ELEKTROTEHNIŠKI VESTNIK 82(3): 130-138, 2015
PREGLEDNI STROKOVNI ČLANEK

Pristopi k načrtovanju in razvoju rešitev digitalnega zdravja

Urban Sedlar, Mojca Volk, Janez Bešter

Univerza v Ljubljani, Fakulteta za elektrotehniko, Tržaška 25, 1000 Ljubljana, Slovenija
E-pošta: urban.sedlar@fe.uni-lj.si

Povzetek. Zlivanje medicine in zdravstva z informacijsko-komunikacijskimi tehnologijami je pomemben korak na poti do dostopnejše, kakovostnejše, cenejše in bolj personalizirane zdravstvene oskrbe ter učinkovitejše preventive. Hiter napredek tehnike, ki smo mu priča na drugih področjih, pa v kompleksnih sistemih digitalnega zdravja ni dovolj. Zaradi interdisciplinarnosti področja in velikega števila vključenih deležnikov obstaja nevarnost, da so razvite rešitve neustrezne z vidika zdravnikov, pacientov, regulatorjev ali drugih deležnikov. Posledično je potreben sistematičen pristop k zasnovi in razvoju rešitev. V članku podamo pregled postopka inženiringa zahtev, ki temelji na identifikaciji in vključitvi vseh deležnikov v postopek ugotavljanja in analize zahtev, kar je osnova za poznejše načrtovanje in razvoj sistema. Podamo pregled glavnih deležnikov rešitev digitalnega zdravja in njihovih pričakovanj. Potem opišemo dobre prakse razvijalcev sistema. Končno se dotaknemo še varstva osebnih podatkov, na katerem se srečajo vsi deležniki; to področje ima implikacije tako za delo inženirjev in razvijalcev kot medicinskega osebja ter posledično močno vpliva tudi na arhitekturo in funkcionalnosti celotne rešitve digitalnega zdravja.

Ključne besede: eZdravje, načrtovanje programske opreme, interdisciplinarna komunikacija, varstvo osebnih podatkov pacientov, računalniška varnost

An approach to designing and developing digital health solutions

Merging of medicine and health with the information and communication technologies presents an important step towards a more accessible, higher quality, cheaper and more personalized healthcare, as well as a more efficient prevention. However, the rapid progress of technology alone is not enough. Due to the interdisciplinary nature of the field and the large number of the involved stakeholders, there is a danger that the developed solutions are unsuitable from the perspective of doctors, patients, regulators or any other stakeholder. Therefore, a systematic approach to designing and developing such solutions is needed. In this paper we present an overview of the process of *requirements engineering*, which is based on the identification and involvement of the relevant stakeholders in the process of requirements elicitation and analysis. To provide the basis for designing and developing such systems, we analyze the main stakeholders of the digital health solutions, particularly with regard to their expectations, and present the best practices for software development. Finally, we discuss the issue of data protection, involving each individual stakeholder, because of its implications both for the medical personnel and engineers and its significant impact on the architecture and functionality of the digital health solutions.

Keywords: eHealth, software design, interdisciplinary communication, patient data privacy, computer security

1 UVOD

Digitalno zdravje je hitro razvijajoče se področje, ki združuje zdravstvo, medicino in sodobne informacijsko-komunikacijske tehnologije (IKT). S tem lahko medicinskemu osebju omogoči učinkovitejše delo, pacientom pa lažje obvladovanje zdravstvenih težav. Z uporabo sodobnih digitalnih tehnologij, zlasti brezžičnih naprav in senzorjev, interneta, mobilne povezljivosti, socialnih omrežij, napredka na področju medicinskih oslikav, genomike, obdelave velikih količin podatkov (angl. big data) in zdravstvenih informacijskih sistemov [1] ima potencial, da poveča učinkovitost zdravstvenega sistema [2], obenem pa je vzvod za povečevanje splošnega dobrega počutja populacije [3], podaljševanja življenja in izboljševanja njegove kakovosti.

Pojem digitalno zdravje obsega več sorodnih izrazov [4]: eZdravje (zdravstvene storitve, v katerih so uporabljene IKT tehnologije), mZdravje (zdravstvene storitve s poudarkom na uporabi mobilnih terminalov in omrežij) [5], telemedicina (zagotavljanje zdravstvenih storitev na daljavo) ter oskrba in zdravstvena nega na daljavo. Tako lahko obsega model, v katerem sodelujejo zgolj medicinski strokovnjaki (angl. Business-to-Business, B2B), in model, v katerem medicinski strokovnjaki sodelujejo s pacienti (angl. Business-to-Patient, B2P) [4]. Tretji model, v katerem sodelujejo izključno pacienti med seboj (npr. v spletni skupnosti) [6], pa ima velik potencial z vidika zbiranja statističnih

Prejet 5. maj, 2015
Odobren 19. maj, 2015

podatkov o boleznih, diagnozah in učinkih terapij [7], [8], še večjega pa z vidika medsebojnega obveščanja in komunikacije med pacienti.

