://nvd.nist.gov) za odpravo odkritih ranljivosti največkrat priporočajo redno nameščanje popravkov. Vendar je pred instalacijo popravkov

potrebno oceniti tveganja v kolikor instalacije ne izvedemo ter raziskati možnosti, kako bo to vplivalo na druge dele sistema. Vse avtomatske posodobitve naj se uporabljajo le v kolikor jih je možno tudi razveljaviti.

Standard ISO/IEC17799:2005 v poglavju, ki pokriva pridobitev, razvoj in vzdrževanje sistemov priporoča, da se vse zahteve glede varnosti opredelijo, utemeljijo in dokumentirajo že v projektni fazi razvoja oblikovanja zahtev. Standard predvideva različne kontrole, s katerimi se preveri ali se zagotavlja:

- validacija vhodnih in izhodnih podatkov,
- integriteta sporočil,
- odkrivanje kakršnegakoli nepravilnega procesiranja zaradi napak ali namernega dejanja,
- zaščita integritete, celovitosti in zaupnosti s pomočjo metod kriptografije,
- varovanje sistemskih datotek in izvorne kode,
- varnost razvojnega okolja,
- menedžment odkritih ranljivosti.

Nadzor nad tem, kdo lahko uporablja aplikacijo, evidenco baze podatkov ali datoteko, lahko organizaciji pomaga zaščititi podatke. Tak nadzor se lahko vrši tudi s pomočjo dnevnikov (log datotek), ki je v slovenskem zdravstvu v nekaterih primerih že v veljavi (npr. aplikacija eSPP pri IVZ RS).

2.10.5. Varnost podatkov

Zbirke podatkov so v ozadju sistemov, od katerih je odvisno naše vsakdanje življenje, pa naj gre za bančni račun, zdravniško kartoteko, pokojnino, podatke zaposlenega ali kaj drugega. Vse večji pritiski in težnje po t.i. nepapirnatem poslovanju so privedli do tega, da zbirke podatkov vsebujejo vedno več občutljivih podatkov, zaradi česar so za napadalce čedalje več vredne. Za varnost podatkovnih zbirk je ključnega pomena znanje administratorja, ki sistem nadzira in z njim upravlja. Ta problem postane pereč v manjših zdravstvenih ustanovah, ki imajo tako kot velike podobne oziroma enake zdravstvene in osebne podatke, vendar manj sredstev. Zato imajo manj zaposlenega strokovnega kadra in verjetno sklenjene vzdrževalne pogodbe, ki zagotavljajo nižji nivo storitev kot večje ustanove. Tveganja zlorab v zvezi z zbirkami podatkov povečujejo varnostne pomanjkljivosti (Bratuša, 2006):

- v omrežnih protokolih brez avtentifikacije,
- v omrežnih protokolih z avtentifikacijo,
- v avtentifikacijskih protokolih,
- pri dostopu do funkcionalnosti brez avtentifikacije,
- pri izvršitvi arbitrarne kode v trinzičnih elementih SQL,
- pri izvršitvi arbitrarne kode v varovanih elementih SQL,
- pri razširjanju privilegijev na podlagi SQL injection,
- pri krajevnem razširjanju privilegijev.

Varnost naj se v procese vključuje čim bolj zgodaj, po možnosti v fazi načrtovanja podatkovnih virov. Neprimerno načrtovane procese je težko zaščititi. Temeljno pravilo naj bo, da je prepovedano vse, kar ni dovoljeno, ki ga potem nadgrajujemo z natančnejšimi dovoljenji. S stališča varnosti je bolje predpisati posamezne dovoljene načine izmenjave, kakor pa razmišljati o vseh prepovedanih.

V anketi sem ustanove povprašal, kako zagotavljajo varovanje dostopa do podatkov.

2.10.6. Uporabniški nivo

Najšibkejši člen informacijske varnosti je uporabnik (Bratuša, 2006, str 215). Najpomembnejši napotek uporabniku je, da je pri uporabi programske opreme zelo previden. Poleg tehničnih ukrepov in znanja je predvsem priporočljiva uporaba zdrave človeške pameti. Dosedanje varnostne politike v računalniških omrežjih so se v glavnem ukvarjale s preprečevanjem fizičnega dostopa do aktivne mrežne opreme, z zagotavljanem redundantnih povezav in napajanja ter z aktivnimi požarnimi zidovi in sistemi za zaznavanje poskusov vdorov. Problem nastane, kadar uporabniki, ki so del takega omrežja, uporabljajo prenosne računalnike, s katerimi se povezujejo tako v internet kot v intranet, mnogokrat tudi preko omrežij sumljivega porekla, kot so javne vroče točke po letališčih, hoteli, … Edini varovalni mehanizem je tu seveda blokada fizičnega dostopa ter priklopa v omrežje. Rešitev problema je v ideji, da se v omrežje vdela dodaten upravljalni sloj, ki bo dejanski dostop do omrežja dovolil končnim napravam šele, ko bodo izpolnile vse zahtevane pogoje. Politika organizacije določa pogoje. Na primer, da so nameščeni vsi varnostni popravki operacijskega sistema, da so knjižnice protivirusnega sistema stare največ nekaj dni, da je aktivna požarna pregrada, ...

2.10.7. Varnostna politika

Vsaka ustanova naj bi imela varnostno politiko varovanja informacij. Ta dokument naj bi bil osnova za vse ostale dokumente, ki varnostno problematiko obravnavajo bolj podrobno in so namenjeni reševanju specifičnih problemov. Politika varovanja informacij je interni akt organizacije, ki jasno določa navodila v zvezi z varnostjo in odgovornostmi zaposlenih za izvajanje te politike. Vsebuje pravila obnašanja in delovanja znotraj organizacije, obenem pa določa, kaj je in kaj ni dopustno. Varnostna politika je vodilo vodstvene strukture podjetja ali organizacije, ki definira kaj, kako in kdo je odgovoren za varno upravljanje informacij. To je dokument, ki ga razumejo vsi zaposleni in definira pravila za upravljanje z informacijami in uporabniki teh informacij. Sestavni del varnostne politike pa so tudi varnostni načrti, ki definirajo, na kakšen način se v podjetjih izvaja zaščita zaupnih in kritičnih poslovnih informacij. Varnostna politika naj bi služila vsem zaposlenim in zunanjim sodelavcem ter izvajalcem kot neposreden vir pravil in navodil za učinkovito in varno uporabo informacijsko telekomunikacijske opreme in varovanja podatkov. Sistemsko naj bi zajemala vsa področja ustanove. Izvajanje varnostne politike ter njeno dopolnjevanje na podlagi pridobljenih praktičnih izkušenj in periodičnih analiz mora spremljati stalen nadzor.

Ustanova potrebuje varnostno politiko, da sporoči svojim zaposlenim, kakšne so njihove obveznosti in odgovornosti pri delu z informacijami in s pomembnimi dokumenti. Varnostna politika je nujna, ker definira načine varne uporabe informacijsko telekomunikacijske tehnologije. Obstoj varnostne politike pa je lahko ključni faktor, ko se pojavijo težave (spori, tožbe, ipd.).

Varnostna politika je lahko sestavljena kot en dokument ali pa več nivojsko, od krovne politike na najvišjem nivoju, prek politik za posamezna področja, do posameznih navodil in obrazcev na najnižjem nivoju. Krovna varnostna politika predstavlja temeljni dokument za varovanje informacij v ustanovi. Osnovni cilj dokumenta je pridobivanje podpore in priprava organizacije na izgrajevanje celovitega sistema varovanja.

Informacijska varnostna politika je seveda posvečena predvsem zagotavljanju informacijske varnosti, vendar pa varnost ni sama sebi namen, temveč je povezana z delovanjem ustanove. Strokovnjaki lahko učinkovito uporabijo tehnologijo varovanja, ki je na voljo le, če ima organizacija ustrezno varnostno politiko (Jaklič, 2002, str. 34). To pa pomeni, da je potrebno za vsak podatek določiti, kdo in kakšne pravice dostopa naj ima, potrebno stopnjo zaščite, … Za ohranjanje budnosti je potrebno skrbeti za redno izobraževanje zaposlenih. Sama varnostna politika, če je samo kos papirja, ne pomeni nič. Ključni dejavnik je človek, zato je potrebno dvigovati varnostno zavest. Varnostna politika, ki je zaradi narave posla ni mogoče izvesti v celoti, ni dobra.

Informacijska varnostna politika je formalen dokument, ki ga mora sprejeti vodstvo. Zaradi formalnosti bo njen obvezni sestavni del tudi jasna navedba začetka in morebitnega konca veljavnosti. Informacijska varnostna politika naj velja za vse redno in pogodbeno zaposlene pa tudi za tretje stranke. Zavezanost posameznika k informacijski varnostni politiki je določena s pogodbo, ki jo podpišeta obe stranki. Veljavnost za posameznika se začne z dnem podpisa in preneha s koncem pogodbe, če ni drugače določeno.

Organizacije sprejemajo varnostne politike z namenom izogibanja varnostnim incidentom in zaradi doseganja čim večje stopnje informacijske varnosti. Informacijska varnost oz. varnost sistemov in informacij pa je neločljivo povezana z (informacijskim) pravom, zato lahko urejenost pravnih vprašanj v zvezi z informacijskimi sistemi pomembno prispeva k celoviti informacijski varnosti. Najprej se zastavi vprašanje pravne narave varnostne politike. Ta je lahko samo neobvezno priporočilo za zaposlene in zunanje sodelavce, lahko pa je obvezno navodilo, katerega nespoštovanje potegne za seboj disciplinske ukrepe, lahko pa tudi civilne tožbe ali celo kazenski pregon. Drugo pomembno pravno vprašanje v zvezi z varnostnimi politikami je, kako so te umeščene v notranje pravne akte organizacij (statut, sklepi, pogodbe z zaposlenimi in zunanjimi sodelavci itd.). Od tega je odvisna tudi njihova pravna narava oz. obveznost njenega spoštovanja za različne subjekte.

V anketi sem zdravstvene ustanove povprašal, ali imajo sprejet dokument varnostne politike za področje informatike.

2.10.8. Upravljanje neprekinjenega poslovanja

Z uvedbo postopkov za neprekinjeno poslovanje in okrevanje želimo zmanjšati posledice izgube informacij za organizacijo na sprejemljivo raven (ISO/IEC 17799, 2005). Program upravljanja neprekinjenega poslovanja (UNP) v organizaciji je nekakšen zasilni izhod, ki ga vodstvo organizacije uporabi, ko odpovedo preventivni ukrepi in pride do nesreče ali incidenta, ki povzroči prekinitev običajnega poteka poslovnih procesov (Grasselli, 2006, str 20-22). Gre za kompleksen proces preprečevanja in upravljanja incidentov ter nenazadnje vzpostavitve normalnega delovanja po incidentu (Šinigoj, 2008, str. 15). Vodstvo organizacije torej z vpeljavo programa UNP vzpostavi poslovne procese in organizacijo dela ter zagotovi znanje, ljudi in vire, potrebne za delo v izrednih razmerah.

Glede na prepletenost poslovanja in informacijske tehnologije začne večino postopkov neprekinjenega poslovanja oddelek informatike, ki zagotavlja obnovo informacijskega sistema v primeru izpada.

V anketi sem ustanovam zastavil naslednja vprašanja:

- kako zagotavljate delovanje v primeru izpada napajanja?
- kako zagotavljate varnostno kopiranje in hranjenje podatkov?
- kako pogosto vršite varnostno kopiranje podatkov?
- kako pogosto vršite kontrolo arhivov?
- koliko časa potrebujete za vzpostavitev sistema pri hudem izpadu (v urah)?
- kaj uporabljate za obveščanje o izpadu?

2.11 Pravne podlage elektronskega poslovanja v zdravstvu

Sodobne informacijske tehnologije podpirajo in določajo delovne procese in omogočajo elektronsko zajemanje in arhiviranje vseh vrst podatkov. Sodoben način dela zahteva tudi ustrezno zakonodajo, ki storitvam informacijske družbe da pravno podlago. Temeljna skrb evropskih pravnih aktov in slovenske zakonodaje je ustrezno in zaupno ravnanje z osebnimi podatki posameznika in dosledno spoštovanje pravic uporabnika zdravstvenih storitev. Za področje eZdravja so posebnega pomena naslednje direktive EU:

- 95/46/EC – Direktiva o varovanju podatkov, ki zahteva, da morajo biti osebni podatki:
  - obdelani pravično in zakonito;
  - zbrani le za določene namene;
  - pravilni in posodobljeni;
  - neprenosljivi tretjim strankam brez dovoljenja;
  - neprenosljivi iz države, ki nimajo ustrezne zaščite za osebne podatke;
  - zaščiteni s strani nadzornika podatkov organizacije.
- 97/66/EC – Direktiva o obdelavi osebnih podatkov in varovanju zasebnosti v telekomunikacijskem sektorju,
- 1999/93/EC – Direktiva o pravnih podlagah za uporabo elektronskega podpisa,

- 2002/58/EC – Direktiva o zasebnosti in elektronskih komunikacijah,
- 2002/21/EC – Direktiva o zakonskih okvirih za elektronska komunikacijska omrežja in servise.

Drugi zakoni, ki jih je potrebno pri uvajanju elektronskega poslovanja v zdravstvo potrebno upoštevati, so še:

- Zakon o elektronskem poslovanju in elektronskem podpisu.

  Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP, Ur. l. RS, št 57/2000) predstavlja podlago za elektronsko poslovanje. Država želi z omenjenim zakonom spodbujati hiter tehnološki razvoj elektronskega poslovanja in odstraniti normativne ovire za elektronsko poslovanje s posebnim poudarkom na izenačitvi zanesljivih elektronskih oblik s klasično papirno obliko in izenačitvi varnih ter zanesljivih elektronskih podpisov z lastnoročnim podpisom.

- Zakon o zbirkah podatkov s področja zdravstvenega varstva. (Ur. l. RS, št. 65/2000).
- Zakon o varstvu osebnih podatkov.

  Po zakonu (Ur. l. RS. št. 59/1999), ki je doživel eno poglavitnih sprememb leta 2004 (Ur.l. RS, št. 86/2004), je osebni podatek katerikoli podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen. Občutljivost osebnih podatkov, na primer imena, priimka, datuma rojstva, številke zdravstvenega zavarovanja, se po sprejemu v zdravstveno obravnavo precej poveča. V tem zakonu tiči tudi nekaj pravnih ovir pri realizaciji elektronskega zdravstvenega zapisa, saj strogo postavlja omejitve pri povezavah posameznih zbirk podatkov.

- Zakon o elektronskih komunikacijah (Ur. l. RS št. 43/2004).
- Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih (ZVDAGA, Ur. l. RS št. 30/2006).

3 PRIPRAVLJENOST NA ELEKTRONSKO POSLOVANJE

V zdravstvu se izraz eHealth oziroma eZdravje dostikrat razume kot e-poslovanje. Vendar eZdravje ni samo elektronsko poslovanje v zdravstvu, zajema širše področje. Zdravniki

neradi uporabljajo izraz elektronsko poslovanje, saj zdravstvenega varstva ne jemljejo kot posel in pacienta kot stranko. Tak način razmišljanja verjetno izhaja iz zdravniške etike, ki jih zavezuje pomagati ljudem. Že izraz zdravniške usluge nakazuje tak način razmišljanja. Kljub temu pa se zdravniške storitve na nek način »prodajajo« pacientom. V zdravstvenih ustanovah je tudi množica procesov, ki so podobni tistim v storitvenih ali proizvodnih organizacijah. Tako imajo na primer opravka z dobavitelji zdravil in medicinske opreme, hrane, tekstila, … in storitev. Zato tudi lahko govorimo o elektronskem poslovanju v zdravstvenem sektorju (European Commission, 2007).

Prehod v elektronsko poslovanje poteka kot evolucijski proces preko več stopenj. Osnova temu razvoju je primerna pravna zakonodaja in tehnološka infrastruktura. Razvoj poteka z prenovo procesov, ki vključujejo motivirane ljudi, ki znajo s pomočjo tehnologije dosegati poslovne cilje. Privzamemo lahko, da je pravna infrastruktura ustrezna, saj v Sloveniji nekatera podjetja že poslujejo elektronsko na precej visoki stopnji. Tudi projekt KZZ Online (ZZZS, 2007), ki v zdravstvu uvaja nov koncept dostopa do podatkov, to dokazuje.

Prehod organizacije v elektronsko poslovanje poteka postopno in v več fazah (Kovačič, Bosilj Vukšić, 2005, str. 140-141):

- v prvih fazah, ki še niso pravo elektronsko poslovanje, organizacija objavlja svojo ponudbo ali povpraševanje. V ta namen ponujajo uporabnikom dostop do podatkov oziroma informacij na spletnih straneh. Na področju zdravstva bi v tej stopnji spletne strani ustanov lahko nudile informacije o ustanovi, področjih dela, delovnih časih, zaposlenih, čakalnih dobah (statično), ...;

- v naslednjem koraku gre za zamenjevanje klasičnega medija (pošta, telefon,..) z elektronskim. Elektronska pošta je značilen predstavnik naslednje faze v prehodu v e-poslovanje;

- transakcijski nivo, kjer se poslovne transakcije izmenjujejo elektronsko, že zahteva delno prenovo poslovnih procesov;

- višjo in težje izvedljivo raven povezovanja predstavlja faza integracije, ki polno uveljavlja standarde (protokoli, struktura podatkov, ki se izmenjujejo, enotni šifranti,…) in zahteva celovito prenovo procesov;

- faza pretvorbe pa predstavlja takšno prilagodljivost organizacije, ki mu omogoča dinamično vključevanje v različne oblike sodelovanja, tudi mrežne in navidezne povezave (virtualna organiziranost).

Čeprav je dodana vrednost prehoda bistveno višja od vložka, organizacije težko preidejo v fazo integracije, faza poslovne pretvorbe v virtualno organiziranost pa je v danem trenutku za večino organizacij zgolj utopična. Menim, da je razlog predvsem v vzvodu, ki omogoči

in vzpodbudi v prehod na višji nivo ne samo eno organizacijo, temveč njeno celotno okolje. Če bi zdravstveni sektor deloval samo po tržnih pravilih, bi zanj v celoti veljalo delovanje tekmovalnih sil, kot jih je leta 1980 opredelil M. Porter (pogajalska moč posameznikov, pogajalska moč dobaviteljev, nevarnost vstopa novih konkurentov in nadomestne storitve). Tako pa lahko tak vzvod iščemo tudi v nacionalni entiteti, ki nastopa kot avtoriteta in ima možnosti koriščenja denarnega, normativnega in političnega vpliva na okolje.

Pripravljenost na elektronsko poslovanje zdravstvenega in socialnega sektorja in stopnjo zrelosti v primerjavi z drugimi sektorji je po naročilu Evropske komisije v letih 2002-2007 izvajala Empirica (Stroetmann, (2003), European Commission (2004) in European Commission (2007)). Njihove raziskave so se s časom spreminjale, tako po številu vključenih držav, ki se je povečevalo, kot po vprašanjih. Slovenija je zajeta samo v raziskavi leta 2004.

Ustreznost tehnološke in pravne infrastrukture je relativna glede na zahteve procesov in z njimi povezanih aplikacij in jo lahko podajamo samo za dani trenutek. Tako na primer danes kazalec povezava z internetom ni več merodajen, temveč je primernejši pasovna širina, ki je na razpolago aplikacijam, ki se uporabljajo v posameznem poslovnem procesu. Okolje zdravstvene ustanove predstavlja zdravstveni sektor in subjekti, kot so definirani v poglavju 2.3.2. Zato je za pripravljenost na prehod na višjo raven elektronskega poslovanja v zdravstvu ključno stanje tistih subjektov, ki od povprečja najbolj odstopajo in na ta način zavirajo prehod na višjo raven. Te ustanove so tehnološko in kadrovsko bolj podhranjene in tudi sredstva, ki jih namenjajo informatiki, so manjša (Amarasingham et al., 2008). Zato pri posameznem področju tudi opozorim na takšne primere.