Tudi EU priznava velik pomen pobudi eZdravja [9],[10]; drugi akcijski načrt 2012–2020 se osredotoča na spodbujanje raziskav in inovacij s področja eZdravja, promocijo mednarodnega sodelovanja, povečevanja interoperabilnosti storitev eZdravja in povečevanja njegove posvojitve v članicah EU. Evropska komisija ugotavlja, da bi mobilne aplikacije s področja digitalnega zdravja lahko do leta 2017 EU prihranile 99 milijard evrov [11].

Področje digitalnega zdravja je multidisciplinarno in vključuje množico deležnikov (angl. stakeholders) z različnimi znanji in področji ekspertize, od medicine in zdravstva do inženiringa, informatike, prava in družbenih ved, kar je velik izziv za načrtovanje, implementacijo in uvedbo takšnih storitev v klinično prakso.

Eden od projektov, ki se spopadajo z uvajanjem rešitev na tem področju v članicah EU in na Norveškem, je FI-STAR [12], ki na sistematičen način obravnava snovanje, razvoj, testiranje, validacijo in uvedbo rešitev digitalnega zdravja. V članku povzemamo problematiko in dobre prakse, identificirane med razvojem aktualnih rešitev s področja digitalnega zdravja na sedmih lokacijah v EU in na Norveškem; rešitve obsegajo oddaljeno spremljanje diabetesa, KOPB, kardiološke rehabilitacije, stanja onkoloških pacientov in pacientov z bipolarno motnjo ter sledenja in obratne logistike zdravil in informatizacije operacijskih dvoran.

2 PROBLEMATIKA

Rešitve digitalnega zdravja obsegajo širok spekter sistemov in aplikacij: od preprostih, ki pacientom omogočajo informativno spremljanje določenega parametra za lastno uporabo (npr. teža, krvni pritisk, krvni sladkor), do kliničnih, ki so namenjene uporabi v zdravstvenem procesu ali tega celo neposredno uravnavajo. Vsem pa je skupno, da temeljijo na kompleksnem prepletu domenskih znanj s področja medicine, zdravstva, inženiringa in informatike ter še množice povezanih področij. Posledično je za uspešno vzpostavitev in posvojitev rešitve nujno tesno sodelovanje med vsemi deležniki, še zlasti pa med zdravstvenimi strokovnjaki ter inženirji in razvijalci [13].

Z inženirskega vidika sistemi digitalnega zdravja predstavljajo vzajemno delovanje strojne in programske opreme; številne aplikacije, ki imajo za prihodnost velike obete (npr. personalizirana medicina na podlagi obdelave velikih količin podatkov), pa predstavljajo skoraj izključno programsko opremo. Inženirji in informatiki, ki rešitev razvijajo, v številnih primerih ne poznajo dobro medicinskih specifik, načina in scenarijev uporabe sistema, zahtev za delovanje v realnem času [14], zahtev po varnosti [15]–[17], predvsem pa regulatornih omejitev, ki slednje narekujejo. Slabe inženirske prakse, ki imajo lahko na drugih področjih hude finančne posledice, se v zdravstvu dodatno merijo s številom izgubljenih življenj [18] in povzročeno psihološko škodo (npr. objava občutljivih osebnih podatkov).

Vendar pa se rešitev digitalnega zdravja sooča še z drugim, dolgoročnejšim problemom. Rešitev, ki ni bila zasnovana z mislijo na uporabnika, bo poleg naravnega odpora proti spremembam delovnih procesov naletela tudi na odpor uporabnikov zaradi neprijaznosti in slabe uporabniške izkušnje (tako na strani pacientov kot medicinskega osebja) ter na odpor zaradi premajhne dodane vrednosti [19], ki ne upraviči vložka, potrebnega za posvojitev. Kritične napake v zasnovi, ki vplivajo na zanesljivost sistema in zmanjšujejo njegovo varnost, še dodatno zmanjšujejo pripravljenost zdravnikov, da ga uporabljajo v praksi [20],[21]. Posledično je zaradi neustrezne vključitve vseh deležnikov v proces snovanja rešitev klinična uporabnost teh v praksi ogrožena. To je primarni razlog, da je danes večina perspektivnih storitev digitalnega zdravja v praksi nepotrjena, potencialne prednosti, naštete v uvodu, pa ostajajo neuresničene [13],[22].

Če želimo ta trend obrniti, je načrtovanje rešitve nujno izvesti sistematično, spodbuditi vse deležnike, da sodelujejo v procesu, ter med njimi vzpostaviti dialog. Le tako je mogoče zagotoviti ustrezno posvojitev rešitev in njihovo dolgoročno korist. Eden od postopkov, ki to omogočajo, je inženiring zahtev (angl. Requirements Engineering). Pri celotnem postopku pa je po načelih uporabniško usmerjenega načrtovanja (angl. User-centered Design) [23] nujno na osrednje mesto postaviti uporabnika (tj. medicinsko osebje, paciente ali oboje).