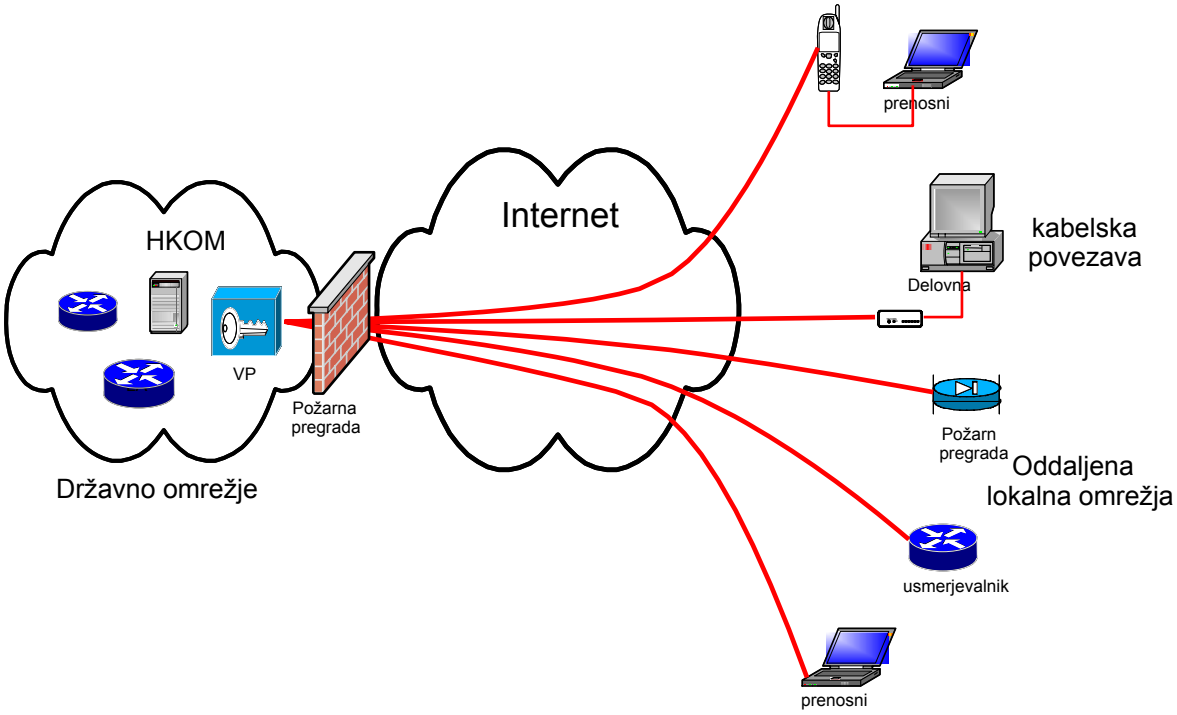
Ob ocenjevanju posameznih kazalcev sem vzel kriterij, po katerem kazalec potrjuje postavljeno hipotezo, če je delež neustreznih ustanov po številu zaposlenih v sektorju manjši od 5%.

3.1 Rezultati ankete

K sodelovanju sem povabil 1591 ustanov, ki spadajo v zdravstveni sektor glede na javno objavljene podatke (www.zzzs.si, 15.7.2006). Od tega sem 905 ustanov, za katere sem pridobil elektronske naslove, povabil k sodelovanju s pomočjo elektronske pošte, ostalim pa sem podatke za prijavo v aplikacijo Spletne ankete poslal preko navadne pošte.

Anketo sem izvajal v obdobju od 18.7.06 do 11.8.06 (24 dni). Anketiranje je potekalo s pomočjo aplikacije Spletne ankete nameščene na delovni postaji Ministrstva za zdravje v omrežju HKOM (hitro komunikacijsko omrežje državnih organov).

Slika 4: Koncept delovanja aplikacije Spletne ankete



Vir: Lasten

Anketiranec se je v internetno aplikacijo prijavil s podatki (uporabniško ime in geslo), ki sem mu jih poslal skupaj s povabilom in povezavo na spletno stran ankete. V obdobju izvajanja ankete je bila na spletnih straneh Ministrstva za zdravje med aktualnimi novicami objavljena tudi povezava na spletno stran ankete. Na povabilo k sodelovanju se je odzvalo 365 ustanov (23%), ki skupno zaposlujejo 31.190 oseb, kar je 74,7 % vseh zaposlenih v zdravstvenem sistemu (Statistični letopis 2006, 2008).

3.1.1. Vrste ustanov

Zdravstvena dejavnost je v Sloveniji organizirana v oblikah:

- javni zdravstveni zavodi; javno zdravstveno mrežo sestavljajo javni zavodi in koncesionarji. Zdravniško službo izvajajo pod enakimi pogoji. Pri zdravnikih v javnih zavodih in koncesionarjih so bolniki upravičeni do vseh pregledov in storitev brez neposrednega doplačila v okviru Pravil ZZZS in urejenega obveznega ter dopolnilnega zavarovanja;

- koncesionarji; zdravniki in zobozdravniki koncesionarji so sestavni del javne zdravstvene mreže in sklepajo koncesije za izvajanje javne zdravstvene službe. Delovnopravni status zdravnika za uporabnika ni pomemben, saj se zdravljenje pri koncesionarju v ničemer ne razlikuje od zdravstvene obravnave pri zdravniku ali zobozdravniku;

- zasebniki brez koncesije; ti zasebni zdravniki in zobozdravniki niso del javnega zdravstva in zato ne prejemajo javnih sredstev od Zavoda za zdravstveno zavarovanje Slovenije. Ne glede na to lahko tudi zasebni zdravniki brez koncesije napotijo svojega bolnika na zdravljenje na sekundarno ali terciarno raven, ko pri zdravljenju ugotovita, da je to strokovno utemeljeno. V anketi niso bili zajeti.

38. člen Zakona o zdravstveni dejavnosti določa tista področja, na katerih sploh ni dovoljeno opravljati zasebne zdravstvene dejavnosti, ne glede na dejstvo ali ima zasebni zdravnik koncesijo ali ne (z izjemo mrliško pregledne službe, ki se sme izvajati na podlagi koncesije in posebnega pooblastila). Sicer pa se smejo navedene dejavnosti izvajati samo v okviru javnih zdravstvenih zavodov.

Na vprašanje o vrsti ustanove je odgovorilo 359 anketirancev. Strukturo ustanov, ki so na vprašanje odgovorile prikazuje Tabela 5: Vrste ustanov, ki so posredovale podatke.

Tabela 5: Vrste ustanov, ki so posredovale podatke

Vrsta ustanove	**Frekvenca**	**Delež**
Javni zavod	114	32%
Zasebnik s koncesijo	231	64%
Drugo	14	3%
Skupaj odgovorov	359	100%

Vir: Lasten

3.1.2. Tipi anketiranih ustanov

Tip ustanove je opredelilo 358 anketirancev. V Tabela 6: Struktura odgovorov glede na tip ustanove, vidimo, da smo največ odgovorov prejeli od bolnišnic (80%), ter zdravstvenih domov (72%). Tabela prikazuje tudi strukturo ustanov, ki smo jih povabili k sodelovanju in deleže prejetih odgovorov glede na celoto.

Tabela 6: Struktura odgovorov glede na tip ustanove

Tip ustanove	Prispeli odgovori	Delež prispelih odgovorov	Povabljene ustanove	Delež odgovorov glede na povabljene
Bolnišnica	24	7%	30	80%
Zdravstveni dom	57	16%	79	72%
Lekarna	22	6%	105	21%
Zdravilišče	3	1%	19	16%
Socialni in posebni zavodi	46	13%	105	44%
Specialistična dejavnost	66	18%	262	25%
Zobozdravstvena dejavnost	63	18%	549	11%
Fizioterapija	25	7%	83	30%
Nega in patronaža	13	4%	68	19%
Reševalni prevozi	2	1%	16	13%
Drugo	37	10%	275	13%
Skupaj odgovorov	**358**	**100%**	**1591**	**23%**

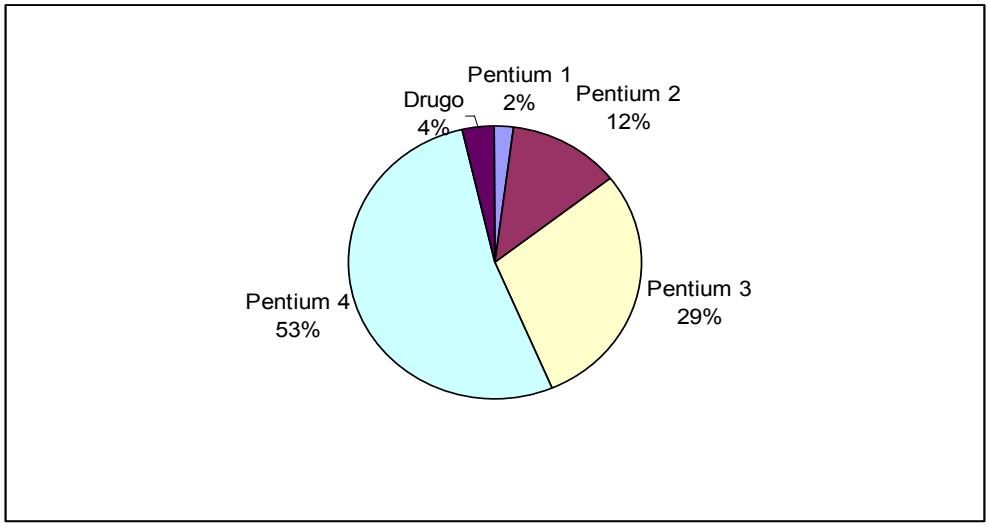
Vir: Lasten

3.1.3. Delovne postaje

Ustanove, ki so podale svoje odgovore na vprašanja o tipu delovnih postaj – računalnikov, imajo skupaj 12.502 računalnika s strukturo glede na tip procesorja, kot prikazuje Graf 1: Struktura delovnih postaj glede na tip procesorja. Delovne postaje s procesorjem generacije Pentium I, II in III ali podobnim so v celoti amortizirane in tudi neustrezne po kriteriju sprejemljivih stroškov vzdrževanja, saj stroški običajnega servisa presežejo vrednost računalnika.

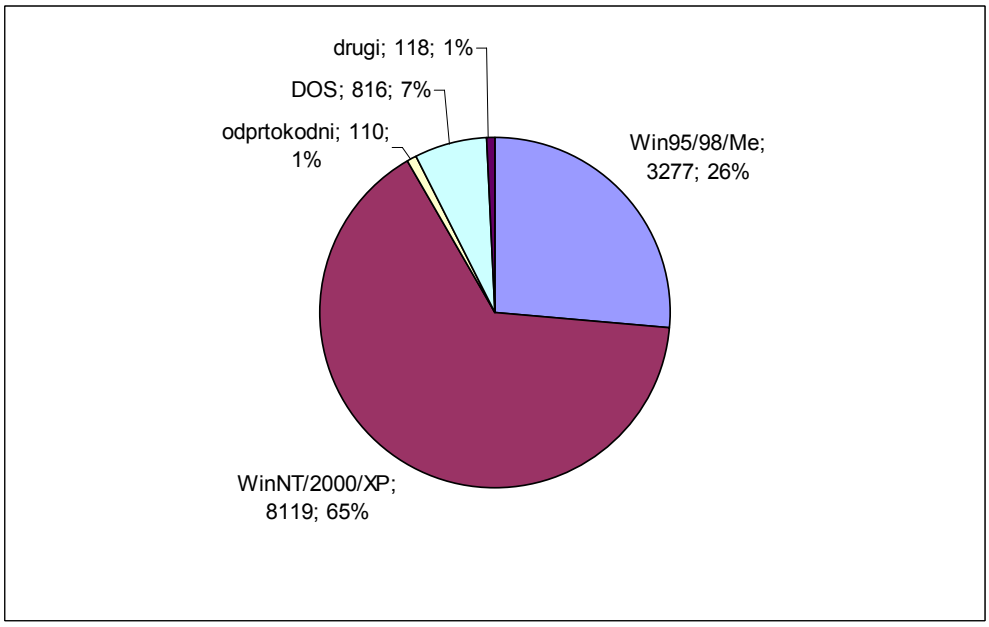
Na delovnih postajah se uporabljajo operacijski sistemi v strukturi, kot jo prikazuje Graf 2: Uporaba operacijskih sistemov na delovnih postajah. Opazen je sorazmerno velik del zastarelih DOS (angl. *Disc Operating System*) Microsoft operacijskih sistemov. Sklepamo lahko, da bo na teh računalnikih uvedba kakršnih koli sodobnih spletnih aplikacij nemogoča.

Graf 1: Struktura delovnih postaj glede na tip procesorja



Vir: Lasten

Graf 2: Uporaba operacijskih sistemov na delovnih postajah



Vir: Lasten

Predvidevamo lahko vsaj naslednje stroške, ki bodo povezani z zagotovitvijo ustreznih pogojev za implementacijo:

- zamenjava računalnikov, na katerih sedaj teče DOS in so po vsej verjetnosti tudi premalo zmogljivi za kakšno sodobnejšo sistemsko programsko opremo,

- zamenjava aplikacij, ki tečejo pod DOS,
- usposabljanje uporabnikov,
- sklenitev novih vzdrževalnih pogodb,
- reševanje novih varnostnih problemov.

Opazen je izrazito majhen delež odprtokodnih operacijskih sistemov (1%).

Potrebna bo zamenjava skoraj polovice delovnih postaj, ki so premalo zmogljive, imajo zastarel operacijski sistem in/ali stroški vzdrževanja presegajo njihovo vrednost. V okviru projekta prenove kartice zdravstvenega zavarovanja se je v te zamenjave že investiralo (Občasnik št.4, 19.10.2006 in Občasnik št.2, 7.5.2007).

3.1.4. Strežniki

Ustanove, ki so podale odgovore na vprašanja o strežnikih, to je 339 ustanov, imajo skupaj 420 strežniških operacijskih sistemov Microsoft in 118 drugih operacijskih sistemov.

Svoj **poštni strežnik** ima 34 ustanov, pri katerih se gibljejo velikosti trdega diska od 9GB do 2000GB. Polovica ustanov ima poštne strežnike z velikostjo trdega diska manj kot 73GB. Velikost RAM pomnilnika se giblje od 128MB do 4GB. Pri tem ima polovica strežnikov manj kot 884MB spomina. Hitrost procesorjev se giblje od 90MHz do 3200MHz. Polovica strežnikov pa ima procesor počasnejši od 2400MHz.

Datotečni strežnik ima 97 ustanov, pri katerih se velikosti trdega diska gibljejo od 1GB do 4818GB. Polovica ustanov ima poštne strežnike z velikostjo trdega diska manj kot 80GB. Velikost RAM pomnilnika se giblje od 128MB do 8192MB. Pri tem ima polovica strežnikov manj kot 774MB spomina. Hitrost procesorjev se giblje od 180MHz do 3600MHz. Polovica strežnikov pa ima procesor počasnejši od 2400MHz.

Večnamenske strežnike uporablja 67 ustanov, pri katerih se velikost trdega diska giblje med 1GB in 900GB. Polovica ustanov ima večnamenske strežnike z velikostjo trdega diska manj kot 80GB. Velikost RAM pomnilnika se giblje od 64MB do 4096MB. Pri tem ima polovica strežnikov manj kot 1024 MB spomina. Hitrost procesorjev se giblje od 100MHz do 3600MHz. Polovica strežnikov pa ima procesor počasnejši od 2800MHz.

Spletni strežnik ima 17 ustanov. Velikost trdega diska se giblje od 1GB do 500GB. Polovica teh strežnikov ima diske velikosti manjše od 66GB. Velikost RAM pomnilnika se giblje od 128MB do 2000MB. Pri tem ima polovica strežnikov manj kot 896MB spomina.

Hitrost procesorjev se giblje od 500MHz do 3200MHz. Polovica strežnikov pa ima procesor počasnejši od 2000MHz.

Večje ustanove imajo več različnih strežnikov.

3.1.5. Uporaba po profilih uporabnikov in tipu ustanove

Ustanove, ki so podale odgovore na anketna vprašanja, skupno zaposlujejo 31.190 ljudi različnih poklicev. V strukturi, kot jo prikazuje Tabela 7: Struktura zaposlenih in oseb, ki pri delu uporabljajo računalnik, pa 26.652 ljudi. Razliko med 31.190 in 26.652 predstavlja pomožno osebje npr. kuharice, hišniki, perice in drugi. V povprečju 68% zaposlenih v zdravstveni dejavnosti pri svojem delu uporablja računalnik. Razmerje števila zaposlenih in števila delovnih postaj je 1,44. V povprečju dela 1,44 ljudi z enim računalnikom, ki si ga delijo. Lahko rečemo da je računalnikov dovolj, saj gre v večini primerov vsaj za dvoizmensko delo (primer zdravstvenih domov) ali celo neprekinjen proces v primeru bolnišnic. Če bi vse zdravstvene ustanove delovale neprekinjeno, bi bilo ustrezno razmerje tudi, če bi prišel en računalnik na tri uporabnike.

Tabela 7: Struktura zaposlenih in oseb, ki pri delu uporabljajo računalnik

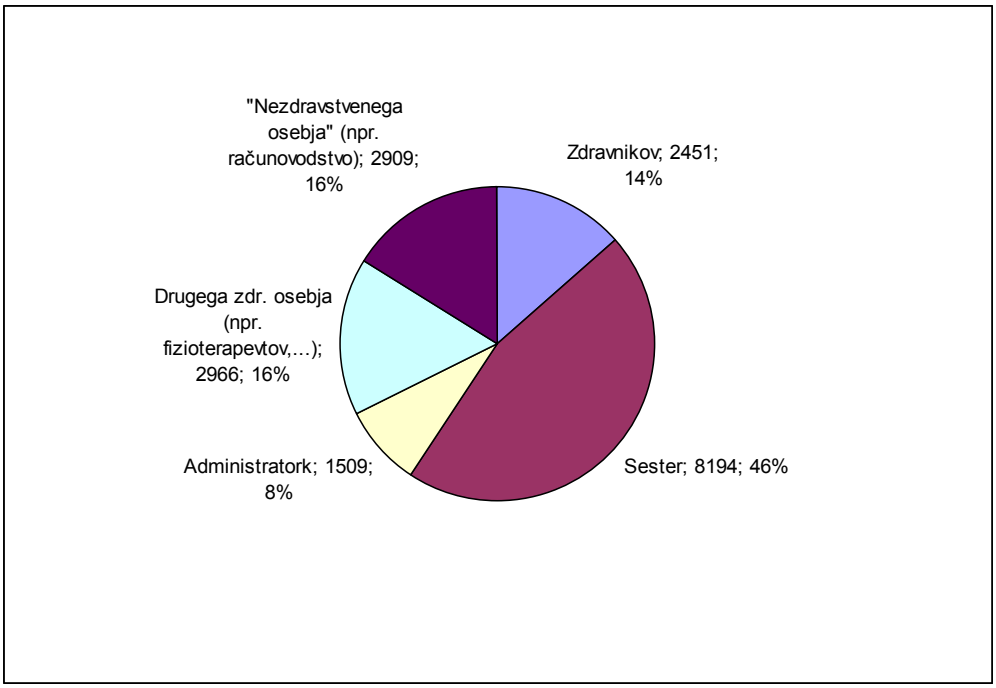
	Koliko je v vaši ustanovi zaposlenih?	**Število osebja, ki pri delu uporablja računalnik?**	**Koliko zaposlenih oseb v povprečju uporablja računalnik ?**
Zdravnikov	4.101	2.451	60%
Sester	9.825	8.194	83%
Administratork	1.610	1.509	94%
Drugega zdr. osebja (npr. fizioterapevtov,...)	4.981	2.966	60%
"Nezdravstvenega osebja" (npr. računovodstvo)	6.135	2.909	47%
Skupaj	**26.652**	**18.029**	**68%**

Vir: Lasten

Taylor in Leitman (2002) podajata podatke, da se v primarnem zdravstvu v povprečju evropske petnajsterice računalniki uporabljajo v 80 % primerov, pri tem na Finskem in Nizozemskem 100%, v Grčiji 52% in na Portugalskem 37%. Sicer je datum res oddaljen, vendar bi za Slovenijo že takrat lahko rekli, da vse zdravstvene ustanove uporabljajo računalnike, vsaj za pripravo podatkov obračuna na ZZZS. Torej je potrebno pogledati,

kdo uporablja računalnik, kar nam prikazuje Graf 3: Struktura uporabnikov računalnikov, in koliko, kar nam prikazuje Graf 4: Koliko pri svojem delu uporabljajo računalnik.

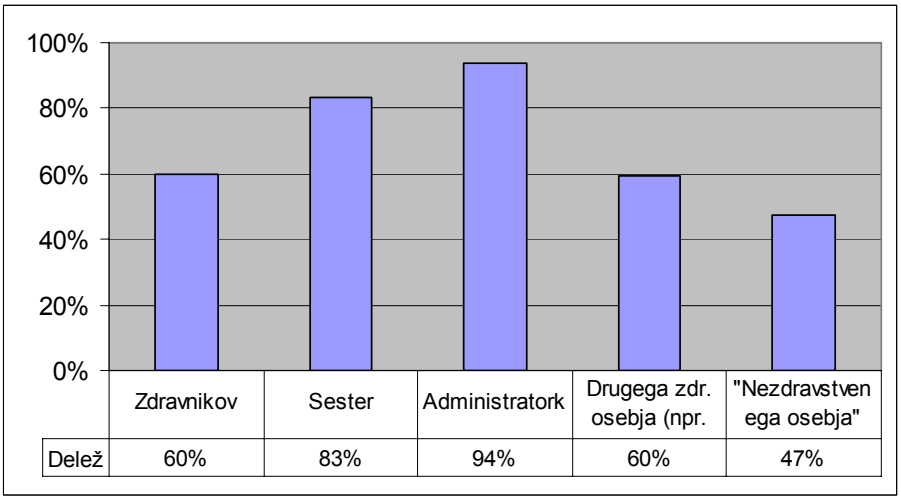
Graf 3: Struktura uporabnikov računalnikov



Vir: Lasten

Iz dobljenih podatkov lahko ugotovimo, da računalnik pri svojem delu največ uporabljajo administratorke (94%) in sestre (83%). Od zdravnikov jih računalnik uporablja 60 %, kar prikazuje Graf 4: Koliko pri svojem delu uporabljajo računalnik. Laerum, Ellingsen in Faxvaag (2001) v svoji raziskavi navajajo, da ima na Norveškem 93% zdravnikov v bolnišnicah na voljo računalnik v svojih prostorih, v 97% pa imajo do njega dostop v prostorih, namenjenih kliničnemu delu.

Graf 4: Koliko pri svojem delu uporabljajo računalnik



Vir: Lasten

Benson (2002) trdi, da zdravniki na primarni ravni več uporabljajo računalnike, ker jih je v manjše sisteme lažje uvesti, kot v velike (npr. bolnišnice). V Tabela 8: Primerjava deleža uporabnikov med primarno in sekundarno ravnjo vidimo, da je razmerje števila uporabnikov/številom računalnikov pri bolnišnicah večje kot pri zdravstvenih domovih, vendar to še ne pomeni, da so bolnišnice slabše opremljene. Bolnišnice namreč običajno obratujejo neprestano, zdravstveni domovi pa dvoizmensko ali še manj.

Tabela 8: Primerjava deleža uporabnikov med primarno in sekundarno ravnjo

Tip ustanove	**Vrsta ustanove**	**Št. rač.**	**Št. zaposlenih**	**Št. zap. / št. PCjev**	**Št. upor.**	**Št. upor./št. PCjev**	**Št. upor. / št. zap.**
Bolnišnica		7106	18980	2,67	11874	1,67	63%
Zdravstveni dom							
	Javni zavod	2545	4902	1,93	3155	1,24	64%
	Zasebnik s koncesijo	57	71	1,25	64	1,12	90%

Vir: lasten

Zanimiva je izrazita razlika v številu uporabnikov računalnikov med zaposlenimi v zasebnem sektorju (90%) na primarni ravni, v primerjavi z bolnišnicami (63%) ali javnimi zavodi na primarni ravni (64%). Zasebniki verjetno poskušajo povečati učinkovitost z uporabo informacijsko komunikacijskih tehnologij in poskušajo svoje procese informacijsko podpreti in imajo zato tudi več uporabnikov v strukturi zaposlenih. Podobno primerjavo sem naredil še po poklicih za zdravnike, sestre in administratorke, kar prikazuje Tabela 9: Primerjava uporabe računalnikov med poklici.

Tabela 9: Primerjava uporabe računalnikov med poklici

Tip ustanove	**Vrsta ustanove**	**Št. zdravnikov**	**Zdravniki uporabniki PC**	**Delež**
Bolnišnica		2694	1929	72%
Zdravstveni dom				
	Javni zavod	1108	278	25%
	Zasebnik s koncesijo	34	27	79%
		Št. sester	**Sestre uporabnice PC**	**Delež**
Bolnišnica		6401	5133	80%
Zdravstveni dom				
	Javni zavod	2225	2165	97%
	Zasebnik s koncesijo	33	30	91%
		Št. administratork	**Administratorke uporabnice PC**	**Delež**
Bolnišnica		1425	1330	93%
Zdravstveni dom				
	Javni zavod	43	42	98%
	Zasebnik s koncesijo	5	5	100%

Vir: Lasten

Zanimivo je, da obstajajo pomembne razlike med uporabo računalnikov pri zdravnikih na primarni ravni (25 %) in sekundarni ravni (72 %) zdravstvenega varstva. Pomembna

razlika obstaja tudi med zdravniki v javnih zavodih (zdravstveni domovi), ki računalnik uporabljajo le v 25 %, in zdravniki zasebniki s koncesijo, ki uporabljajo računalnik v 79 %.

Uporaba med zdravniki na sekundarni ravni in koncesionarji na primarni ravni je primerljiva s stanjem v razvitih članicami EU pred leti (Taylor & Leitman, 2002). Ta časovni razkorak cca šestih let bi lahko vzeli kot oceno našega zaostajanja za njimi.

Dobljene vrednosti lahko služijo kot izhodišče za razpravo o dosedanjih pomanjkljivih spodbudah za izvajalce na primarni ravni, predvsem za zdravstvene zavode. Razloge za majhen delež uporabe IKT s strani zdravnikov na primarni ravni bi morda lahko iskali v pomanjkljivi funkcionalnosti obstoječih elektronskih kartotek, neobstoječih storitvah izmenjave podatkov med izvajalci (recepti, napotnice, odpustna pisma ipd.), neveščosti zdravnikov pri uporabi IKT, premajhnega zavedanja prednosti IKT in v delovnih procesih.

Zdravnik na primarni ravni potrebuje za delo (tj. vnos, obdelavo in prikaz) z bolnikovimi podatki, elektronski zdravstveni karton, podporo pri kliničnem delu (sistemi za podporo pri odločanju, ekspertni sistemi, sistemi za opominjanje, iskalniki informacij ipd.) ter izmenjavo podatkov z ostalimi udeleženci v zdravstvenem sistemu in uporabnikom zdravstvenih storitev (odpustna pisma, napotnice, recepti, naročanje storitev, laboratorijski izvidi ipd.). Na drugi strani potrebuje ustrezno opremo: osebni računalnik, dostop do interneta in lokalnega omrežja, opremo za zagotavljanje avtentikacije zdravnika in (glede na organizacijo dela lahko tudi) uporabnikov zdravstvenega sistema (čitalec kartic – profesionalnih in uporabniških, digitalni certifikat za zdravnika in ostalo medicinsko osebje po potrebi). Delovni proces zdravnika v bolnišnici je bolj raznolik. Zaradi večje administrativne podpore temu namenjenega osebja potrebuje manj organizacijskih orodij, zato pa več nestrukturiranih storitev (predvsem spletnih, kot so iskanje strokovnih informacij, telekonzultacije, izmenjava visokoresolucijskih slik – teleradiologija in druge). Zdravniki se pogosto premalo zavedajo prednosti, ki jih prinaša delo s podatki v elektronski obliki: enkratni vnos, dostopnost, transparentnost podatkov, možnosti iskanja, nadgradnja z inteligentnimi sistemi za opravljanje rutinskih nalog, kot je na primer iskanje in obveščanje o kontrolnih pregledih. Posledično obstaja nevarnost, da med privzemanjem IKT prehitro obupajo, predvsem v primerih, ko je delovni proces izrazito storilnostno naravnan. Kot primer bi lahko navedli vnos podatkov, ko mnogi zdravniki menijo, da je pisanje s tipkovnico prepočasno in ne upoštevajo prihranka časa zaradi podatkov v elektronski obliki v prihodnje (npr. predpisovanje stalne terapije, ko namesto ponavljajočega se pisanja receptov zadošča le klik ali dva). O možnostih IKT je potrebno načrtno osveščanje in izobraževanje zdravnikov v vseh korakih izobraževanja (Meglič et al., 2007).

3.1.6. Aplikacije in funkcionalnosti

Tabela 10: Uporaba aplikacij prikazuje, koliko ustanov uporablja katere aplikacije ter katere nameravajo začeti ali jih želijo začeti uporabljati v roku dveh let. Vsi, ki so na vprašanje odgovorili (230), uporabljajo aplikacije, namenjene fakturiranju. Naslednje najpogostejše aplikacije so namenjene poročanju statističnih podatkov na IVZ RS in Statistični urad RS. Najbolj zaželene aplikacije pa so elektronski zdravstveni karton, naročanje pacientov in čakalne liste, ter napotnice in naročila laboratorijskih testov.

Naročanje pacientov preko spleta, čakalne vrste, VoIP, eNapotnice, eOdpustna pisma, naročila laboratorijskih testov so aplikacije, ki v današnjem času niso tehnološki čudeži, njihova cena je sprejemljiva, njihova uvedba bi prinesla veliko zadovoljstva, povečala učinkovitost in zmanjšala stroške. Primere dobrih praks, kot so telekonzultacije v transfuzijski službi je potrebno organizacijsko podpreti in razširiti na nacionalni nivo (Breskvar et. al, 2006).

Tabela 10: Uporaba aplikacij

Tip aplikacije	Število ustanov, ki aplikacijo uporablja	Število ustanov, ki jo namerava uporabljati v roku 1-2let
Naročilo laboratorijskih testov	18	60
Napotnice	18	63
Odpustna pisma	18	57
Fakturiranje	230	21
Statistika (npr z IVZ, SURS,...)	121	34
Elektronski karton pacienta	17	72
Izmenjava digitalnih RTG slik (npr PACS)	22	58
Posvetovanja/ videokonference (zvok in slika)	19	62
Izmenjava kardioloških slik, EKG,..	17	56
VoIP – uporaba informacijskega omrežja za prenos zvoka, telefonske storitve,.	17	59
Naročanje pacientov preko spleta in čakalne liste	17	69
Druge aplikacije	31	35

Vir: lasten

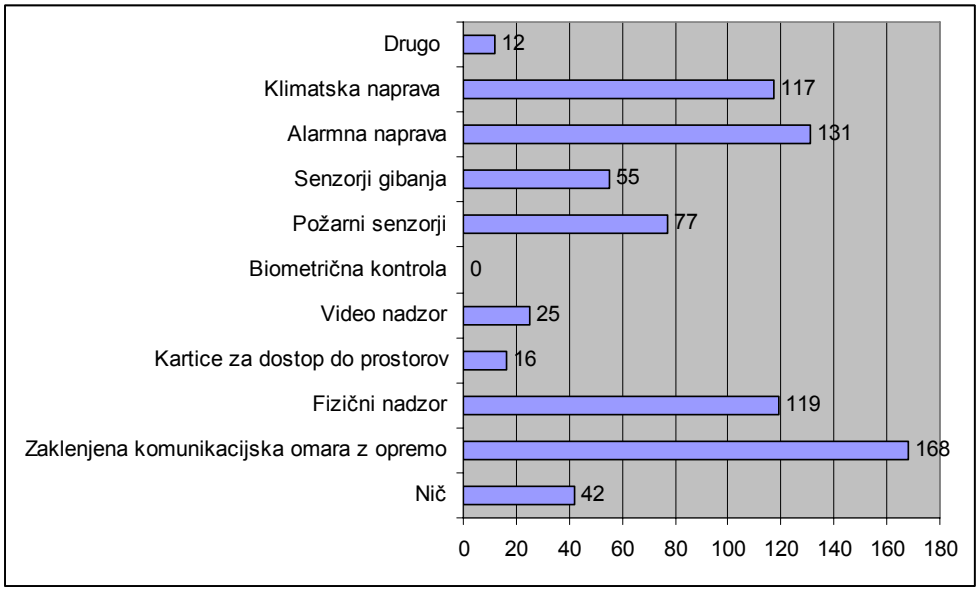
3.1.7. Varovanje ključne informacijsko komunikacijske opreme

V anketi je na vprašanje: Kako zagotavljate varovanje ključne informacijsko komunikacijske opreme, odgovorilo 340 ustanov. Odgovore prikazuje Graf 5: Načini varovanja ključne informacijske komunikacijske opreme. Anketiranec je lahko izbral tudi več odgovorov oziroma načinov, na katere izvaja varovanje. Zaskrbljujoče je dejstvo, da 42 (11%) ustanov sploh ne izvaja nobenega posebnega varovanja svoje ključne informacijske opreme. Ker te ustanove predstavljajo samo 0,34% zaposlenih zdravstvenega sektorja, kazalec potrjuje hipotezo. Dvanajst ustanov (3%) pa navaja, da izvajajo druge načine varovanja med drugim:

- poseben zaklenjen prostor z omejenim dostopom,
- varovanje objekta z varnostno službo,
- alarmna naprava v sklopu objekta,
- senzorji toplote in izliva vode.

Ustanove bi potrebovale priporočila za področje informacijske varnosti.

Graf 5: Načini varovanja ključne informacijske komunikacijske opreme



Vir: Lasten

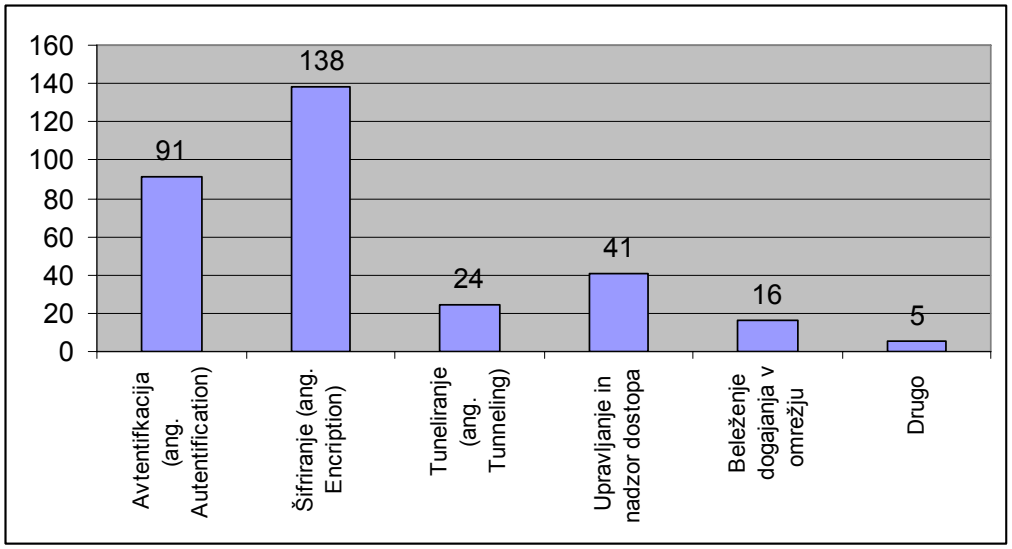
Računalniška soba je prostor, kjer delujejo strežniki, mrežna oprema in z njima povezana oprema, skratka ključna informacijsko komunikacijska oprema. Računalniška soba potrebuje posebno varovanje pred vdorom. Nekateri jo imenujejo tudi varna soba. Fizičen dostop do računalniške opreme predstavlja potencialno vstopno točko v sistem in mora

zato biti strogo nadzorovan. Vsak dostop (vhod) mora biti zato opremljen s kontrolo dostopa. Senzorji gibanja in video kamere se uporabijo za dokumentiranje vseh fizičnih aktivnosti v prostoru. Če je možno, naj bodo ohišja strežnikov in komunikacijskih omar opremljena s ključavnicami. Uporaba ohranjevalnikov zaslona, ki zahtevajo geslo, naj se uporablja povsod, še posebej pa pri opremi, ki se jo pušča brez nadzora – strežniki in delovne postaje. Priporočljiva je tudi uporaba gesel na nivoju BIOSa in »BOOT level« gesel ali »power on« gesel.

3.1.8. Zaščita podatkov, ki se izmenjujejo

V anketi sem ustanove povprašal, kako vršijo zaščito podatkov, ki jih izmenjujejo. Prejel sem 204 odgovore. Ustanove so lahko izbrale več različnih načinov zaščite. Rezultate prikazuje Graf 6: Izvajanje zaščite pri izmenjavi podatkov.

Graf 6: Izvajanje zaščite pri izmenjavi podatkov



Vir: Lasten

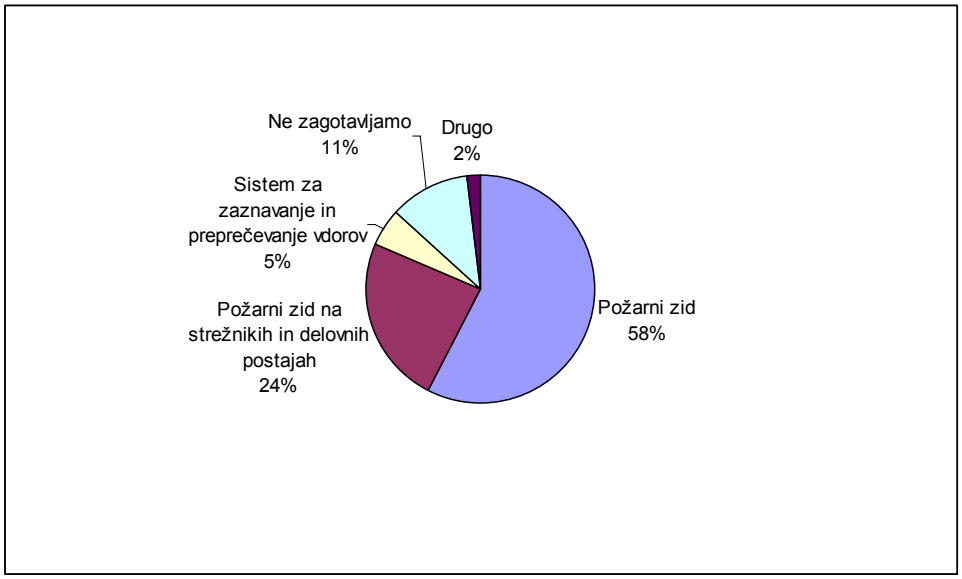
Napadalci izkoriščajo predvsem ranljivost zaščitnih mehanizmov ali pomanjkljivo uporabo in slabe nastavitve le-teh. Za zagotavljanje čim višje ravni varnosti omrežij moramo uporabiti vse zaščitne mehanizme, ki so na voljo. Razpolagati moramo z novejšimi bolj zmogljivimi napravami ali vsaj nadgrajevati programsko in strojno opremo.

Napadi na omrežje so različni, od pregledovanja (skeniranja) vrat za ustvarjanje točne slike omrežja, ter zaznavanja možnih slabosti do popolne blokade z napadom iz več računalnikov hkrati DDOS (Distributed Denial of Service).

Požarni zid je sistem, zasnovan za preprečitev nepooblaščenega dostopa do notranjega omrežja ali intraneta. Požarne zidove je mogoče vpeljati na strojno ali programsko opremo ali kombinacijo obojega. V kolikor je nastavljen v skladu z varnostno politiko, nudi najboljšo zaščito omrežja pred zunanjimi napadi in vdori. Tako omogoča zaznavanje vdorov in njihovo blokiranje, filtriranje vsebine (npr. prihajajoče nezaželene pošte), tvorjenje navideznih zasebnih omrežij (VPN) in druge vrste zaščite.

Na anketno vprašanje: Kako ustanova izvaja varovanje pred zunanjimi vdori v informacijski sistem, je odgovorilo 345 ustanov. Informacija, ki kliče po osveščanju ustanov, je, da 39 ustanov (11%) ne izvaja nikakršne zaščite pred vdori. Te ustanove predstavljajo 0,36% zaposlenih v sektorju. Kazalec potrjuje hipotezo. Anketiranci v 2% primerov navajajo druge načine varovanja pred zunanjimi vdori, med drugim, da računalnika(ov) nimajo povezanega v omrežje. Strukturo odgovorov prikazuje Graf 7: Struktura načinov varovanja informacijskih sistemov pred zunanjimi vdori.

Graf 7: Struktura načinov varovanja informacijskih sistemov pred zunanjimi vdori



Vir: Lasten

Po podatkih raziskave (Verduyn, 2005) v letu 2005 v ZDA:

- 98,2% organizacij uporablja protivirusno zaščito (podjetja ter vladne in druge ustanove),
- 90,7% organizacij je imelo pred omrežjem pravilno postavljene požarne zidove,
- 75% je tudi aktivno uporabljalo protivohunsko programje in protioglaševalski program.

3.1.9. Varovanje dostopa do podatkov

Na anketno vprašanje: Kako ustanova zagotavlja varovanje dostopa do podatkov, je odgovorilo 355 ustanov. Ustanova je na vprašanje lahko podala več odgovorov oziroma izbrala več načinov, ki jih izvaja, kar prikazuje Tabela 11: Načini varovanja dostopa do podatkov. Najpogostejši način varovanja dostopa do podatkov je uporaba gesel in različnih identifikacijskih kartic. Biometrične rešitve za varovanje dostopa do podatkov imajo implementirane samo v eni ustanovi.