3 POSTOPEK INŽENIRINGA ZAHTEV

Inženiring zahtev je disciplina, ki sistematično pristopi k identifikaciji zahtev sistema in jih prevede v specifikacijo, na podlagi katere izvajalec (skupina programerjev in inženirjev) takšen sistem izdela [24]. Postopek inženiringa zahtev je razdeljen v pet glavnih sklopov:

1. **Poizvedovanje o zahtevah** sistema. To se lahko izkaže za netrivialno, saj zahteve lahko obsegajo tudi tacitno oz. implicitno znanje, ki je določeni skupini deležnikov (npr. zdravnikom) samoumevno [25]. Če znanje ni eksplicitno formulirano v obliki zahteve, je to za razvoj sistema ovira, zaradi katere je lahko končna rešitev nezadovoljiva ali neustrezna. Praksa inženiringa zahtev se poslužuje številnih tehnik za odkrivanje zahtev, ni pa mogoče zagotoviti, da so identificirane vse. Posledično je treba postopek kontinuirano izvajati tudi med samim projektom in na novo odkrite zahteve sproti vpletati v zasnovo in razvoj. Tipični načini za poizvedovanje obsegajo anketiranje in intervjuvanje deležnikov, delavnice s preigravanjem scenarijev, viharjenjem (angl. brainstorming), introspekcijo in

modeliranjem, opazovanje delovnega procesa deležnikov, branje dokumentacije in specifikacij obstoječih sistemov, pouporaba zahtev podobnega sistema, prototipiranje ter obratni inženiring in sistemsko arheologijo (tj. ugotavljanje zahtev iz že vzpostavljenih sistemov) [26].

2. **Analiza zahtev** obsega pridobitev poglobljenega razumevanja rešitve oz. produkta, konceptualno modeliranje sistema na podlagi razumevanja zahtev ter identifikacijo in razrešitev morebitnih konfliktov med posameznimi zahtevami ali deležniki. Tako zagotovimo, da so zahteve jasne, nekonfliktne in da vključujejo vse vidike sistema.
3. **Specifikacija zahtev** obsega izdelavo dokumentacije, ki zajema zahteve sistema in programske opreme, s čimer so omogočeni sistematičen pregled, ocena in potrditev zahtev.
4. **Validacija zahtev** poteka nenehno v preostalih štirih fazah. Njen cilj je zagotoviti, da končni produkt/rešitev ustreza potrebam deležnikov; tipični postopki validacije so formalni in neformalni pregledi, za kompleksnejše ali kritične sisteme pa tudi uporaba tehnik *formalne verifikacije*.
5. **Upravljanje zahtev**, ki poteka od začetka projekta do konca uporabe sistema, vključuje spremljanje sprememb zahtev na sledljiv način ter komunikacijo in usklajevanje z vsemi deležniki.

Ključno je, da so že v prvi fazi v postopek poizvedovanja o zahtevah vključeni vsi deležniki.

Opisana metodologija je bila tudi izhodišče projekta FI-STAR, ki obsega sedem različnih pilotov rešitev digitalnega zdravja v sedmih državah, in odziv deležnikov na njeno uporabo je bil izjemno pozitiven. Brez sistematičnega pristopa k iskanju in vključitvi deležnikov ter analizi, validaciji in spremljanju zahtev bi bilo obvladovanje projekta takšne velikosti in kompleksnosti nepredstavljivo.

4 IDENTIFIKACIJA DELEŽNIKOV

Preden je mogoče začeti s poizvedovanjem o zahtevah, je treba deležnike identificirati. V znanstveni literaturi je opisanih več pristopov k njihovi klasifikaciji, vendar je v sistemih digitalnega zdravja najbolj smiselna razdelitev v štiri kategorije: *ponudnike, prejemnike, nadzornike in podpornike* [27]. Te kategorije lahko podrobneje delimo naprej, kot je prikazano na sliki 1.

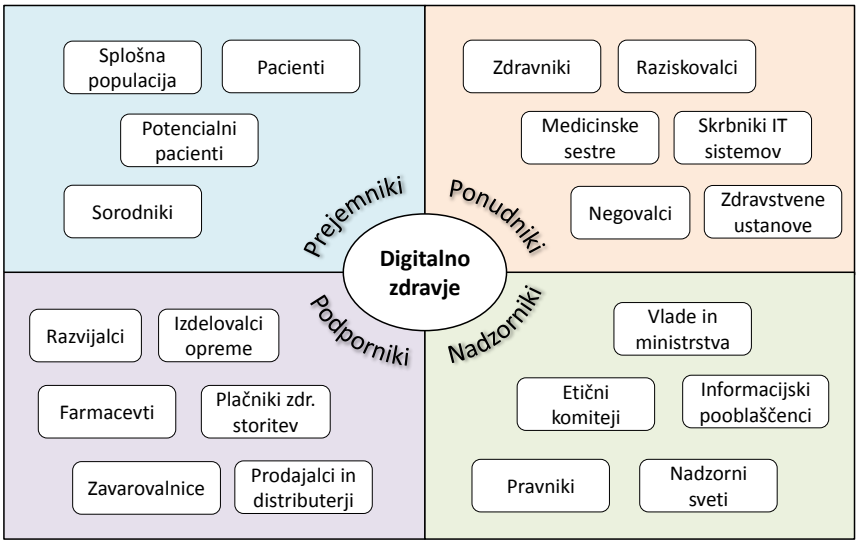
Za vsako od naštetih skupin so v nadaljevanju podrobneje opisana ključna pričakovanja v kontekstu vzpostavitve in uporabe rešitve digitalnega zdravja. Seznam pričakovanj je lahko vodilo za identifikacijo zahtev sistema in kontrolo; rešitev digitalnega zdravja, ki namerno ali nenamerno preprečuje doseganje naštetih ciljev, tvega težave s posvojitvijo, kar dolgoročno ogroža celoten vložek, potreben za njen razvoj in uvedbo.