Tabela 11: Načini varovanja dostopa do podatkov

Načini	**Frekvenca**
Gesla	346
Kartice	114
Biometrika	1
Nič	3
Drugo	2

Vir: Lasten

Pod drugo je anketiranec lahko navedel, na kakšen način varuje dostop do podatkov. Pridobljeni odgovori navajajo mehansko zaklepanje prostora. Kljub temu, da 3 ustanove, ki predstavljajo 0,33% zaposlenih v zdravstvenem sektorju, ne izvajajo nobenega varovanja dostopa do podatkov, kazalec potrjuje hipotezo.

Gesla so gotovo eden od nivojev zaščite, vendar se poraja vprašanje, kako dobro se le-te varuje. Z namenom zagotavljanja večje varnosti se običajno zahteva minimalna dolžina in kombinacija velikih in malih črk ter številk. Seveda vsa varnostna priporočila ne pomenijo nič, v kolikor uporabnik gesla le-tega zapiše npr. na listek, ki ga ima nalepljenega na monitor. Z namenom povečanja varnosti se največkrat uvede časovna omejenost veljavnosti za gesla.

Nadzor dostopa do podatkov, računalnikov in omrežja in uveljavljanje pravice dostopa naj se izvaja na osnovi tega:

- kaj vemo – geslo,
- kaj imamo - ključ, identifikacijska kartica,
- kdo smo - prstni odtisi, vzorci krvnih žil v mrežnici, barva glasu,
- šifriranje podatkov – šifre.

Obvladovanje dostopa mora izhajati iz poslovnih potreb, ter hkrati zagotavljati jasno porazdeljeno odgovornost uporabnikov in omogočati jasno upravljanje dostopa do operacijskih sistemov in uporabniških rešitev tako pri delu v poslovnih prostorih, mobilnem poslovanju in delu na daljavo. Obvladovanje dostopa pomeni tudi nadzor nad dostopom do sistemov in podatkov, ter njihovo uporabo. Glede na politiko zaščite lahko razdelimo sisteme na štiri skupine (Jaklič, 2002):

- uporabnik dobi pravico dostopa do podatkov, ko le-te potrebuje (po potrebi). Pravica je omejena na natanko tiste podatke, ki jih potrebuje.

- podatki so v največji možni meri dostopni uporabnikom. To pa ne pomeni, da imajo vsi uporabniki pravico do vseh podatkov, vendar so posameznemu uporabniku nedostopni le tisti, ki res morajo biti nedostopni.

- odprti pristop zaščite podatkov. Praviloma imajo uporabniki pravico dostopa do vseh podatkov, z izjemo tistih, ki so eksplicitno zaščiteni.

- zaprti pristop zaščite podatkov. Praviloma uporabniki nimajo pristopa do nobenega podatka, z izjemo tistih, za katere dobijo posebno dovoljenje. Očitno omogoča ta pristop boljšo zaščito, saj pri odprtem pristopu lahko pozabimo zaščititi določen del podatkovnega vira, s tem pa lahko vsi uporabniki dostopajo do teh podatkov. Tak pristop je priporočljiv tudi pri nastavitvah opreme npr. požarnega zidu, torej je prepovedano vse, kar ni posebej dovoljeno.

Večinoma so pravice dostopa do podatkov vezane na posameznega uporabnika. Zaradi enostavnejšega vzdrževanja lahko uporabnike, ki imajo enake pravice, združimo v skupine in potem vežemo pravice na skupino. Uporabnik ima lahko do posameznega podatka različne pravice dostopa in sicer gre za poljubno kombinacijo naslednjih vrst dostopa: definiranje, doseganje, vnos, brisanje in spremembe.

Glede na pogoje, pod katerimi sme uporabnik dostopati do podatkov, ločimo naslednje vrste zaščite:

- vsebinsko odvisna zaščita (dovoljenje za doseganje dela podatkovnega vira je odvisno od vsebine podatkov),

- vsebinsko neodvisna zaščita (pravice dostopa so vnaprej določene za vsakega uporabnika in podatkovni element),

- kontekstno odvisna zaščita (isti podatkovni element je v določenem kontekstu dostopen posameznemu uporabniku, v drugem kontekstu pa istemu uporabniku ne,

- zaščita statističnih podatkovnih baz.

V kontekstu varnosti in zaščite podatkov govorimo tudi o zaščiti statističnih podatkovnih baz. Statistične podatkovne baze omogočajo uporabniku, da izvaja na podatkih o posameznih objektih le statistične operacije, kot npr. vsota, povprečje. Z drugimi besedami, uporabnik lahko dobi le sumarne podatke, ne pa tudi individualnih podatkov, to je podatkov o posameznikih. Žal pa ni dovolj, da uporabniku ne dovolimo doseganja podatkov o posameznikih, saj je mogoče iz več sumarnih podatkov sklepati na podatke o posameznikih (Jaklič, 2002).

3.1.10. Izdelava varnostnih kopij

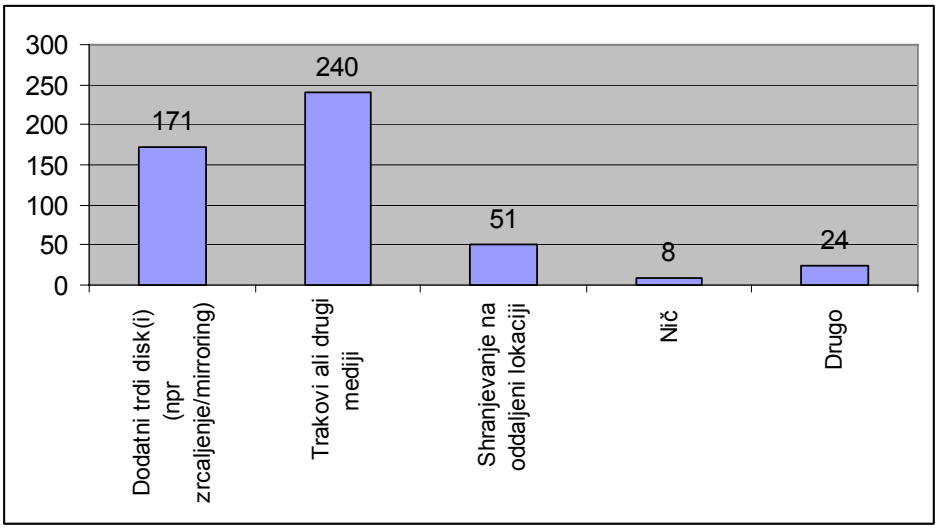
Zaradi različnih razlogov se nam lahko zgodi, da se podatkovni vir poškoduje. Magnetni trak se razmagneti, računalnik uniči strela,… Za take primere moramo zagotoviti način, da lahko podatkovni vir obnovimo. Za računalniško podprto bazo podatkov je to največkrat občasna izdelava rezervne kopije, hkrati pa elektronsko beležimo vsako aktivnost, ki je bila narejena na podatkovni bazi od prejšnje izdelave rezervne kopije. Na podlagi obojega lahko v primeru nesreče - poškodovanja baze le-to vrnemo v stanje pred nesrečo. Pogostost izdelovanja rezervne kopije je odvisna od varnostne politike organizacije in ne more biti prepuščena skrbniku podatkovne baze.

Poleg tega, da vemo, kako bomo podatke rešili v primeru nesreče, moramo imeti tudi načrt, kako bomo ukrepali v času, ko podatki ne bodo dostopni, torej do končanja obnove vira. Poslovanje mnogih organizacij je neposredno odvisno od dostopa do podatkov. V skrajnih primerih imajo nekatere organizacije ves čas dve enaki kopiji istega podatkovnega vira.

Nadzor celovitosti, varnosti, ter obnavljanje in nadgradnjo celostno obravnavamo kot zaščito podatkovnih virov. Pri tem z nadzorom celovitosti zaščitimo vir pred tem, da bi ga uporabnik nenamerno privedel v nekonsistentno stanje. Varnost zagotavlja zaščito pred namernimi poskusi oškodovanja. Z obnavljanjem in nadgradnjo pa odpravljamo posledice nesreč.

Na anketno vprašanje: Kako zagotavljate varnostno kopiranje in hranjenje podatkov, je odgovorilo 337 ustanov. Ustanova je lahko podala več odgovorov oziroma načinov. Anketiranci odgovarjajo, da podatke shranjujejo tudi na zgoščenki CD (angl. *Compact Disk*), DVD (angl. *Digital Versatile Disc*) in ZIP medijih, ter celo USB (angl. *Universal Serial Bus*) pomnilnikih in disketah. V 8 ustanovah pa varnostnega kopiranja sploh ne izvajajo. Te ustanove na srečo predstavljajo samo 0,31% vseh zaposlenih v zdravstvenem sektorju. Kazalec potrjuje hipotezo. Odgovore prikazuje Graf 8: Struktura načinov varnostnega kopiranja.

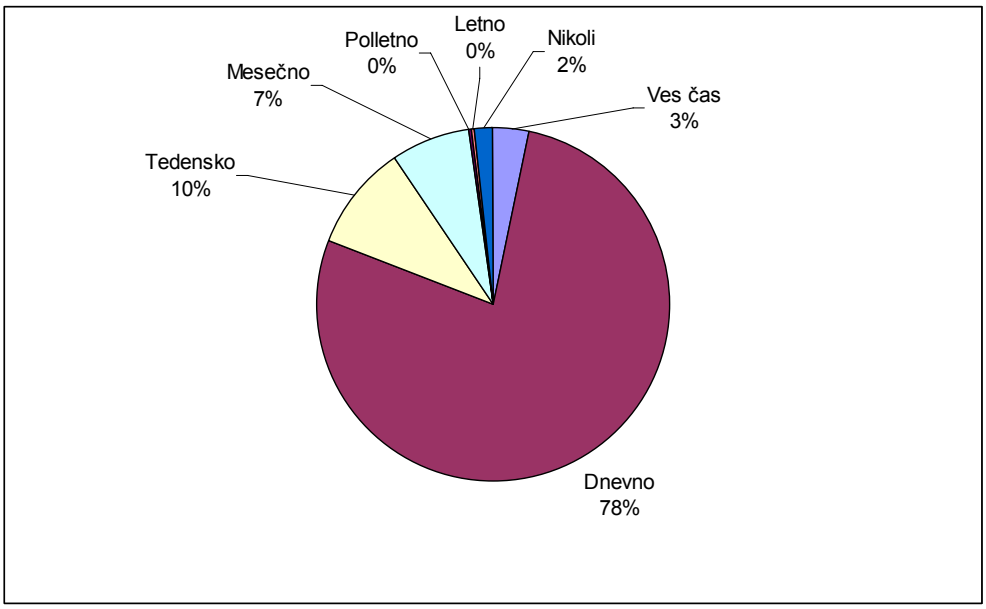
Graf 8: Struktura načinov varnostnega kopiranja



Vir: Lasten

Na anketno vprašanje: Kako pogosto ustanova vrši varnostno kopiranje podatkov, je odgovorilo 356 ustanov. Strukturo odgovorov prikazuje Graf 9: Kako pogosto ustanove vršijo varnostno kopiranje podatkov.

Graf 9: Kako pogosto ustanove vršijo varnostno kopiranje podatkov



Vir: Lasten

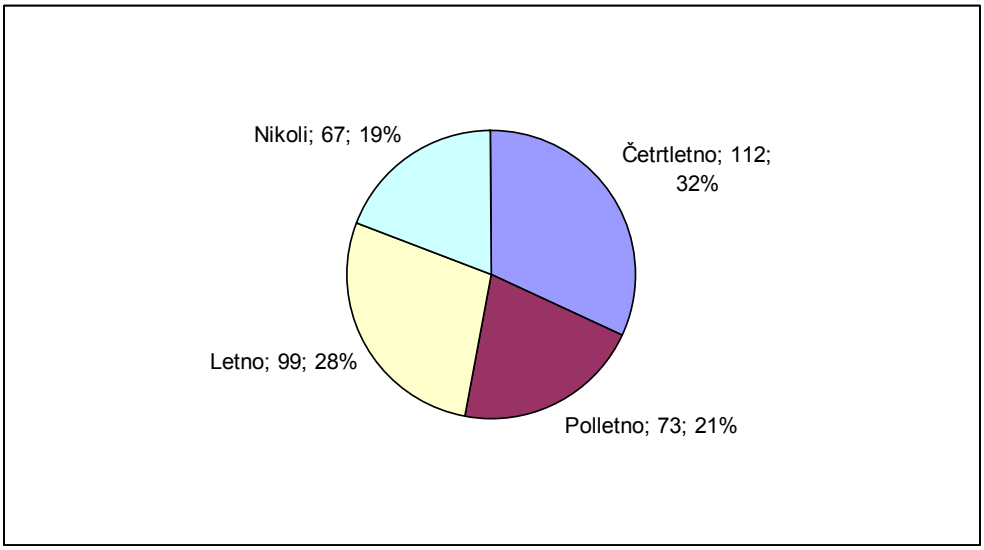
Obilica podatkov je sicer blagor, a iz vidika varovanja ter ohranjanja berljivosti formata tudi gorje. Zato se odločamo, da shranimo samo sumarne podatke, detajlne pa arhiviramo

ali zavržemo. Pri tem seveda spoštujemo zakonske zahteve. V kolikor podatke uničujemo, je potrebno v skladu z navodili varnostne politike, posebno za občutljive podatke, to opraviti tako, da jih ni možno restavrirati po nobeni znani metodi. Sodoben elektronski arhiv bo moral obvladovati in varno hraniti obe vrsti dokumentov, tako izvorne papirne (tudi slike) kot tudi izvorno elektronske dokumente.

Varno hranjenje dokumentov na enem mestu je vstopnica, ki poleg prihrankov na področju hranjenja dokumentacije omogoča narediti naslednji korak – upravljanje poslovnih procesov, v katerih dokumenti nastopajo.

Na anketno vprašanje: Kako pogosto kontrolirajo arhivske podatke (berljivost medija,…), je odgovorilo 351 ustanov. Kar 67 (19%) ustanov svojih arhivskih podatkov nikoli ne preveri. Te ustanove predstavljajo 3,99% zaposlenih v zdravstvu, kar pa je manj od postavljene meje 5%, zato kazalec potrjuje hipotezo. Odgovore prikazuje Graf 10: Kako pogosto vršite kontrolo arhivskih podatkov.

Graf 10: Kako pogosto vršite kontrolo arhivskih podatkov



Vir: Lasten

3.1.11. Varnost pred virusi

Na anketno vprašanje: Kako ustanova zagotavlja varnost pred virusi, je odgovorilo 353 ustanov. Možnih je bilo več odgovorov oziroma načinov, ki jih prikazuje Tabela 12: Načini varovanja pred virusi. Uporabniki navajajo tudi druge načine, ter kombinacije načinov.

Tabela 12: Načini varovanja pred virusi

Način	Frekvenca
Na strežnikih	163
Na delovnih postajah	254
Pri dostopu do interneta	193
Nič	11
Drugo	3

Vir: Lasten

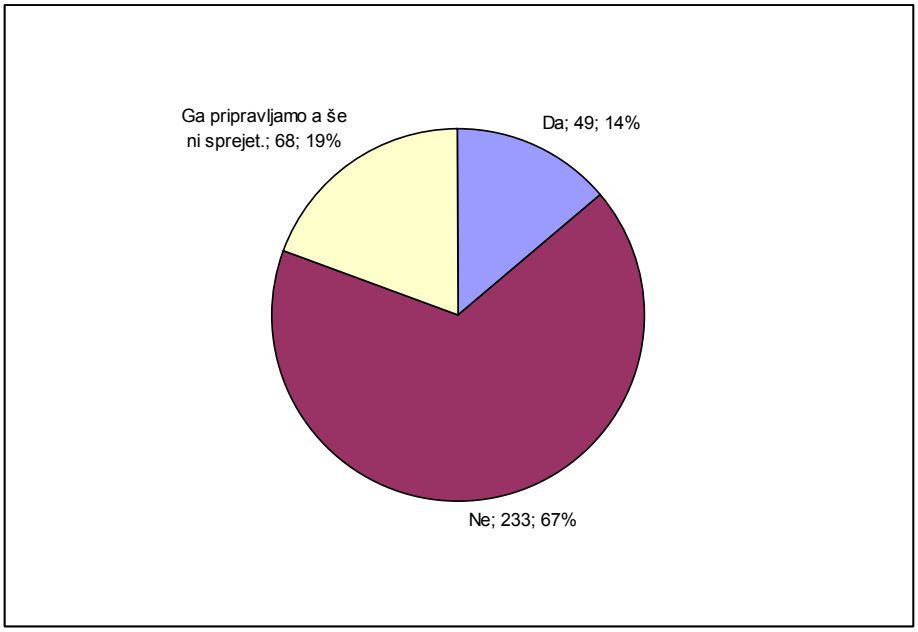
Glede na to, da je tveganje zlonamerne kode, ki jo večina laikov razume pod izrazom računalniški virus, precej visoko, sem pričakoval, da ne bo nobene ustanove, ki ne bi imela neke zaščite. Vendar 11 ustanov (3,1%) v ta namen ne izvaja nikakršne zaščite. Te ustanove zaposlujejo 0,2% vseh zaposlenih v zdravstvenem sektorju. Gre za manjše zasebne ustanove, ki se verjetno zanašajo na zaprtost svojih sistemov. Ker do sedaj še nihče ni bil obsojen in kaznovan s kakšno konkretno kaznijo za izgubo ali razkritje osebnih podatkov in posledično ponovljene preiskave bolnika, se pojavljajo tudi takšne ustanove.

3.1.12. Varnostna politika

Namen vprašanja je bil ugotoviti delež anketiranih ustanov, ki imajo sprejeto ustrezno politiko kot osnovo in usmeritev nadaljnjim aktivnostim.

Na anketno vprašanje: Ali imate sprejet dokument – varnostno politiko za področje informatike, je odgovorilo 350 ustanov. Graf 11: Ali imate sprejet dokument - varnostno politiko za področje informatike prikazuje odgovore. Ustanove, ki nimajo sprejete varnostne politike (233), niti je ne pripravljajo, predstavljajo 50,13% celotnega zdravstvenega sektorja. Kazalec ne potrjuje hipoteze.

Graf 11: Ali imate sprejet dokument - varnostno politiko za področje informatike



Vir: Lasten

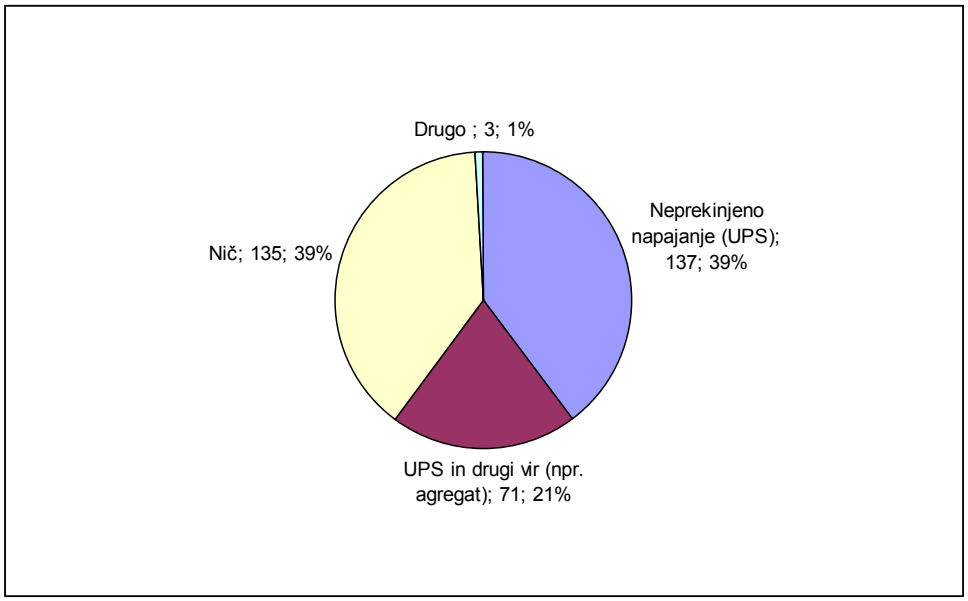
OZIS do sedaj ustanovam v zdravstvenem sektorju za področje informacijske varnosti ni dal še nobene smernice. Predlagam, da upoštevajo priporočila Agencije za pošto in elektronske komunikacije RS, ki je pripravila in na svojih spletnih straneh (www.apek.si) objavila Smernice za zagotavljanje varnosti omrežij elektronskih komunikacij in informacijskih sistemov, kjer priporoča, da:

- ustanova dokumentira, vzpostavi, vzdržuje, nadzoruje in nenehno izboljšuje sistem upravljanja informacij, kot je to opisano v naslednjih dokumentih:
  - standardi SIST ISO/IEC 27001:2006 in SIST/IEC 17799:2005;
  - priporočilo ITU-T X.1051.
- ustanova izdela načrt neprekinjenega poslovanja in načrt za ponovno vzpostavitev, ki sta osnovana na varnostni politiki in sistemu za upravljanje informacij ter ju dokumentira, vzpostavi, vzdržuje, nadzoruje in nenehno izboljšuje,
- se ustanova prepriča ali njeni postopki in infrastruktura ustrezajo zahtevam teh smernic.

3.1.13. Oskrba z energijo

Odgovor na anketno vprašanje: Kako ustanova zagotavlja delovanje informacijskega sistema v primeru izpada napajanja, je posredovalo 346 ustanov. Strukturo odgovorov podaja Graf 12: Struktura načinov zagotavljanja delovanja v primeru izpada napajanja. Kot druge načine so anketiranci navedli uporabno prenosnih računalnikov z vgrajenimi baterijami. Kar 135 ustanov (39%) informacijskih sistemov ni pripravljenih za delo v primeru izpada napajanja. Gre za majhne ustanove, ki skupno predstavljajo 1% zdravstvenega sektorja po zaposlenih. Kazalec potrjuje hipotezo. Izpad napajanja je eden od pogostejših tveganj, ki so mu izpostavljene ustanove.

Graf 12: Struktura načinov zagotavljanja delovanja v primeru izpada napajanja



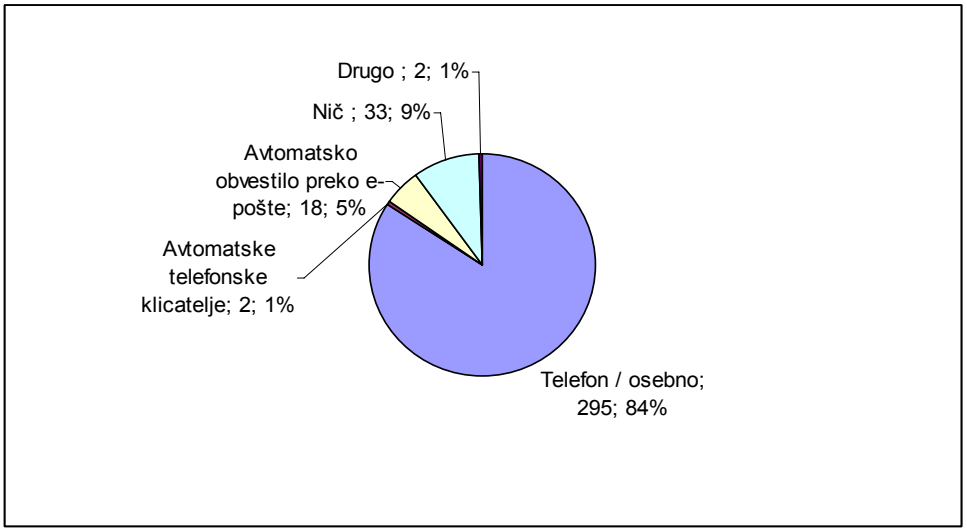
Vir: Lasten

Na anketno vprašanje: Koliko časa potrebujete za vzpostavitev informacijskega sistema pri hudem izpadu, je odgovorilo 250 ustanov.

V primeru hude okvare ustanove v povprečju potrebujejo 11,3 ure za vzpostavitev informacijskega sistema. Mogoče se zdravniki zanašajo na svojo usposobljenost za delo v izrednih razmerah.

Na anketno vprašanje: Kakšen način ustanove uporabljajo za obveščanje o izpadu informacijskega sistema, je odgovorilo 350 ustanov. Najpogosteje osebno oziroma s pomočjo telefona ustrezno urgirajo, kar prikazuje Graf 13: Obveščanje o izpadu informacijskega sistema.

Graf 13: Obveščanje o izpadu informacijskega sistema



Vir: Lasten

Zaradi kritičnih poslovnih procesov (reševanje življenj) bi pričakoval, da bodo zdravstvene ustanove vpeljevale elemente neprekinjenega poslovanja podobno kot npr v bančnih institucijah, pa ga ne. Mogoči razlogi za takšno stanje so (Graselli, 2006):

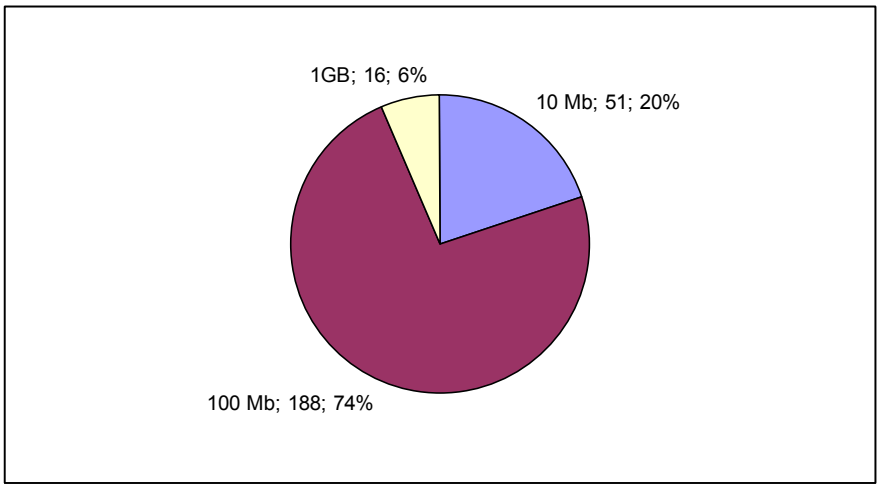
- informatika v zdravstvu še nima zadosti pomembne vloge v ključnih procesih,
- ključni procesi so zadosti dobro pokriti z ročnimi /alternativnimi postopki,
- zakonodajalec ni opravil svoje vloge z uvedbo ustrezne regulative.

Sodobne informacijske tehnologije podpirajo delovne procese in omogočajo elektronsko zajemanje in arhiviranje vseh vrst podatkov. Istočasno pa pred ustanove sodoben način dela prinaša izzive, povezane z varovanjem zbranih podatkov skladno z zakonodajo.

3.1.14. Lokalna računalniška omrežja

Ustanove sem povprašal, kakšno hitrost omogoča njihovo lokalno računalniško omrežje. Prejel sem 255 odgovorov, ki jih prikazuje Graf 14: Hitrosti lokalnih računalniških omrežij (LAN) izvajalcev zdravstvenih storitev. Za 51 ustanov (20%) lahko rečemo, da ima zastarela računalniška omrežja s hitrostjo 10Mbit/s, ki niso primerna za zdravstvene ustanove. Te ustanove predstavljajo 2,9% vseh zaposlenih v zdravstvu, kar pomeni, da gre za manjše ustanove. Kazalec je manjši od postavljenega kriterija 5% in zato potrjuje hipotezo.

Graf 14: Hitrosti lokalnih računalniških omrežij



Vir: Lasten

Sodobne komercialne različice protokolov (različice Etherneta) imajo tipično kapaciteto prenosnega kanala 100Mbit/s in 1Gbit/s. Prepustnost omrežja ni odvisna samo od ožičenja in protokola, temveč tudi od ponujanega prometa, ki ga ob uporabi ustvarjajo računalniki, priključeni v omrežje. Zato omrežja z naraščanjem števila aplikacij in uporabnikov postanejo ozko grlo.

Iz odgovorov ustanov sledi, da je v povprečju 95% računalnikov priključenih v lokalno računalniško omrežje (LAN). V povprečju ima v anketiranih ustanovah dostop do interneta 81% računalnikov.

Če ima nek računalnik povezavo z internetom, to pomeni troje:

- uporablja protokolarni sklad TCP/IP,
- ima svojo IP številko,
- lahko pošilja pakete vsem računalnikom, ki so povezani z internetom.

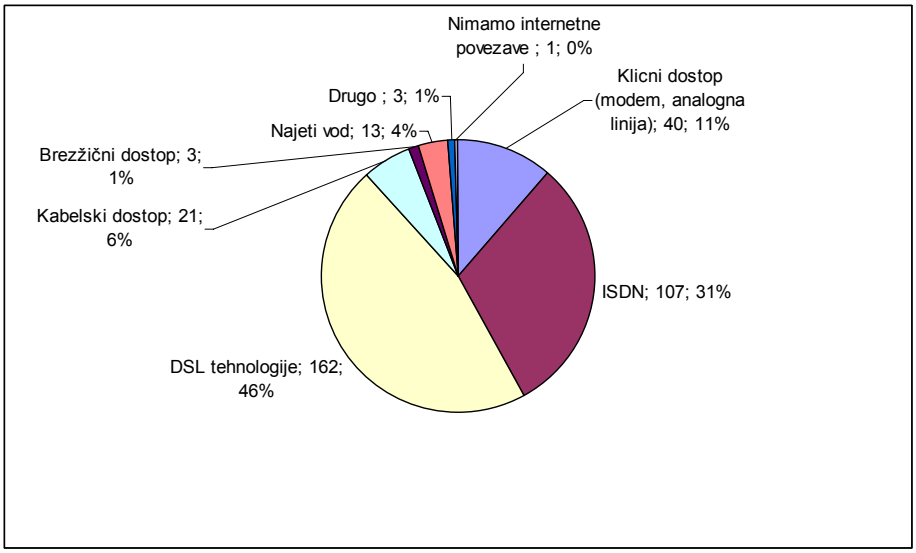
V začetku je za uporabnika povezava z internetom pomenila štiri klasične omrežne aplikacije ali storitve: elektronsko pošto, oddaljeno prijavljanje, novice in prenos datotek. Od začetka devetdesetih pa še www ali svetovni splet, ki predstavlja nepregledno množico koristnih, zanimivih in tudi popolnoma neuporabnih podatkov.

3.1.15. Komunikacije med zdravstvenimi ustanovami

Dostop do interneta postaja vse bolj ključnega pomena tudi za zdravstvene ustanove. Integrirana zdravstvena informacijska omrežja naj bi povezovala bolnice, laboratorije, lekarne, splošne zdravnike in socialne centre. Medsebojno naj bi komunicirala preko varnih povezav. Primer vključuje standardizirane sporočilne sisteme, kot na primer eRecept in eNapotnica, ter storitve telemedicine kot konzultacije za pridobitev drugega mnenja ali teleoskrbe. Širokopasovna dovolj zmogljiva povezava je pomembna zaradi naraščajočega števila uporabnikov v bolnišnicah in potreb sodobnih aplikacij po zmogljivih prenosnih poteh.

Kot vidimo iz Graf 15: Vrste dostopov do interneta glede na uporabljeno tehnologijo, ima 46% ustanov hitrost sprejema podatkov 1Mbps, najbolj razširjene pa so DSL tehnologije. Te rezultate sem dobil na podlagi odgovorov 351 ustanov.

Graf 15: Vrste dostopov do interneta glede na uporabljeno tehnologijo

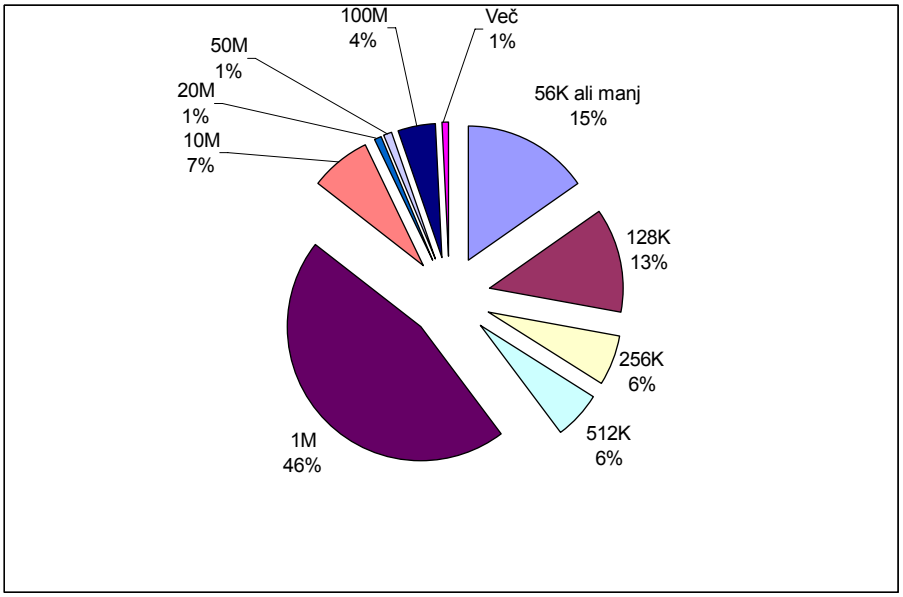


Vir: Lasten

Neustrezen modemski dostop ima 11% ustanov, ki predstavljajo 0,25% delež ustanov po zaposlenih.

Z vprašanjema o hitrosti obstoječe internetne povezave za sprejem podatkov Graf 16: Hitrosti sprejema podatkov (download) in pošiljanje podatkov Graf 17: Hitrosti pošiljanja podatkov (upload) sem poskušal ugotoviti strukturo hitrosti prenosa podatkov v ustanovah zdravstvenega sektorja.

Graf 16: Hitrosti sprejema podatkov (download)



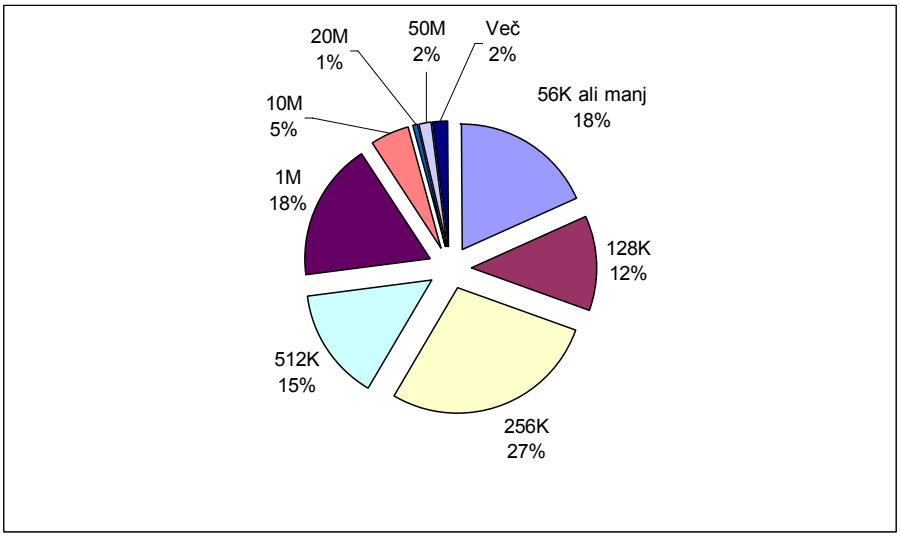
Vir: Lasten

Povprečna hitrost sprejema podatkov za bolnišnice je 98Kbps na delovno postajo. Takšna hitrost ustreza zahtevam projekta KZZ Online (ZZZS, 2007), ki priporoča 64Kbps in potrjuje postavljeno hipotezo. Žal pa za celoten sektor to ne velja, saj je v ustanovah, ki po zaposlenih predstavljajo 56% sektorja hitrost sprejema podatkov manjša od 64Kbps. Kazalec zato ne pritrjuje hipotezi.

Trenutno mogoče problem ni tako občuten, saj še ni v uporabi komunikacijsko zahtevnih aplikacij (teleradiologija, telekonference ipd). S povečevanjem števila pa bo problem postal bolj pereč. V ustanovah, kjer je pomanjkanje denarja kroničen problem, je razumljivo, da se odločajo za manj zmogljive povezave, saj je strošek komunikacij vsakomesečen.

Trend sodobnega poslovanja vodi k večji izmenjavi podatkov z uporabo različnih aplikacij. Tudi v Sloveniji lahko pričakujemo, da bodo potrebe po hitrosti in kapaciteti informacijsko komunikacijskih povezav zdravstvenih ustanov naraščale. Posamezne ustanove uporabljajo tehnološko zahtevne aplikacije, zaradi česar bo ob morebitnem dimenzioniranju nacionalnega zdravstvenega omrežja potrebno upoštevati takratne specifične potrebe teh ustanov. Zmogljivosti omrežja se bodo morale prilagajati aplikacijam, ki jih bodo ustanove vpeljevale v svoje procese.

Graf 17: Hitrosti pošiljanja podatkov (upload)



Vir: Lasten

Izmed 345 ustanov, ki so odgovorila, na koliko lokacijah delujejo, jih 110 deluje na več kot eni lokaciji, skupaj na 529 lokacijah. Na največ lokacijah deluje ustanova iz Ljubljane, na 50 lokacijah. Na eni lokaciji deluje 235 ustanov, 60 ustanov deluje na dveh lokacijah (modus), ostale pa na več lokacijah. Na kakšne načine so ustanove povezane s svojimi dislociranimi enotami, prikazuje Tabela 13: Načini povezav ustanov z več lokacijami.

Tabela 13: Načini povezav ustanov z več lokacijami

Načini povezav	**Delež**
Najeti vodi	9%
Brezžična povezava	5%
Preko internetnih povezav	36%
Niso povezane - povezave ne potrebujejo.	29%
Niso povezane - povezava bi bila potrebna.	18%
Drugo	4%

Vir: Lasten

Petindvajset ustanov (18%) z več lokacijami svojih lokacij medsebojno še nima povezanih, menijo pa, da bi bila povezava potrebna. Štirideset ustanov (29%) z več lokacijami pa svojih lokacij nima povezanih in tudi menijo, da povezava ni potrebna. Nekatere ustanove pa imajo povezanih samo del lokacij. To ne pomeni, da dislocirane enote nimajo dostopa do interneta, temveč, da oddelki znotraj nekaterih ustanov niso povezani. To na

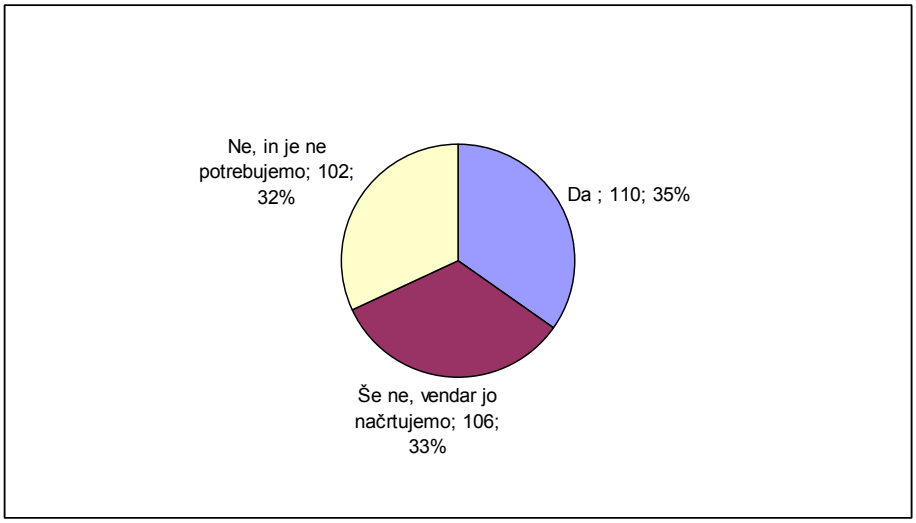
pripravljenost zdravstvenega sektorja na elektronsko poslovanje ne vpliva, kaže pa na možnosti izboljšav delovnih procesov takšnih ustanov.

3.1.16. Komunikacije zdravstvenih ustanov z državljani

Pomen eZdravja je v tem, da se postavi državljana v središče z namenom, da se izboljša interakcija širokega dela udeležencev, ki skrbijo za njegove potrebe (eHealth ERA report, 2007).

Od 318 ustanov, ki so odgovorile na vprašanje, jih 65% nima svoje spletne strani, od teh jih približno polovica tudi meni, da je ne potrebuje. Ustanove, ki menijo, da spletne strani ne potrebujejo, so manjše in skupaj predstavljajo slab odstotek vseh zaposlenih v zdravstvenem sektorju. Menim, da si ravno te ustanove s takšnim razmišljanjem škodujejo, saj na internetu ni velikih ali majhnih; so samo prisotni in tisti, ki jih ni. Rezultate prikazuje Graf 18: Ali imate svojo spletno stran?