4.1 Prejemniki

Skupina prejemnikov je razlog za obstoj zdravstvenega sistema, zato je v vsaki rešitvi digitalnega zdravja nujno zagotoviti, da prejemnikom neposredno ali vsaj posredno koristi. Prejemniki obsegajo tako paciente in njihove družinske člane, kot tudi širšo populacijo z vidika preventive; prav zadnji vidik je največji potencial rešitev digitalnega zdravja, saj omogoča spremembo paradigme zdravstvenega sistema od kurative k preventivi.

Ključni cilji rešitve digitalnega zdravja z vidika prejemnikov so:

- Pospeševanje okrevanja; zmanjševanje smrtnosti in morbidnosti.
- Zniževanje stroška oskrbe in skrajševanje čakalnih dob. Večjo dostopnost zdravstvenih storitev ne glede na fizično lokacijo in oddaljenost od zdravstvenih institucij; zmanjševanje potrebe po



Slika 1: Razdelitev deležnikov digitalnega zdravja

obisku zdravstvene ustanove; možnost rehabilitacije doma.
- Boljše in bolj personalizirano svetovanje. Lažja dostopnost do zdravstvenih informacij.
- Zmanjševanje občutka izoliranosti, strahu in izključitve.
- Zagotovitev preproste uporabe in vzdrževanja (če pacient neposredno uporablja rešitev).
- Predstavitev informacij na najprimernejši in najbolj dostopen način (upoštevaje morebitne probleme uporabnosti pri različnih skupinah populacije, npr. starostnikih).
- Skrb za varnost podatkov in zasebnost pacienta.
- Možnost enakopravne uporabe za vse paciente.
- Dovoljevanje svobodne odločitve, katere samostojno zbrane podatke želi uporabnik deliti z medicinskim osebjem.
- Omogočanje spremljanja stanja pacienta na daljavo njegovim skrbnikom. Olajšana možnost komunikacije skrbnika/družinskega člana z zdravniškim osebjem.
- Spodbujanje zdravega načina življenja in ozaveščanje širše populacije; zmanjševanje števila hospitalizacij.

4.2 Ponudniki

Medicinsko osebje je v središču zdravstvenih odločitev; skrbi za pravilno diagnozo, izbiro primerne terapije, spremljanje postopka zdravljenja, vzdrževanje dobrega odnosa s pacienti, ob vsem tem pa tudi spremljanje raziskav in informirano sprejemanje odločitve o njihovi uporabi v praksi. Ponudniki pa poleg medicinskega osebja vključujejo tudi predstavnike medicinskih ustanov in skrbnike informacijskih sistemov. Zlasti zadnji so eden od pogosto spregledanih deležnikov.

Poglavitni identificirani cilji rešitev digitalnega zdravja z vidika ponudnikov so:
- Skrajševanje časa, potrebnega za posameznega pacienta; povečevanje učinkovitosti interakcije s pacientom; olajševanje odločitev; možnost spremljanja pacientov na daljavo; avtomatizacija določenih procesov.
- Omogočanje novih načinov zdravljenja in terapije.
- Lažje zagotavljanje udobja pacientov.
- Zmanjševanje obremenitev, možnosti za napake in potreb po ročnem vnosu podatkov.
- Zagotovitev preproste uporabe rešitve (če jo osebje neposredno uporablja).
- Predstavitev informacij na najprimernejši in najbolj dostopen način (upoštevaje morebitne probleme uporabnosti in uporabniške izkušnje); možnost uporabe rešitve tudi kot pedagoškega orodja za informiranje pacientov.
- Z vidika predstavnika medicinske ustanove: zmanjševanje stroškov hospitalizacije in stroškov medicinskega osebja; preprečevanje nepotrebnih hospitalizacij in povečevanje števila prostih postelj. Varovanje podatkov in zasebnosti pacientov. Možnost enakopravne uporabe rešitve za vse paciente. Ponudba novih storitev in boljša promocija ustanove.
- Z vidika skrbnika informacijskega sistema: rešitev, ki deluje brez napak in s čim manj vzdrževanja; rešitev, ki ne ogroža integritete in zasebnosti podatkov. Rešitev, ki zagotavlja sledljivost podatkov ter je lahko nameščena hitro in brez težav.