Graf 18: Ali imate svojo spletno stran?



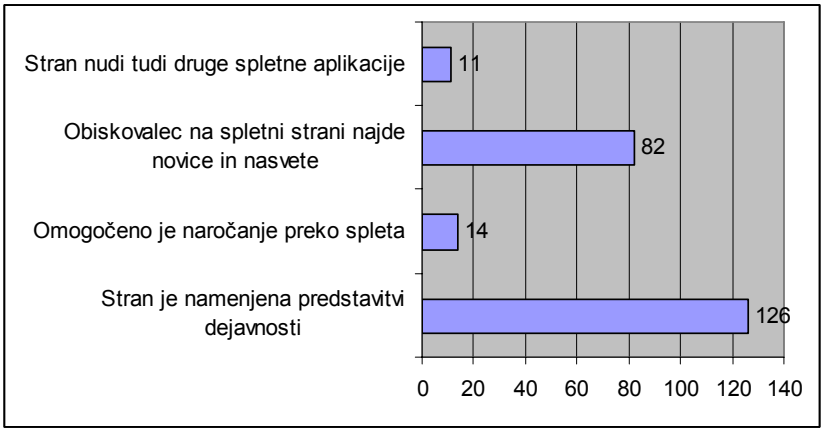
Vir: Lasten

Skandinavske dežele so že leta 2002 (Taylor & Leitman, 2002) imele na področju primarnega zdravstva večji delež ustanov s spletno stranjo. Za primerjavo: Finska (63%), Nizozemska (47%) in Švedska (42%).

Svoje spletne strani ima 106 ustanov, ki omogočajo različne funkcionalnosti, kot prikazuje Graf 19: Funkcionalnosti, ki jih spletne strani ustanov omogočajo. Na spletnih straneh nekaterih ustanov obiskovalci lahko najdejo tudi:

- informacije o vrsti in ceni storitev,
- opravijo informativni test: ali sem primeren kandidat za refraktivno očesno operacijo?
- kontakt glede vprašanj oz. informacij,
- pogosta vprašanja in odgovore,
- prijavnice za izobraževanja,
- razne povezave (Ministrstvo, itd....),
- spletno trgovino,
- mnenja, forumi, ankete, ...,
- intranet (informacije za zaposlene),
- ordinacijske čase,
- katalog informacij javnega značaja.

Graf 19: Funkcionalnosti, ki jih spletne strani ustanov omogočajo



Vir: Lasten

Uvedba enotne vstopne zdravstveno-informacijske točke je nujna za lažji dostop državljanov do vseh informacij, potrebnih za uveljavljanje zdravstvenega varstva. S poenostavljanjem dostopa in izmenjave podatkov se poveča število rednih uporabnikov

informacij. Upravljavcem in izvajalcem v sistemu zdravstvenega varstva s tem omogočimo lažjo izmenjavo znanja in prakse ter standardizacijo ravni storitev, državljanom pa priložnost posamezne storitve in informacije dobiti po spletu. Vse to vodi v razbremenitev sistema.

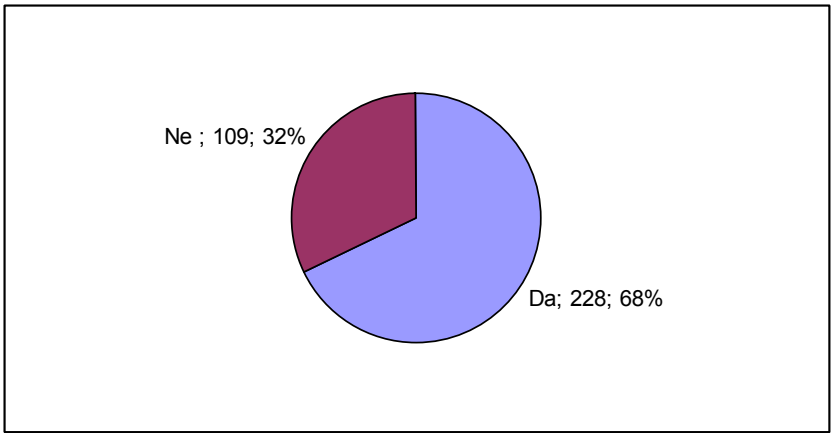
Raziskava RIS (Vehovar & Jovan & Dolničar, 2001) je pokazala, da skoraj 60% celotne slovenske aktivne populacije izraža zanimanje, da bi z elektronsko komunikacijo preko računalnika ali kakega drugega elektronskega medija dobili zdravniški nasvet ali interpretacijo zdravniških izvidov. Ugotovili so, da večjo uporabo internetnih strani povezanih z zdravstvom zavirajo:

- pomanjkanje kvalitetnih spletnih vsebin,
- premalo prijazno organizirane informacije,
- zaskrbljenosti za varnost osebnih podatkov,
- splošno nezaupanje virom na internetu.

Približno tretjina respondentov je bila pripravljena plačevati za dostop do zdravstvenih/farmacevtskih informacij na internetu. Obstaja splošen in velik interes za internetne informacije o lastnostih zdravil, posebno o pravilni uporabi, nezaželenih učinkih, dostopnosti v lekarnah ter interakcijah zdravil.

Na vprašanje: Ali vaša oprema omogoča oddaljen dostop, je odgovorilo 337 ustanov. Strukturo odgovorov prikazuje Graf 20: Ali vaša oprema omogoča oddaljen dostop? 68% ustanov ima opremo, ki omogoča oddaljen dostop. Ustanove, ki nimajo ustrezne opreme predstavljajo 16,25% zaposlenih v zdravstvenem sektorju. Kazalec ne potrjuje hipoteze.

Graf 20: Ali vaša oprema omogoča oddaljen dostop?



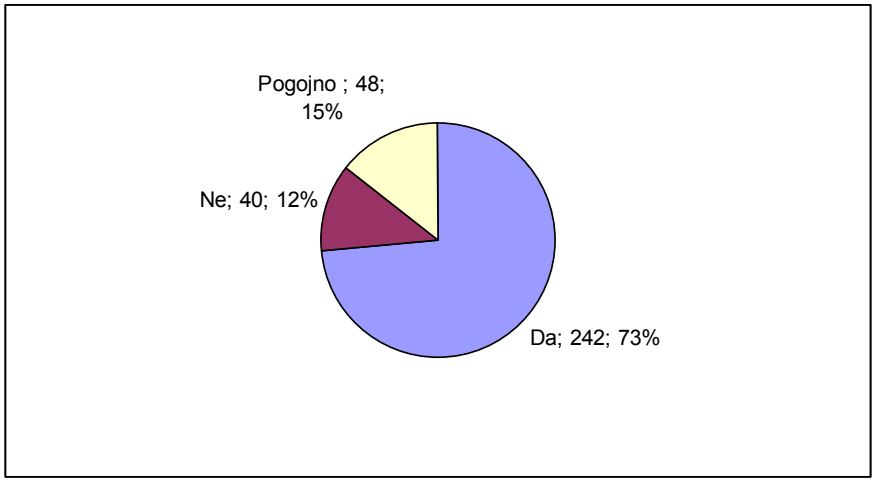
Vir: lasten

3.1.17. Interes za vključitev v nacionalno zdravstveno omrežje

V Evropi ima kar nekaj držav zdravstvene ustanove povezane v nacionalna zdravstvena omrežja. Nekaj primerov, Švedska Sjunet (Larson & Malmqvist, 2003), Anglija NHSnet (Benson, 2002), Dansko zdravstveno podatkovno omrežje (Popovič U., 2007) in drugi kot primer baltskih držav (Baltic Health Network). Razlogi in tehnične rešitve so delno različne in delno podobne. Varnost podatkov je skupna skrb, ki so jo v preteklosti reševali z zasebnimi omrežji najetih povezav, v zadnjem času pa s pomočjo VPN povezav in drugih varnostnih mehanizmov. Naslednji razlogi pa izhajajo iz želje po dostopnosti in izmenjavi podatkov med ustanovami, ki je pogojena s standardizirano komunikacijo vseh povezanih ustanov, enotnem upravljanju in skupnih varnostnih politikah. Vsekakor pa je potrebno upoštevati tudi stroškovni učinek. Sedaj vsaka ustanova na trgu telekomunikacij nastopa kot posamezen kupec. Razumljivo ima zato majhno pogajalsko moč. V kolikor pa bi zdravstveni sektor na trgu pri nakupih komunikacijskih povezav nastopil enotno, pa to predstavlja kupca s skoraj 50.000 zaposlenimi in cca. 1600 lokacijami, kar pa pomeni čisto druge cene in pogoje, tudi glede kvalitete storitev.

Graf 21: Interes za vključitev v nacionalno zdravstveno informacijsko omrežje prikazuje strukturo odgovorov 330 ustanov, kolikor se jih je izrazilo glede interesa za vključitev v nacionalno zdravstveno informacijsko omrežje. Interes za vključitev v omrežje je med ustanovami zelo velik.

Graf 21: Interes za vključitev v nacionalno zdravstveno informacijsko omrežje



Vir: Lasten

Oseminštirideset ustanov (15%) je pogojno za vključitev v omrežje. Na njihove odločitve bodo vplivali naslednji dejavniki:

- če bi to pomenilo cenejše in bolj učinkovito poslovanje, med seboj združljive in lahko uporabne programe za dnevno delo s pacienti, ki bi omogočili tudi

izmenjavo izvidov, napotnic in odpustnic ter končno vpogled v lastne statistične podatke, ki jih pošiljamo na IVZ,

- v primeru kompatibilnosti programske in strojne opreme,
- če bi vedel več o tem info. omrežju – potrebujemo več informacij,
- odvisno od pogojev in koristi, odvisno kaj bo omogočalo in koliko bo stalo,
- če bi imeli dostop do baze podatkov o zdravilih,
- če poenostavi poslovanje,
- če bodo vključene tudi lekarne,
- odvisno od stroškov vključitve (vzdrževanja) in pridobljenih koristi vključitve,
- v kolikor bo to potrebno zaradi izvajanja dejavnosti,
- čim prej - za vse lokacije - ustrezne pasovne širine, ki omogočajo centralizirano poslovanje,
- če ne bi bila vključitev prevelik strošek (nakup nove opreme, ...).

Navedeni pomisleki so zelo koristni vhodni podatki pri oblikovanju primernega poslovnega modela. Sklepamo lahko, da bo za ustanove odločilno razmerje stroški/koristi, ter ustrezna informiranost (promocija) koristi nacionalnega zdravstvenega informacijsko komunikacijskega omrežja. Omrežje mora ponuditi nekaj več in ne bistveno dražje, kot omogočajo obstoječe povezave ustanov. Potrebno je pravočasno začeti z informiranjem ustanov, ter promocijo za ozaveščanje o vlogi in možnostih, ki jih omrežje z nacionalnimi aplikacijami nudi na področju eZdravja.

3.1.18. Mnenja, pripombe in predlogi anketirancev

Nekateri anketiranci so v anketi podali tudi svoja mnenja, pripombe in predloge. Njihova mnenja prikazuje nekaj izbranih misli (brez prilagoditev):

- kdaj se bodo zadeve premaknile iz nulte točke,
- velika želja po uporabi nacionalnih aplikacij in izobraževanju na temo izrabe informacijske tehnologije,

- Ministrstvo za zdravje bi moralo začeti z izobraževanjem menedžmenta glede prednosti, izzivov, slabosti in nevarnosti informacijskih sistemov. Prikazati jim morajo, kako lahko z učinkovitim informacijskim sistemom spremljajo poslovanje zavoda tako s finančnega kot iz strokovnega vidika. Pomembno je tudi predstaviti ustrezno varnostno politiko,

- izmenjava podatkov naj bo pripravljena na takšen način, da za izvajalce ne bo predstavljala dodatnega administrativnega dela, ampak to le olajšala - kar ni lahko, je pa nujno za uspeh dobrega sodelovanja in postavitve mreže,

- najprej je potrebno poenotiti sistem za nabavo licenc pri Microsoftu,

- centralizacija in standardizacija infrastrukture, opreme, aplikacij ter varnostne politike na nacionalnem nivoju,

- želje po uvedbi regijskih centrov, ki za svoje delovanje potrebujejo informacijsko podporo.

SKLEP

V Sloveniji obstajajo številni zdravstveno informacijski sistemi, ki so bili razviti znotraj ali za potrebe javnih zdravstvenih institucij in so namenjeni predvsem zadovoljevanju njihovih lastnih potreb, ter medsebojno niso povezani in težko povezljivi. Vzrokov je več, med drugim tudi neobstoječe zdravstveno komunikacijsko omrežje, ki bi zagotavljalo varen in standardiziran okvir komunikacij in storitev in s tem povečano učinkovitost, ter večjo pogajalsko moč nasproti ponudnikom. Razpršenost virov informacijsko komunikacijskega sistema je naravna posledica razvoja in je danes jedro problemov, ki jih je potrebno rešiti. Podatki, zbrani s to anketo, so pokazali na velik interes ustanov v zdravstvenem sektorju tako za nacionalno zdravstveno informacijsko komunikacijsko omrežje, kot tudi za aplikacije razvite na nacionalnem nivoju. Pogoj za izmenjavo je dogovorjena, standardizirana oblika. Za namen ureditve področja zdravstveno informacijskih standardov je Ministrstvo za zdravje ustanovilo Odbor za zdravstveno informacijske standarde. Ker je trend integracije storitev v tako imenovane večpredstavne storitve ter razvoj omrežij v t.i. integrirana omrežja, ki so primerna za prenos podatkov za kakršnokoli storitev, pričakujem, da bodo tudi nacionalni projekti v zdravstvu imeli to smer.

Ustreznost tehnološke in pravne infrastrukture je relativna glede na zahteve procesov in z njimi povezanih aplikacij in jo lahko podajamo samo za dani trenutek. Za pripravljenost na prehod na višjo raven elektronskega poslovanja v zdravstvu je ključno stanje tistih subjektov, ki od povprečja najbolj odstopajo in na ta način zavirajo prehod sektorja na višjo raven.

Bolj kot potreba po sodobnejši opremi se v rezultatih ankete kaže potreba po sodobnih aplikacijah. Ustanove se namreč zavedajo in težijo k temu, da mora informacijska tehnologija njim in njihovim strankam-pacientom olajšati delo in življenje. Sorazmerno nizki odstotki uporabe računalnikov pri delu nekaterih profilov so verjetno posledica premajhnega vedenja o možnostih, ki jih informacijska tehnologija lahko nudi in ne premajhne količine. Izobraževanje, tudi že v šolskem sistemu in promocija novih aplikacij sta načina sprememb. Na pomanjkanje smernic, standardov in priporočil na področju informacijskih tehnologij in varnosti so manjše ustanove, ki so v Sloveniji v večini, še bolj občutljive kot večje. Ob uvedbi novih projektov je pomembno, da se ustanovam predstavi koristi, ki morajo presegati njihove stroške.

Pomembnost varnosti in zasebnosti narašča z razvojem informacijske infrastrukture in elektronskih storitev. Informacijski sistemi so in bodo vse bolj povezani z internetom in kot takšni izpostavljeni različnim grožnjam vdorov, zlorab podatkov in njihovega uničenja. Ker se v zdravstvu razpolaga z množico osebnih, zdravstvenih in drugih zaupnih podatkov v obliki pisnega, elektronskega in slikovnega gradiva, je to gotovo področje, ki mu bo na nacionalnem nivoju potrebno posvetiti posebno pozornost. Največ lahko storimo s tem, da zahtevamo, da so elementi varnosti in zasebnosti integrirani v razvoj novih storitev, ter da izobražujemo končne uporabnike rešitev.

Iz stališča tehnološke opremljenosti izvajalcev se je postavljena hipoteza magistrske naloge, da je zdravstveni sektor v Sloveniji pripravljen na elektronsko poslovanje, potrdila le delno. Ob upoštevanju kriterija, da kazalec ne podpira hipoteze, če je delež neustreznih ustanov po številu zaposlenih v sektorju večji od 5%, so ugotovitve po posameznih kazalcih naslednje:

Računalniki. V zdravstvenem sektorju v povprečju dela 1,44 ljudi z enim računalnikom, ki si ga delijo. Računalnikov je dovolj, saj gre v večini primerov vsaj za dvoizmensko delo (primer zdravstvenih domov) ali celo neprekinjen proces v primeru bolnišnic. Če bi vse zdravstvene ustanove delovale neprekinjeno, bi teoretično bilo ustrezno razmerje tudi, če bi prišel en računalnik na tri ljudi. Potrebna je zamenjava skoraj polovice delovnih postaj, ki so premalo zmogljive, imajo zastarel operacijski sistem in/ali stroški vzdrževanja presegajo njihovo vrednost. V okviru projekta prenove kartice zdravstvenega zavarovanja se je v ta namen že investiralo. **Kazalec potrjuje hipotezo.**

Komunikacije. Prehod v elektronsko poslovanje poteka kot evolucijski proces, preko več stopenj. Opazoval sem:

- lokalna omrežja: v povprečju je 95% računalnikov priključenih v lokalna računalniška omrežja. Za 51 ustanov (20%) lahko rečemo, da ima zastarela računalniška omrežja s hitrostjo 10Mbit/s, ki niso primerna za zdravstvene ustanove. Te ustanove predstavljajo 2,9% vseh zaposlenih v zdravstvu, kar pomeni, da gre za manjše ustanove. **Kazalec** je manjši od postavljenega kriterija 5% in zato **potrjuje hipotezo**.

- dostop do interneta: v povprečju ima v anketiranih ustanovah dostop do interneta 81% računalnikov. Modemska povezava, ki jo ima še vedno 11% ustanov, ni dovolj. Potrebna je primerno zmogljiva povezava. Povprečna hitrost sprejema podatkov za bolnišnice je 98Kbps na delovno postajo. Takšna hitrost ustreza zahtevam projekta KZZ Online, ki priporoča 64Kbps in potrjuje postavljeno hipotezo. Žal pa za celoten sektor to ne velja, saj je v ustanovah, ki po zaposlenih predstavljajo 56% sektorja, hitrost sprejema podatkov manjša pod 64Kbps. **Kazalec zato ne pritrjuje hipotezi**.

- Štirideset ustanov (29%) z več lokacijami svojih lokacij nima povezanih, in tudi menijo, da povezava ni potrebna. To ne pomeni, da dislocirane enote nimajo dostopa do interneta, temveč, da oddelki znotraj nekaterih ustanov niso povezani. To na pripravljenost zdravstvenega sektorja na elektronsko poslovanje ne vpliva, kaže pa na možnosti izboljšav delovnih procesov takšnih ustanov. Dvomim, da imajo te ustanove tako različne procese, da povezave ne bi potrebovale. Bolj verjetno je, da se ne zavedajo priložnosti, ki bi jih takšne povezave ob ustrezni integraciji lahko prinesle.

- Ustanove, ki menijo, da spletne strani ne potrebujejo, so manjše in skupaj predstavljajo slab odstotek vseh zaposlenih v zdravstvenem sektorju. Menim, da si ravno te ustanove s takšnim razmišljanjem škodujejo, saj na internetu ni velikih ali majhnih; so samo prisotni in tisti, ki jih ni. **Kazalec potrjuje hipotezo**.

- 68% ustanov ima opremo, ki omogoča oddaljen dostop. Ustanove, ki nimajo ustrezne opreme predstavljajo 16,25% zaposlenih v zdravstvenem sektorju. **Kazalec ne potrjuje hipoteze.**

Varnost. področje informacijske varnosti v vse bolj povezanem sistemu postaja čedalje pomembnejše.

- Zaskrbljujoče je dejstvo, da 42 (11%) ustanov sploh ne izvaja nobenega posebnega varovanja svoje ključne informacijske opreme. Ker te ustanove

predstavljajo samo 0,34% zaposlenih zdravstvenega sektorja, **kazalec potrjuje hipotezo.**

- Informacija, ki kliče po osveščanju ustanov, je, da 39 ustanov (11%) ne izvaja nikakršne zaščite pred vdori. Te ustanove predstavljajo 0,36% zaposlenih v sektorju. **Kazalec potrjuje hipotezo.**

- Kljub temu, da 3 ustanove, ki predstavljajo 0,33% zaposlenih v zdravstvenem sektorju, ne izvajajo nobenega varovanja dostopa do podatkov, **kazalec potrjuje hipotezo.**

- V 8 ustanovah pa varnostnega kopiranja sploh ne izvajajo. Te ustanove na srečo predstavljajo samo 0,31% vseh zaposlenih v zdravstvenem sektorju. **Kazalec potrjuje hipotezo.**

- Kar 135 ustanov (39%) informacijskih sistemov ni pripravljenih za delo v primeru izpada napajanja. Gre za majhne ustanove, ki skupno predstavljajo 1% zdravstvenega sektorja po zaposlenih. **Kazalec potrjuje hipotezo.**

- Kar 67 (19%) ustanov svojih arhivskih podatkov nikoli ne preveri. Te ustanove predstavljajo 3,99% zaposlenih v zdravstvu, kar pa je manj od postavljene meje 5%, zato **kazalec potrjuje hipotezo**.

- Ustanove, ki nimajo sprejete varnostne politike (233), niti je ne pripravljajo, predstavljajo 50,13% celotnega zdravstvenega sektorja. **Kazalec ne potrjuje hipoteze.**

- Kar 135 ustanov (39%) informacijskih sistemov ni pripravljenih za delo v primeru izpada napajanja. Gre za majhne ustanove, ki skupno predstavljajo 1% zdravstvenega sektorja po zaposlenih. **Kazalec potrjuje hipotezo**.

Procesi in aplikacije. Prenova in informatizacija procesov v javnih ustanovah poteka počasneje kot pri zasebnikih, na kar nakazujejo tudi deleži uporabnikov po posameznih profilih in vrstah ustanov. Vzrok lahko iščemo v velikosti ustanov. Javne ustanove so v povprečju večje kot zasebne. Pri uporabi aplikacij se kaže pomembna vloga ZZZS, saj je področje plačil pri vseh ustanovah izvedeno elektronsko. Da bi dosegli podoben napredek pri drugih aplikacijah, je potrebno, da vzpostavljene nacionalne entitete začnejo s svojim delom.

Ustanove v zdravstvu so na različnih stopnjah elektronskega poslovanja. Od stopnje, ko nimajo še niti spletne strani, do uvajanja stopnje, ko so že sposobni izpeljati elektronsko transakcijo. Za nobeno od ustanov pa ne moremo reči, da že v celoti posluje na stopnji integracije ali popolnoma elektronsko. Razloge lahko iščemo tudi v tem, da tudi, če bi ustanova sama izpolnjevala pogoje za popolnoma elektronsko poslovanje, nima partnerjev,

ki bi bili primerljivo razviti, da bi z njimi lahko elektronsko poslovala. Za razliko od gospodarstva, kjer nekatera močna podjetja svojim partnerjem diktirajo pogoje, ki zagotavljajo razvoj oskrbovalne verige, tega v zdravstvu ne zasledimo. Takšno vlogo bi morala prevzeti Svet za informatiko v zdravstvu in Center za informatiko v zdravstvu, tudi z definiranjem standardov opremljenosti izvajalcev, ki posamezni ustanovi v dejavnosti omogočajo elektronsko poslovanje s subjekti v zdravstvenem sistemu, kot pogojem za pridobitev dovoljenja za delo poleg običajnih pogojev, kot so na primer izobrazba in prostor.

4 LITERATURA

1. Alvarez, R.C. (2002, 17. september). The promise of e-Health - a Canadian perspective. *eHealth International*. Najdeno 20. decembra 2008 na spletnem naslovu http://www.pubmedcentral.nih.gov/articlerender.fcgi?tool=pubmed&pubmedid=12459044

2. APEK Agencija za pošto in elektronske komunikacije Republike Slovenije (2006, 1. september). Smernice za zagotavljanje varnosti omrežij elektronskih komunikacij in informacijskih sistemov. Najdeno 1. decembra 2008 na spletnem naslovu http://www.apek.si/sl/datoteke/File/predmetna_zakonodaja/smernice_za_zagotavljanje_varnosti.pdf

3. Amarasingham, R., Diener-West M., Plantinga, L., Cunningham, C. A., Gaskin J. D., Neil R Powe R. N. (2008, 15.september). Hospital characteristics associated with highly automated and usable clinical information systems in Texas, United States. *BMC Medical Informatics and Decision Making* 2008, 8 (39). Najdeno 29. januarja 2009 na spletnem naslovu http://www.biomedcentral.com/1472-6947/8/39

4. Bates, D.W. (2002). The quality case for information technology in healthcare. *BMC Medical Informatics and Decision Making*, 2:7. Najdeno 13. novembra 2008 na spletnem naslovu http://www.pubmedcentral.nih.gov/articlerender.fcgi?tool=pubmed&pubmedid=12396233

5. Belochi, L. (2003). *Telemedicine Glossary*. (5th ed.) Brusseles: European Commission.

6. Benson T. (2002, 9 november). Why general practitioners use computers and hospital doctors do not - Part 1: incentives. *BMJ - British Medical Journal*. 325:1086-1089. Najdeno 20. januarja 2009 na spletnem naslovu http://www.bmj.com/cgi/content/full/325/7372/1086?maxtoshow=&HITS=10&hits=10&RESULTFORMAT=1&author1=benson%252C+t&title=why+general+practitioners+&andorexacttitle=and&andorexacttitleabs=and&andorexactfulltext=and&searchid=1115217420109_12423&stored_search=&FIRSTINDEX=0&sortspec=relevance&resourcetype=1,2,3,4

7. Bešter, J. Kos, A. (2001, 9. marec). Slovenska informacijska infrastruktura. Najdeno 10. novembra 2008 na spletnem naslovu http://www.ltfe.org/wp-content/pdf/sii.pdf

8. Bešter, Kos, Homan, Pustišek (1998): Development of Slovenian Information Infrastructure. *Zbornik konference Mobility and Convergence of Communication Technologies*. Ljubljana.

9. Bratuša T. (2006). *Hekerski vdori in zaščita.* (druga izdaja). Ljubljana: Založba Pasadena.

10. Breskvar, M., Bricl, I., Stopar, P., Tasič. J., Meža, M., Rožman, P. (2006). Pilotna uvedba telekonzultacij v transfuzijsko službo. *Zbornik kongresa Slovenskega društva za*

medicinsko informatiko, Zdravje na informacijski poti (str. 198-207). Zreče: Slovensko društvo za medicinsko informatiko.

11. Car, J. & Sheikh, A. (2004, 21. avgust). Information in practice Email consultations in health care: 1—scope and effectiveness. *BMJ - British Medical Journal.* 329:435-438, Najdeno 27. decembra 2008 na spletnem naslovu http://www.bmj.com/cgi/content/full/329/7463/435

12. COBIT 4.1: Control Objectives, Management Guidelines, Maturity Models. The IT Governance Institute (ITGI). Najdeno 12. oktobra 2008 na spletnem naslovu http://www.isaca.org/cobit

13. Commission of the European Communities (2004, 20.april). Follow-up to the high level reflection process on patient mobility and health care developments in the European Union. COM (2004) 301 final, Brussels. Najdeno 10. decembra 2008 na spletnem naslovu http://www.ehtel.org/publications/publications-other-studies-and-reports/com2004-0301en01.pdf/view

14. Commission of the European Communities - COM (2004, 30. april) 356: Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions: e-Health - making health care better for European citizens:An action plan for a European e-Health Area, Brussels. Najdeno 1. decembra 2008 na spletnem naslovu http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2004:0356:FIN:EN:PDF

15. Coiera E. (2003). *Guide to Health Informatics.* London:Hodder. Najdeno 5.decembra 2008 na spletnem naslovu http://www.coiera.com/bk-intro.htm.

16. Dimovski, V., Penger S. & Škerlavaj, M. (2002). *Temelji organiziranja in odločanja*. Ljubljana: Ekonomska fakulteta.

7. Dixon, D. R. & Dixon, B. J. (1994). Adoption of information technology enabled innovations by primary care physicians: model and questionnaire development. *Proc Annu Symp Comput Appl Med Care*, 631-5. Najdeno 5.decembra 2008 na spletni strani http://www.pubmedcentral.nih.gov/picrender.fcgi?artid=2247957&blobtype=pdf

17. Englebardt, S. P. & Nelson, R. (2002). *Health Care Informatics - An Interdisciplinary Approach*. Mosby.

18. eHealth ERA report (2007, marec). *eHealth priorities and strategies in European countries*. Najdeno 21. decembra 2008 na spletnem naslovu http://www.ehealtheurope.net/img/document_library0282/ehealthPriorities_and_Strategies.pdf

19. European Commission, DG Enterprise & Industry (2008, junij). *ICT standards in the health sector: current situation and prospects*. Najdeno 3. januarja 2009 na spletnem

naslovu http://www.ebusiness-watch.org/studies/special_topics/2007/documents/Special-study_01-2008_ICT_health_standards.pdf

20. European Commission, Enterprise Directorate-General (2004, Maj). *Electronic Business in the Health and Social Services Sector*. Najdeno 26. januarja 2009 na spletnem naslovu http://www.ebusiness-watch.org/studies/sectors/health_generic/documents/Health_2004_I.pdf

21. European Commission, Enterprise & Industry Directorate (2007). *ICT and e-Business in Hospital Activities*. Najdeno 26. januarja 2009 na spletnem naslovu http://www.ebusiness-watch.org/studies/sectors/health_hospital/documents/Hospitals_2006.pdf

22. Eysenbach G. (2001). What is e-health? *Journal of Medical Internet Research,* 3(2):e20. Najdeno 20. decembra 2008 na spletnem naslovu http://www.jmir.org/2001/2/e20/

23. Gaspari, I., Anžur, A., Kravanja, M. (2006). Vključevanje zdravstva v elektronsko poslovanje državne uprave. *Zbornik kongresa Slovenskega društva za medicinsko informatiko, Zdravje na informacijski poti* (str. 28-35). Zreče: Slovensko društvo za medicinsko informatiko.

24. Gradišar, M. (2003). *Uvod v informatiko*. Ljubljana: Ekonomska fakulteta.

25. Gradišar, M., Jaklič J. & Turk T. (2007). *Osnove poslovne informatike*. Ljubljana: Ekonomska fakulteta.

26. Grasselli, P. (2006). Zakaj je pomembna zmogljivostno zrelostna ocena programa UNP. *Varnostni forum* maj, str. 20-22.

27. Iljaž, R., Kersnik, J. & Roženberger, M. (2005). Uporaba računalniške tehnologije med zdravniki v primarnem zdravstvu – pilotska študija. *Zdravstveno varstvo*, (44), str.206-214.

28. Ilijaž, R. (2005). Elektronski zdravstveni zapis in »online« zdravstvene storitve v osnovnem zdravstvu, *Informatica Medica Slovenica*, 10 (1), str 26-34.

29. Ilijaž, R. (2007). Elektronski posvet med zdravstvenim osebjem in uporabnikom zdravstvene storitve. *Informatica Medica Slovenica,* 12 (1), str 24-33.

30. Jaklič, J. (2002). *Upravljanje in uporaba podatkov*. Ekonomska fakulteta: Ljubljana.

31. Kaushal, R., Shojania, K.G. & Bates, D.W. (2003). Effects of computerized physician order entry and clinical decision support systems on medication safety: a systematic review. *Arch Intern Med*, 163 (12), 1409-16. Najdeno 20. decembra 2008 na spletnem naslovu http://www.ncbi.nlm.nih.gov/pubmed/12824090

32. Kadivec M., (2007). Sodobna slikovna diagnostika v onkologiji in čakalne dobe. *Zdravstveni vestnik,* 76, str. 795–798. Najdeno 14. decembra na spletnem naslovu http://vestnik.szd.si/st07-12/795-798.PDF

33. Kane, B. & Sandz, D., Z. (1998). Guidelines for the Clinical Use of Electronic Mail with Patients. *American Medical Informatics Association*. Jan–Feb, 5(1), 104–111. Najdeno 13. januarja 2009 na spletnem naslovu http://www.pubmedcentral.nih.gov/articlerender.fcgi?tool=pubmed&pubmedid=9452989

34. Kodele, D., Košir, F., Marušič, D. & Sušelj, M. (2005). *Strategija eZdravje2010.* Ljubljana: Ministrstvo za zdravje. Najdeno 11.septembra 2007 na spletnem naslovu http://www.mz.gov.si/fileadmin/mz.gov.si/pageuploads/mz_dokumenti/delovna_podrocja/zdravstveno_varstvo/kodele/eZdravje116slo.doc

35. Kokol, P. (2003). Poročilo o udeležbi na sestanku IMIA – NI Sig, 12.11.2002, San Antonia, ZDA. *Informatica Medica Slovenica*, 8(1), 88-89.

36. Kondža, B. (2008, 14. julij). Rak – Damoklejev meč sodobne družbe. *Delo*. Najdeno 15. decembra 2008 na spletnem naslovu http://delo.si/clanek/63706

37. Kotnik, M. (2006). Informacijska varnost je visoko na mojem seznamu ključnih nalog. *Varnostni forum*. jul/avg, str.19-22.

38. Kovacich, L. G. & Halibozek, P. E. (2003). *The Managers' handbook for corporate security – establising and managing a successful assets protection program*. USA: Butterworth – Heinemann imprint of Elsevier Science.

39. Kovačič, A., Groznik A. & Ribič M. (2005). *Temelji elektronskega poslovanja.* Ljubljana: Ekonomska fakulteta.

40. Kovačič, A., Jaklič, J., Štemberger I.,M. & Groznik, A. (2004). *Prenova in informatizacija poslovanja.* Ljubljana: Ekonomska fakulteta.

41. Kovačič, A., Bosilj Vukšič, V. (2005). *Management poslovnih procesov.* Ljubljana: GV Založba.

42. Laerum, H., Ellingsen, G. & Faxvaag, A. (2001, 8.december). Doctors´ use of electronical medical records systems in hospitals: cross sectional servey. *BMJ - British Medical Journal*, 323:1344-1348. Najdeno 4. Novembra 2008 na spletnem naslovu http://www.bmj.com/cgi/content/full/323/7325/1344

43. Larson, M. & Malmqvist, G. (2003). *Sjunet – The National IT Infrastructure for Healthcare in Sweden.* Najdeno 10. decembra 2008 na spletnem naslovu http://vefir.unak.is/ICTConference/Larson.pdf

44. Marušič, D. (2007). Uvodnik. *Bilten ekonomika, organizacija in informatika v zdravstvu,* str. 37. Ljubljana: Inštitut za varovanje zdravja Republike Slovenije.

45. Meglič, M., Marušič, D., Anžur, A. & Kodele, D. (2007a). Organizacijski vidik opremljenosti in uporabe informacijskih in komunikacijskih tehnologij v zdravstvu v Sloveniji. *Zdravstveno varstvo*, letnik 46, številka 3, str. 113-115. Ljubljana: Inštitut za varovanje zdravja Republike Slovenije.

46. Meglič, M., Marušič, D., Kodele, D. & Anžur, A. (2007b). E-Zdravje2010 – po enem letu. *Bilten ekonomika, organizacija in informatika v zdravstvu,* letnik 23, številka 2, str. 42-45. Ljubljana: Inštitut za varovanje zdravja Republike Slovenije.

47. Meglič, M., Marušič, D., Anžur, A. & Kodele, D. (2007c). Opremljenost in uporaba informacijskih tehnologij v bolnišnicah in zdravstvenih domovih v Sloveniji. *Informatica Medica Slovenica, 12 (2),* str. 34-39. Ljubljana: Slovensko društvo za medicinsko informatiko.

48. Oh H., Rizo C., Enkin M. & Jadad A. (2005). What Is eHealth?: A Systematic Review of Published Definitions. *Journal of Medical Internet Research,* 7(1):e1. Najdeno 20. decembra 2008 na spletnem naslovu http://www.jmir.org/2005/1/e1/

49. Planinc, N., Šorli, J., Kralj, U., Fuart, F., Slavec, S., (2004). Elektronski zapis podatkov o pacientu – pridobitve in dileme. *Zbornik kongresa E-zdravje v e-Sloveniji.* Ljubljana: Slovensko društvo za medicinsko informatiko.

50. Podgorelec, V. (1999). Razvoj informatike v medicini in zdravstvu. *Zdravstvena informatika,* 1-13. Urednik: Peter Kokol. Maribor: Visoka zdravstvena šola.

51. Popovič, U. Š., Jerčinović, A., Štefotič L. Š., Anžur, A. Gašperšič, J. & Jauk, A. (2007, 27.maj). *Konceptualni model nacionalnega zdravstveno informacijskega sistema (eZIS).* Ljubljana: Ministrstvo za zdravje. Najdeno 1. decembra na spletnem naslovu http://www.mz.gov.si/fileadmin/mz.gov.si/pageuploads/mz_dokumenti/informatika/Microsoft_Word_-_wwwArhitektura_eZIS_v21.pdf.

52. Potts, A. L., Barr, F. E., Gregory, D. F., Wright, L. & Patel, N. R. (2004). Computerized phisician order entry and medication errors in pediatric critical care unit. *Pediatrics,* 113 (1), str. 59-63.

53. Potokar, M. (2006). S trikotnika CEO/CIO/CSO na kvadrat CEO/CIO/SCO/LO. *Varnostni forum*, sep, str.21-22.

54. Praprotnik, M. (2006). Avtomatizacija IT – upravljanje uporabniških identitet. *Varnostni forum,* feb, str.24-27.

55. Rolih, G. (2006). Varnost brezžičnih omrežij. *Varnostni forum*, sep, str. 9-10.

56. Rudel, D. (2005). Upravljanje z varnostjo informacij v zdravstvenih organizacijah. *Informatica Medica Slovenica*, 10 (1), str.1-8.

57. Slovenski inštitut za standardizacijo: *Standardizacija, definicije.* Najdeno 10. decembra 2008 na spletnem http://www.sist.si/slo/g1/g112.htm.

58. Slovenski inštitut za standardizacijo SIST ISO/IEC 17799:2005, Information technology - Security techniques - Code of practice for information security management.

59. Slovenski inštitut za standardizacijo SIST ISO/IEC 27001:2006, Information technology – Security techniques – Information security management systems – Requirements.

60. Stead, W. W., Kelly, B. J. & Kolodner R. M. (2005). Achievable Steps Toward Building a National Health Information Infrastructure in the United States. *American Medical Informatics Association*, 12 (2), str. 113–120. Najdeno 25. decembra 2009 na spletnem naslovu http://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=551543

61. Stroetmann, K. A. (2003, Februar). ICT and Electronic Business in the Health and Social Services Sector in the EU. *Empirica Schriftenreihe Report 02/2003*. Najdeno 26. januarja 2009 na spletnem naslovu http://www.empirica.com/publikationen/documents/No02-2003_eBiz-Health.pdf

62. Šavnik J. (2006). Odprtokodni sistemi za zaznavanje vdorov. *Varnostni forum*, jul/avg, str. 28-30.

63. Šinigoj A. (2008). *Razvoj metode upravljanja tveganj povezanih z informacijskimi sredstvi v podjetjih.* Ljubljana: Doktorska disertacija.

64. Tamblyn, R., Huang, A., Perreault, R. Jacques, A., Roy, D., Hanley, J., McLeod, P. & Laprise, R. (2003). The medical office of the 21st century (MOXXI): effectivness of computerized decision-making support in reducing inappropriate prescribing in primary care. *CMAJ - Canadian Medical Association Journal*, 169 (6), str. 549-556. Najdeno 10. decembra na spletnem naslovu http://www.pubmedcentral.nih.gov/articlerender.fcgi?tool=pubmed&pubmedid=12975221

65. Taylor, H. & Leitman, R. (2002, 8.avgust). European physicians especially in Sweden, Netherlands and Denmark, lead U.S. in use of electronic medical records. *Harris Interactive Health Care News*, 2(16), str. 1-3. Najdeno 10. decembra 2008 na spletnem naslovu http://www.harrisinteractive.com/news/newsletters/healthnews/HI_HealthCareNews2002Vol2_Iss16.pdf

66. Toth, M., (2008, 30. september). Kako do večje učinkovitosti sistema zdravstvenega varstva. *Delo*, str. 5.

67. Van Bemmel, J.H. & Musen M.A. (1997). *Handbook of Medical Informatics*. AW Houten, Netherlands: Bohn Stafleu Van Loghum; Heidelberg, Germany: Springer Verlag.