4.3 Podporniki

Podporniki zagotavljajo, da zdravstveni sistem nemoteno deluje. Plačniki zagotavljajo financiranje ponudnikov; proizvajalci snujejo in razvijajo rešitve in tehnologije, ki omogočajo nove, boljše in učinkovitejše procese; distributerji pa skrbijo za dobavo dobrin in storitev uporabnikom (bodisi medicinskemu osebju, institucijam ali pacientom).

Glavni identificirani cilji rešitve digitalnega zdravja z vidika plačnikov so cenovna dostopnost storitev, povečanje ekonomske učinkovitosti procesov v zdravstvu ter povečevanje deleža primarne in sekundarne preventive, s čimer se dolgoročno zniža skupni strošek zdravstva.

Z vidika proizvajalcev pa cilji poleg ekonomske rasti obsegajo tudi zagotavljanje varnosti pacientov in varnosti osebnih podatkov, motivacijo za razvoj naprednejših rešitev in gradnikov (senzorjev in merilnikov, algoritmov, računalniških komponent, zdravil, biotehnologije), boljšo standardizacijo biometričnih naprav in skladnost z regulativo.

Posebno vlogo ima med podporniki skupina razvijalcev (informatikov, inženirjev, oblikovalcev, preizkuševalcev in verifikatorjev), ki sodelujejo pri načrtovanju rešitve ter jo končno tudi implementirajo in preizkusijo. Izzive in dobre prakse s tega področja navedemo v poglavju Razvojna ekipa.

4.4 Nadzorniki

Nadzorniki regulirajo zdravstveni ekosistem, s čimer zagotavljajo visok standard zdravstva in varnost pacientov ter skrbijo, da ni ogrožena varnost njihovih osebnih podatkov in zasebnosti.

Cilji rešitve digitalnega zdravja z vidika regulatorjev so predvsem skladnost z lokalnimi, regionalnimi, državnimi in EU smernicami in zakonodajo; skladnost z nacionalnimi in mednarodnimi standardi ter obravnavanje problematike lastništva podatkov in zasebnosti pacienta.

5 RAZVOJNA EKIPA

Vsaka rešitev digitalnega zdravja je kombinacija strojne in programske opreme. Strojno opremo sestavljajo platforma (terminali in strežniki) ter različne vhodno/izhodne naprave (npr. senzorji in aktuatorji). Razvoj strojne opreme zahteva skrbno načrtovanje ter po navadi poteka po metodologiji vodnega slapu (angl.

waterfall), kjer si razvojne faze sledijo zaporedoma: od načrtovanja prek izdelave do testiranja in verifikacije, tej pa sledi še postopek certifikacije z oceno tveganja.

Ker pa je v večini primerov preprosteje in ceneje kupiti in uporabiti obstoječo strojno opremo, hiter napredek elektronike pa tej še dodatno znižuje ceno, je po meri narejena programska oprema pogosto nesorazmerno večji vložek v sistem. Takšne rešitve digitalnega zdravja lahko opišemo kot *programsko intenzivne*.

Pri razvoju programske opreme je poleg modela vodnega slapu z dolgimi razvojnimi fazami na voljo tudi več drugih pristopov. Med njimi sta najbolj znana iterativni razvoj (spiralni model, ki ga sestavlja več krajših iteracij vodnega slapu) in agilna metodologija, ki temelji na fleksibilnem pristopu k razvoju, hitrim odzivom na spremenjene zahteve in pogostim iteracijam [28].

Zaradi interdisciplinarne narave rešitve je v postopek pogosto vključenih več razvojnih in strokovnih ekip, ki na eni strani obsegajo inženirje, informatike, programerje, grafične in industrijske oblikovalce, na drugi pa medicinsko osebje in raziskovalce. Takšna heterogenost poleg potrebe po dobri komunikaciji v posamezni ekipi narekuje tudi potrebo po dobri komunikaciji in sodelovanju med skupinami.

Razvojna ekipa mora v predvidenih rokih zasnovati in razviti programsko opremo, izvesti potrebno testiranje in validacijo ter zagotoviti pomoč pri evalvaciji rešitve. Testiranje mora potekati skozi vse faze razvojnega procesa z uporabo metod, kakršne so preizkusi posameznih enot (angl. unit tests), integracijski preizkusi, ali z uporabo preizkusov na podlagi modela (angl. model-based testing). Postopek validacije ugotavlja skladnost s specifikacijami in standardi. Končno pa morajo razvijalci zagotoviti tudi ustrezno podporo pri integraciji rešitve v klinično okolje. Pri tem je treba upoštevati še možnost dodatnih prilagoditev in nadgradenj za podporo programskih vmesnikov in komunikacijskih protokolov, potrebnih za povezavo novih gradnikov z obstoječo (angl. legacy) infrastrukturo.