68. Vehovar, V., Brečko, N. B. (2007, november). *RIS 2007 – Uporaba interneta*. Najdeno 10. decembra 2008 na spletnem naslovu http://www.ris.org/uploadi/editor/1229017546Uporaba%20interneta_2007.pdf

69. Vehovar, V., Jovan, M., Dolničar, V. (2001, 26.december). *Zdravstvo in farmacija 2001*. Najdeno 20. decembra 2008 na spletnem naslovu http://www.ris.org/index.php?fl=2&lact=1&bid=142&menu=0

70. Verduyn B. (2005). *FBI – Cyber Squadvir: 2005 FBI Computer Crime Survey*. Najdeno 3. januarja 2009 na spletnem naslovu http://www.digitalriver.com/v2.0-img/operations/naievigi/site/media/pdf/FBIccs2005.pdf

71. Vidmar, T. (2002). *Informacijsko komunikacijski sistem.* Ljubljana: Založba Pasadena.

72. Wilson, P. Leitner, C. & Moussalli, A. (2004, 5-6 Maj). Mapping the Potential of eHealth: Empowering the Citizen through eHealth Tools and services. *Presented at the eHealth Conference, Cork, Ireland*. Najdeno 3. decembra 2008 na spletnem naslovu http://aei.pitt.edu/6092/01/2004_E_01.pdf

5 VIRI

1. Ministrstvo za zdravje: *Letni načrt razvoja nacionalne zdravstvene informatike za obdobje julij 2008 do december 2009*. Najdeno 1. decembra 2008 na spletnem naslovu http://www.mz.gov.si/fileadmin/mz.gov.si/pageuploads/mz_dokumenti/informatika/Letni_nacrt_2008_09_v18_new.doc

2. Ministrstvo za zdravje: *Temeljna listina za ustanovitev Sveta za informatiko v zdravstvu*. Najdeno 1.decembra 2008 na spletnem naslovu http://www.mz.gov.si/fileadmin/mz.gov.si/pageuploads/Svet_za_informatiko_SIZ_in_OZIS/SIZ_Temeljna_listina.doc

3. Ministrstvo za zdravje: *Poslovnik Sveta za informatiko v zdravstvu*. Najdeno 1.decembra 2008 na spletnem naslovu http://www.mz.gov.si/fileadmin/mz.gov.si/pageuploads/Svet_za_informatiko_SIZ_in_OZIS/SIZ_Poslovnik.doc

4. Ministrstvo za zdravje: *Temeljna listina za ustanovitev Odbora za zdravstveno informacijske standarde.* Najdeno 1. decembra 2008 na spletnem naslovu http://www.mz.gov.si/fileadmin/mz.gov.si/pageuploads/Svet_za_informatiko_SIZ_in_OZIS/OZIS_dokumenti_2007/OZIS_Temeljna_listina_v0_51.pdf

5. Ministrstvo za zdravje: *Poslovnik delovanja Odbora za zdravstveno informacijske standarde.* Najdeno 1. decembra 2008 na spletnem naslovu http://www.mz.gov.si/fileadmin/mz.gov.si/pageuploads/Svet_za_informatiko_SIZ_in_OZIS/OZIS_dokumenti_2007/OZIS_Poslovnik_v0_5.pdf

6. Ministrstvo za visoko šolstvo, znanost in tehnologijo, (2007, 29.junij). *Strategija razvoja informacijske družbe v Republiki Sloveniji*. Najdeno 12. oktobra 2008 na spletnem naslovu http://193.2.236.95/dato3.nsf/OC/0707011323466/$file/128v1_7.doc#_Toc170280135

7. Moravec Berger, D., Pribakovič Brinovec, R., Trdič J. (2008). *Zdravstveni statistični letopis 2006*. Ljubljana: Inštitut za varovanje zdravja Republike Slovenije.

8. Resolucija o nacionalnem planu zdravstvenega varstva 2008-2013 »Zadovoljni uporabniki in izvajalci zdravstvenih storitev« (2008). *Uradni list RS*. (Št. 72/2008, 17.julij 2008).

9. Zakon o zbirkah podatkov s področja zdravstvenega varstva. (2000). *Uradni list RS*. (Št. 65/2000, 21.julij 2000).

10. Zakon o elektronskem poslovanju in elektronskem podpisu. *Uradni list RS*. (Št. 57/2000).

11. Zakon o varstvu osebnih podatkov. *Uradni list RS*. (Št. 59/1999).

12. Zakon o zdravstveni dejavnosti. *Uradni list RS*. (Št. 36/2004).

13. Zakon o elektronskih komunikacijah. *Uradni list RS.* (Št. 43/2004).

14. Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih (ZVDAGA). *Uradni list RS*. (Št. 30/2006).

15. Zavod za zdravstveno zavarovanje Slovenije (2007, 30.november). *Inštruktažna konferenca*, Uvajanje sodobnega ON-LINE elektronskega poslovanja v sistem zdravstvenega varstva in zdravstvenega zavarovanja, Grand hotel Union, Ljubljana

16. Zavod za zdravstveno zavarovanje Slovenije (2006, 19.oktober). *Občasnik akti & navodila*, letnik XIV, št.4.

17. Zavod za zdravstveno zavarovanje Slovenije (2007, 7.maj). *Občasnik akti & navodila*, letnik XV, št.2.

6 SLOVAR TUJK IN KRATIC

Automated Medical Record	avtomatizirani medicinski zapis	AMR
Benchmarking	primerjanje, primerjave	
Best-practices	dobre prakse, standardizacija	
Computerized Medical Record	računalniško podprt medicinski zapis	CMR
Compact Disk	zgoščenka	CD
Disc Operating System	operacijski sistem, zasnovan za delo z diskovnimi pomnilniki. Izraz se uporablja tudi kot alternativni naziv operacijskega sistema Microsoft DOS	DOS
Download	sprejem podatkov, dolpoteg	
Digital Subscriber Line	eden od načinov dostopa do interneta, npr. DSL, ADSL, HDSL, IDSL, MDSL, RADSL, SDSL, VDSL	DSL
Electronic Health Record	elektronski zdravstveni zapis	EHR
Electronic Data Interchange	računalniško izmenjevanje podatkov	EDI
Electronic Medical Record	elektronski medicinski zapis	EMR
Electronic Patient Record	elektronski zapis o pacientu	EPR
Health care informatics	informatika v zdravstvu	
Health Informatics	medicinska informatika	
HoneyPots	muholovci	
Host Intrusion Detection Systems	sistemi za odkrivanje vdorov v strežnik	HIDS
Host Intrusion Prevention Systems	sistemi za preprečevanje vdorov v strežnike	HIPS
Information security	informacijska varnost	
Integrated Services Digital	digitalno omrežje z integriranimi storitvami	ISDN

Network		
Internet protocol security	zbirka ukrepov za zagotavljanje varnostnih storitev v sloju IP. Storitve obsegajo avtentikacijo podatkovnega izvora, neokrnjenost in zaupnost podatkov.	IPsec
Interoperability	medobratovalnost, interoperabilnost	
Keylogger	opazovalci tipkovnice	
Kilo bits per second	1000 bitov na sekundo	Kbps
Medical informatics	medicinska informatika	
Mega bits per second	1.000.000 bitov na sekundo	Mbps
Network Intrusion Detection Systems	sistemi za odkrivanje vdorov v omrežje	NIDS
Nursing informatics	informatika v zdravstveni negi	
Patches	popravki	
Patient data file	podatki o pacientu	
Picture Archiving Communication System	sistem arhiviranja in izmenjave slikovnega materiala	PACS
Random Access Memory	pomnilnik z naključnim dostopom	RAM
Quality of Service	kakovost storitve	QoS
Secure Socket Layer	protokol, ki omogoča šifrirano povezavo med strežnikom in odjemalcem	SSL
Set-Top-Box	komunikator	
Sniffer	vohljač	
Spyware	vohunsko programje	
Transmission Control Protocol/Internet Protocol	standardiziran sklad protokolov, na katerem temelji internet	TCP/IP
Unshielded Twisted Pair	neoklopljena parica	UTP
Upload	pošiljanje podatkov	

7 PRILOGA: VPRAŠALNIK

V kolikor potrebujete pri izpolnjevanju ankete pomoč, prosim pokličite Anžur Aleš tel.: 031 777 926 ali pišite na alesanzur@data-bit.si

Vljudno vas prosimo, da vprašalnik izpolnite do 30.06.2006 do 15. ure.

	Splošni podatki	
1	**Naziv ustanove**	(Text)
	Naslov ustanove	(Text)
	Davčna številka	(številka)
	Matična številka	(številka)
2	**Vrsta ustanove**	
	Javni zavod	(Izbira)
	Zasebnik s koncesijo	(Izbira)
	Drugo	(Izbira)
3	**Tip ustanove**	
	Bolnišnica	(Izbira)
	Zdravstveni dom	(Izbira)
	Lekarna	(Izbira)
	Zdravilišče	(Izbira)
	Socialni in posebni zavodi	(Izbira)
	Specialistična dejavnost	(Izbira)
	Zobozdravstvena dejavnost	(Izbira)
	Fizioterapija	(Izbira)
	Nega in patronaža	(Izbira)
	Reševalni prevozi	(Izbira)
	Drugo	(Izbira)
4	**Kdo je izpolnjeval anketo (ime in priimek, položaj)**	(Text)
5	**Kontaktna oseba za področje informatike (ime in priimek, položaj, tel#, e_naslov)**	(Text)
6	**V kolikor je kontaktna oseba za področje informatike vaš zunanji partner izpolnite**	
	Naziv podjetja - vašega vzdrževalca	(Text)
	Naslov podjetja	(Text)
	Davčna številka	(številka)
	Matična številka	(številka)
7	**Skupno število zaposlenih v zdr. ustanovi?**	(število)
	zdravnikov	(število)
	sester	(število)
	administratork	(število)
	drugi (RTG, fizioterapevti,…)	(število)
	"nezdravstveno osebje" (npr. računovodstvo)	(število)

8	**Število osebja, ki pri delu uporablja računalnik?**	
	zdravnikov	(število)
	sester	(število)
	administratork	(število)
	drugi (RTG, fizioterapevti,…)	(število)
	"nezdravstveno osebje" (npr. računovodstvo)	(število)
	Splošni podatki o opremljenosti ustanove	
9	**Skupno število računalnikov v ustanovi?**	(število)
10	**Koliko imate delovnih postaj (računalnikov) s procesorjem tipa/ranga?**	
	Pentium	(število)
	Pentium II	(število)
	Pentium III	(število)
	Pentium IV	(število)
	Drugo - koliko	(število)
11	**Koliko imate inštaliranih operacijskih sistemov na delovnih postajah**	
	DOS	(število)
	WIN 95/98/ME	(število)
	WIN NT 3.51/4.0	(število)
	WIN 2000	(število)
	WIN XP home	(število)
	WIN XP pro	(število)
	Linux	(število)
	Drugo	(število)

12	**Strežniki (glede na namen)**	število	hitrost procesorja v MHz	diskovne kapacitete v GB	RAM v MB	operacijski sistem
	aplikacijski	(število)	(število)	(število)	(število)	(text)
	poštni	(število)	(število)	(število)	(število)	(text)
	spletni	(število)	(število)	(število)	(število)	(text)
	datotečni	(število)	(število)	(število)	(število)	(text)
	drugo	(število)	(število)	(število)	(število)	(text)

	Vprašanja o varnosti	
13	**Ali ima vaša ustanova sprejet dokument - varnostno politiko za področje informatike?**	
	DA	(Izbira)
	NE	(Izbira)
14	**Kako zagotavljate varnost pred zunanjimi vdori?**	
	požarni zid	(izbira)
	z požarnimi zidovi in na ključnih strežnikih	(izbira)
	vse našteto + na delovnih postajah	(izbira)
	vse našteto + sistemi za zaznavnaje vdorov	(izbira)
	nič	(izbira)
	drugo	(izbira)
15	**Kako zagotavljate varovanje pred virusi - antivirusni program (možnih je več odgovorov)?**	
	na delovnih postajah	(izbira)

	na strežnikih	(izbira)
	pri dostopu do interneta	(izbira)
	nič	(izbira)
	drugo	(izbira)
16	**Kako zagotavljate delovanje v primeru izpada napajanja (možnih je več odgovorov)?**	
	neprekinjeno napajanje (UPS)	(izbira)
	drugi vir (agregat)	(izbira)
	nič	(izbira)
	drugo	(izbira)
17	**Kako zagotavljate varnostno kopiranje in hranjenje podatkov (možnih je več odgovorov)?**	
	na dodatnem trdem disku	(izbira)
	na trakovih ali drugih medijih	(izbira)
	na oddaljeni lokaciji	(izbira)
	drugo	(izbira)
18	**Kako pogosto vršite varnostno kopirnje podatkov?**	
	dnevno	(izbira)
	tedensko	(izbira)
	mesečno	(izbira)
	letno	(izbira)
	nikoli	(izbira)
19	**Kako pogosto vršite kontrolo arhivov?**	
	četrtletno	(izbira)
	polletno	(izbira)
	letno	(izbira)
	nikoli	(izbira)
20	**Koliko časa potrebujete za vzpostavitev sistema pri hudem izpadu (v urah)?**	**(številka)**
21	**Kaj uporabljate za obveščanje o izpadu?**	
	telefon, osebno	(izbira)
	avtomatske telefonske klicatelje	(izbira)
	avtomatsko obvestilo preko elek. pošte	(izbira)
	drugo	(izbira)
	nič	(izbira)
22	**Kako zagotavljate varovanje dostopa do podatkov (možnih je več odogovorov)?**	
	gesla	(izbira)
	kartice	(izbira)
	biometrika	(izbira)
	nič	(izbira)
23	**Kako zagotavljate varovanje ključne IKT opreme (npr. strežnika) (možnih je več odogovorov)?**	
	zaklenjena komunikacijska omara	(izbira)
	fizični nadzor	(izbira)
	kartice	(izbira)
	video nadzor	(izbira)
	biometrična kontrola	(izbira)
	drugo (kaj)	(izbira)
	nič	(izbira)
	požarni senzorji	(izbira)
	senzorji dostopa	(izbira)
	klimatska naprava	(izbira)

	Komunikacija			
24	**Koliko računalnikov ima dostop do interneta?**	(številka)		
25	**Koliko rač. je priključenih v lokalno omrežje (LAN)?**	(številka)		
26	**Kolikšno hitrost dopušča vaše lokalno računalniško omrežje v Mb/s?**	(številka)		
27	**Kakšna tehnologija je uporabljena za dostop do interneta:**		Hitrost (pošiljanja) v Mb/s	Hitrost (sprejemanja) v Mb/s
	ISDN	(izbira)	(številka)	(številka)
	DSL tehnologije	(izbira)	(številka)	(številka)
	kabelski dostop	(izbira)	(številka)	(številka)
	brezžični dostop	(izbira)	(številka)	(številka)
	najeti vod	(izbira)	(številka)	(številka)
	drugo	(izbira)	(številka)	(številka)
28	**Na koliko lokacijah delujete?**	(številka)		
29	**Kako so lokacije med seboj povezane v kolikor jih imate več?**			
	najeti vodi	(izbira)		
	brezžična povezava	(izbira)		
	preko internetnih povezav	(izbira)		
	drugo	(izbira)		
	nič	(izbira)		
	Podatki, ki jih izmenjujete v elektronski obliki, preko informacijskih istemov	Jih izmenjujemo	Jih želimo oz. jih nameravamo izmenjevati v roku 2 let	
30	**naročila laboratorijskih testov**			
	znotraj ustanove	(izbira)	(izbira)	
	med ustanovo in ustanovo drugega nivoja (sekundarni, primarni)	(izbira)	(izbira)	
	med ustanovo in ustanovo istega nivoja	(izbira)	(izbira)	
	med ustanovo in …..	(izbira)	(izbira)	
31	**napotnice**			
	znotraj ustanove	(izbira)	(izbira)	
	med ustanovo in ustanovo drugega nivoja (sekundarni, primarni)	(izbira)	(izbira)	
	med ustanovo in ustanovo istega nivoja	(izbira)	(izbira)	
	med ustanovo in …..	(izbira)	(izbira)	
32	**fakturiranje**			
	znotraj ustanove	(izbira)	(izbira)	
	med ustanovo in ustanovo drugega nivoja (sekundarni, primarni)	(izbira)	(izbira)	
	med ustanovo in ustanovo istega nivoja	(izbira)	(izbira)	
	med ustanovo in ZZZS	(izbira)	(izbira)	
	med ustanovo in MZ	(izbira)	(izbira)	
	med ustanovo in IVZ RS	(izbira)	(izbira)	
	med ustanovo in …..	(izbira)	(izbira)	
33	**statistika**			
	znotraj ustanove	(izbira)	(izbira)	

	med ustanovo in ustanovo drugega nivoja (sekundarni, primarni)	(izbira)	(izbira)
	med ustanovo in ustanovo istega nivoja	(izbira)	(izbira)
	med ustanovo in ZZZS	(izbira)	(izbira)
	med ustanovo in MZ	(izbira)	(izbira)
	med ustanovo in IVZ RS	(izbira)	(izbira)
	med ustanovo in …..	(izbira)	(izbira)
34	**elektronski karton pacienta**		
	znotraj ustanove	(izbira)	(izbira)
	med ustanovo in ustanovo drugega nivoja (sekundarni, primarni)	(izbira)	(izbira)
	med ustanovo in ustanovo istega nivoja	(izbira)	(izbira)
	med ustanovo in ZZZS	(izbira)	(izbira)
	med ustanovo in MZ	(izbira)	(izbira)
	med ustanovo in IVZ RS	(izbira)	(izbira)
	med ustanovo in …..	(izbira)	(izbira)
35	**izmenjava digitalnih RTG (PACS) slik**		
	znotraj ustanove	(izbira)	(izbira)
	med ustanovo in ustanovo drugega nivoja (sekundarni, primarni)	(izbira)	(izbira)
	med ustanovo in ustanovo istega nivoja	(izbira)	(izbira)
	med ustanovo in ZZZS	(izbira)	(izbira)
	med ustanovo in MZ	(izbira)	(izbira)
	med ustanovo in IVZ RS	(izbira)	(izbira)
	med ustanovo in …..	(izbira)	(izbira)
36	**posvetovanja/videokonference (zvok in slika)**		
	znotraj ustanove	(izbira)	(izbira)
	med ustanovo in ustanovo drugega nivoja (sekundarni, primarni)	(izbira)	(izbira)
	med ustanovo in ustanovo istega nivoja	(izbira)	(izbira)
	med ustanovo in ZZZS	(izbira)	(izbira)
	med ustanovo in MZ	(izbira)	(izbira)
	med ustanovo in IVZ RS	(izbira)	(izbira)
	med ustanovo in …..	(izbira)	(izbira)
37	**izmenjava kardioloških slik, EKG, videa**		
	znotraj ustanove	(izbira)	(izbira)
	med ustanovo in ustanovo drugega nivoja (sekundarni, primarni)	(izbira)	(izbira)
	med ustanovo in ustanovo istega nivoja	(izbira)	(izbira)
	med ustanovo in ZZZS	(izbira)	(izbira)
	med ustanovo in MZ	(izbira)	(izbira)
	med ustanovo in IVZ RS	(izbira)	(izbira)
	med ustanovo in …..	(izbira)	(izbira)
38	**VoIP - uporaba informacijskega omrežja za prenos zvoka, telefonske storitve,…**		
	znotraj ustanove	(izbira)	(izbira)
	med ustanovo in ustanovo drugega nivoja (sekundarni, primarni)	(izbira)	(izbira)
	med ustanovo in ustanovo istega nivoja	(izbira)	(izbira)
	med ustanovo in ZZZS	(izbira)	(izbira)
	med ustanovo in MZ	(izbira)	(izbira)
	med ustanovo in IVZ RS	(izbira)	(izbira)
	med ustanovo in …..	(izbira)	(izbira)
39	**Drugo**		

	znotraj ustanove	(izbira)	(izbira)
	med ustanovo in ustanovo drugega nivoja (sekundarni, primarni)	(izbira)	(izbira)
	med ustanovo in ustanovo istega nivoja	(izbira)	(izbira)
	med ustanovo in ZZZS	(izbira)	(izbira)
	med ustanovo in MZ	(izbira)	(izbira)
	med ustanovo in IVZ RS	(izbira)	(izbira)
	med ustanovo in …..	(izbira)	(izbira)

40 **Kako vršite zaščito podatkov, ki jih izmenjujete (možnih je več odogovorov)?**

avtentifikacija (angl. *Autentification*)	(izbira)
šifriranje (angl. *Encryption*)	(izbira)
tuneliranje (angl. *Tunneling*)	(izbira)
upravljanje in nadzor dostopa	(izbira)
beleženje dogajanja v omrežju	(izbira)
drugo	(izbira)

41 **Ali vaša oprema omogoča oddaljen dostop (vašim vzdrževalcem, delo od doma,..)?**

DA	(izbira)
NE	(izbira)

42 **Ali bi vas vključitev v nacionalno zdravstveno informacijsko omrežje zanimala?**

DA	(izbira)
NE	(izbira)
Pogojno (kdaj)	(text)

43 **Opombe, mnenja?**

(text)

Za vaše odgovore se vam zahvaljujem!