Pri samem razvoju programske opreme si razvojna ekipa pomaga z uporaba procesov in orodij za olajševanje in sistematizacijo razvoja ter učinkovitejše sodelovanje. Sem spadajo repozitoriji in sistemi za verzioniranje programske kode, orodja za organizacijo projekta, sistemi za beleženje napak in hroščev (angl. Bug Trackers), kot tudi uporaba avtomatiziranih postopkov testiranja in integracije programske opreme (angl. Continuous Integration). Pregled kode je nuja v vsaki kritični aplikaciji in mora biti prisoten tudi pri vsaki rešitvi digitalnega zdravja, ki nadzira ali vpliva na potek zdravljenja.

Razvita rešitev mora biti tudi uporabniku prijazna, uporabna in koristna. Izhodišče za razvoj uporabniku prijazne aplikacije morajo biti identificirane zahteve in poznavanje konteksta uporabe, v nasprotju z domnevami razvijalcev ali skopim opisom v naročilu, ki ne razkriva nikakršnih domenskih specifik ali implicitnih zahtev. Uporabniška prijaznost je subjektivna metrika, ki jo je mogoče najbolje validirati z izvedbo študije uporabniške izkušnje (angl. User Experience—Ux), del indikatorjev pa je mogoče meriti tudi objektivno, npr. s štetjem klikov/dotikov uporabniškega vmesnika, potrebnih za izvedbo posamezne akcije, ter z uporabo tehnike sledenja očem (angl. Eye tracking).

Drugi z uporabniško prijaznostjo povezan koncept pa je kakovost uporabniške izkušnje (angl. Quality of Experience—QoE). Ta v nasprotju s prijaznostjo interakcije pove, kako hiter je odziv sistema na akcije uporabnika. Zadnje je relativno dobro obvladljiv problem, dokler je sistem v celoti pod nadzorom. Ko pa na zakasnitve vplivajo tudi časi prenosa prek javnega podatkovnega omrežja, lahko odzivni časi in s tem frustracija uporabnika močno narastejo [29]. Smernice s tega področja navajajo tri sekunde kot največji še sprejemljiv odzivni čas sistema na akcijo uporabnika [30].

6 VARSTVO OSEBNIH PODATKOV

Skrb za varovanje podatkov je eden večjih izzivov rešitev digitalnega zdravja, ki ga morajo upoštevati tako razvijalci kot medicinski strokovnjaki. Stroga zakonodaja na eni strani ter hiter napredek ICT in oboroževalna tekma na področju informacijske varnosti na drugi, predstavljata okolje, v katerem je treba skrbno načrtovati vsak varnostni vidik.

Ker na tem področju pridejo v stik vse skupine deležnikov, v nadaljevanju povzemamo ključne problematike, zakonodajo in glavne omejitve, ki jih ta narekuje za izvedbo sistema.

6.1 Zakonodaja

Varovanje zdravstvenih podatkov in varstvo zasebnosti v EU urejajo mednarodni pravni akti in nacionalni zakoni posamezne članice. Pri rešitvi digitalnega zdravja gre tipično za preplet zbiranja, prenosa, shranjevanja, obdelave in posredovanja *občutljivih osebnih podatkov*. V EU je varstvo zasebnosti temeljna človekova pravica, določena tako z Evropsko konvencijo o človekovih pravicah kot z ustavami članic. Tako je na ravni EU treba upoštevati:

- Pravne akte Organizacije združenih narodov (OZN): Splošno deklaracijo o človekovih pravicah, Mednarodni pakt o ekonomskih, socialnih in kulturnih pravicah ter Mednarodni pakt o političnih in državljanskih pravicah; OZN je na tem področju sprejela Smernice glede računalniško vodenih baz osebnih podatkov (UN Guidelines on Computerized Personal Data Files).
- Pravne akte Sveta Evrope: Evropsko konvencijo o človekovih pravicah in temeljnih svoboščinah ter Konvencijo o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov.

- Pravne akte EU: Listino EU o temeljnih pravicah, Uredbo o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah in organih Skupnosti in o prostem pretoku takšnih podatkov, Direktivo 95/46/ES Evropskega parlamenta in Sveta o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter Direktivo o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij.

Poleg zakonodaje in smernic na ravni EU je treba v vsaki članici upoštevati še nacionalne specifike, kar močno zaplete čezmejno sodelovanje in izmenjavo podatkov v rešitvah digitalnega zdravja. Za primer Slovenije evropsko zakonodajo dopolnjujejo še: ustava RS (38. člen) – varstvo osebnih podatkov, zakon o varstvu osebnih podatkov (ZVOP-1), zakon o pacientovih pravicah (ZPacP), zakon o zdravstveni dejavnosti (ZZDej), zakon o zdravniški službi (ZZdrS), zakon o zdravstvenem varstvu in zdravstvenem zavarovanju (ZZVZZ), zakon o zbirkah podatkov s področja zdravstvenega varstva (ZZPPZ), zakon o elektronskem poslovanju na trgu (ZEPT), zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP-UPB1) in zakon o informacijskem pooblaščencu (ZInfP).

Dodatno pa zdravstvene delavce zavezujejo tudi določila medicinske stroke (Hipokratova prisega, Ženevska prisega, Evropske smernice o zaupnosti in zasebnosti v zdravstvenem varstvu, v Sloveniji pa dodatno še Kodeks medicinske deontologije Slovenije in Kodeks etike medicinskih sester in zdravstvenih tehnikov Slovenije).

Ker v praksi lahko pride do različnih ali celo konfliktnih interpretacij zakonskih določil [31], je treba posamezen primer vedno obravnavati individualno, vključenost deležnikov iz skupine *nadzornikov* pa lahko celoten postopek močno olajša.

6.2 Vidiki informacijske varnosti

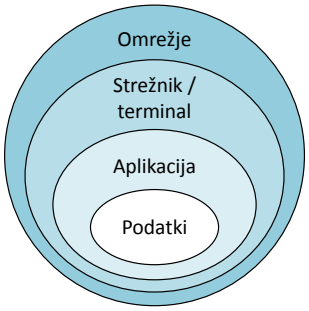
Zakonodaja, povezana z varstvom osebnih podatkov, dobi novo dimenzijo, ko govorimo o digitalnem sistemu. Tradicionalen pristop k varnosti podatkov v zdravstvu je temeljil na omejevanju fizičnega dostopa do zdravstvenega kartona; v digitalnem svetu pa že pojem izvirnika izgubi svoj pomen. Večjo grožnjo varnosti osebnih podatkov pa prinaša dejstvo, da so naprave čedalje pogosteje priključene na komunikacijsko omrežje, ki je povezano z javno telekomunikacijsko infrastrukturo.

Večina podatkovnega prometa se prek omrežij pretaka v obliki paketov Internetnega protokola (IP); same povezave so lahko namenski zakupljeni vodi, še pogosteje pa so kar del javne infrastrukture Interneta. Zadnje še zlasti velja tedaj, ko želimo podatke ali določeno storitev pripeljati neposredno do pacienta, ki komunikacijsko infrastrukturo (modem, usmerjevalnik, terminal) preprosto najema od ponudnika Internetnih storitev.

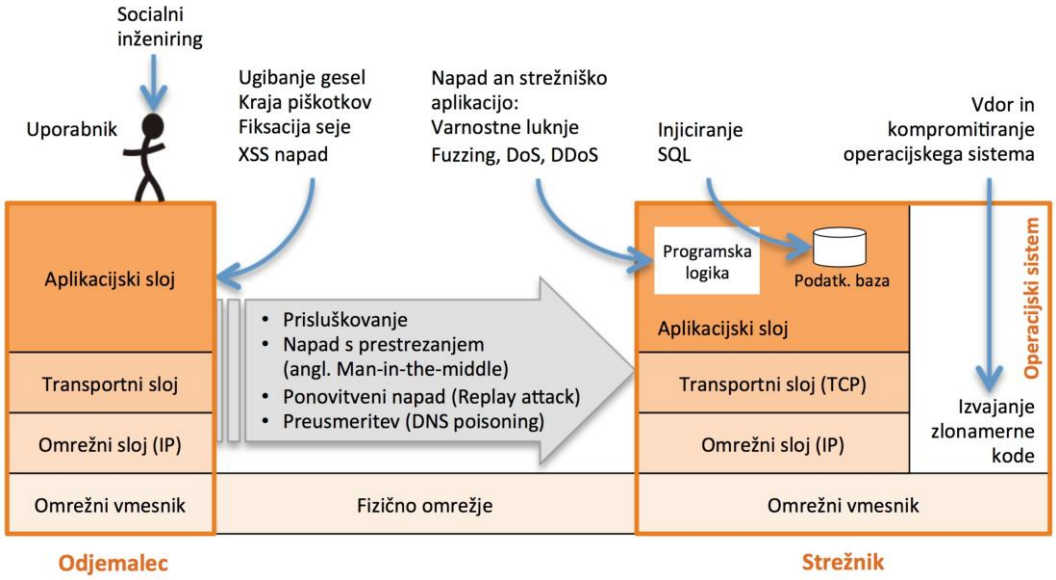
Informacijska varnost je kompleksno področje, ki obsega naslednjih sedem dimenzij [32]:

- **Identifikacija**: pridobivanje podatkov ali metapodatkov, ki enoznačno opisujejo pacienta, zdravnika ali uporabnika.
- **Avtentikacija**: zagotovitev, da je pacient (ali zdravnik) res ta, za kogar se izdaja v postopku identifikacije (to lahko npr. zagotovimo z geslom).
- **Avtorizacija**: zagotovitev, da uporabnik lahko dostopa samo do podatkov (ali izvaja dejanja), za katera je pooblaščen.
- **Nezanikanje** (angl. nonrepudiation): avtentikacija, ki je izvedena tako, da je dokazljiva tudi tretji osebi (posledično uporabnik ne more zanikati, da se je avtenticiral).
- **Integriteta podatkov**: zagotavljanje, da so podatki točni in da se ne morejo nepooblaščeno spremeniti.
- **Razpoložljivost**: zagotovitev, da so podatki vedno dostopni. »Preprečitev dostopa do storitve« (angl. Denial of Service – DoS) je pogost napad, ki si prizadeva zmanjšati ravno razpoložljivosti storitve.
- **Zaupnost**: pomeni, da občutljivi podatki ne morejo priti v roke nepooblaščeni osebi; poleg avtentikacije in avtorizacije to pomeni, da mora biti onemogočeno tudi njihovo prestrezanje na komunikacijskem omrežju, kar je mogoče doseči s šifriranjem.

Za samo varnost podatkov imata pomembno vlogo tudi način in mesto potencialnega napada. Poleg prestrezanja omrežnih podatkov lahko napadalec kompromitira fizično infrastrukturo (strežnik) ali izkoristi ranljivost v aplikaciji ter tako pride do podatkov (slika 2).



Slika 2: Sloji informacijske varnosti



Slika 3: Mesta napada na arhitekturo odjemalec–strežnik

Posledično je v informacijskih sistemih, ki so izpostavljeni javnemu internetnemu omrežju, tipična zahteva tudi anonimizacija ali psevdoanonimizacija podatkov. Anonimizacija zagotovi, da so podatki shranjeni brez vsakršne identifikacije; to zagotavlja, da tudi tedaj, ko podatki pridejo v napačne roke, ni mogoče ugotoviti, na koga se nanašajo, ter tako ne pomenijo kršitve zasebnosti. Žal pa popolna anonimizacija onemogoča tudi poznejšo uporabo v zdravstvenem postopku. Če pa želimo v podatkih ohraniti informacijo, da pripadajo določenemu pacientu (npr. pacientu s šifro 3), govorimo o psevdoanonimizaciji. Takšne podatke je mogoče preprosto deanonimizirati (potreben je le šifrant pacientov), zato je treba iz varnostnih razlogov šifrant hraniti ločeno od podatkov.

Pomembna zahteva zdravstvenih informacijskih sistemov sta tudi beleženje dostopa (ang. logging) in možnost pregleda podatkov o dostopu (angl. auditing). Informacijski sistem mora tako zabeležiti vsak dostop do podatkov, s čimer se doseže popolna sledljivost podatka od prvega vpisa naprej, vključno z vsako spremembo in dostopom.

6.3 *Implikacije za arhitekturo informacijskega sistema*

Danes najpogostejša arhitekturna paradigma informacijskega sistema je odjemalec–strežnik (Slika 3), ki je tudi osnova delovanja svetovnega spleta. Program, ki se obnaša kot klient (tj. odjemalec – pri spletnih aplikacijah je to spletni brskalnik), se poveže na ponudnika podatkov ali storitve (strežnik) in od njega zahteva podatke oz. na njem sproži določeno akcijo.

Ta arhitektura je razširjena predvsem zaradi svoje robustnosti in delovanja v različnih omrežnih konfiguracijah, saj samo strežnik potrebuje javen naslov IP, odjemalec pa se lahko nahaja tudi za omrežnim prehodom oz. v zasebnem omrežju (npr. uporabnik doma). Spletne storitve za prenos podatkov največkrat uporabljajo protokol za prenos hiperteksta (angl. Hypertext Transfer Protocol – HTTP), ki je pred prisluškovanjem (vidik zaupnosti) zaščiten s protokolom za zaščito transportnega sloja (angl. Transport Layer Security – TLS), identiteta odjemalca in strežnika pa je lahko zagotovljena z digitalnim potrdilom.

Prva implikacija zahtev po varnosti podatkov je omejitev, da zaupni podatki ne smejo biti shranjeni na infrastrukturi, ki ni ustrezno zaščitena. V praksi to pomeni, da ni mogoča uporaba strežnikov pri večini ponudnikov gostovanja, kolokacije ali infrastrukture kot storitve (t. i. računalništvo v oblaku). Sprejemljiva je zgolj uporaba infrastrukture v zaščitenem internem omrežju medicinske ustanove, zdravstvenega hrbteničnega omrežja ali pri certificiranih ponudnikih. Druga implikacija je, da strežniki zaradi varnosti ne smejo biti prosto dostopni iz Interneta; to dejstvo močno zaplete dostop uporabnikov (npr. pacientov, zdravnikov) do takšnega sistema, saj se ti pogosto nahajajo v domačem omrežju, na telekomunikacijskem priključku ponudnika internetnih storitev ali na mobilnem omrežju (npr. Edge, 3G, LTE); vsa ta omrežja so del javnega Interneta in uporabljajo naslove, ki jih lahko kompromitira tudi napadalec.

To zaplete arhitekturo sistema za posredovanje podatkov v zaščiteno omrežje (npr. medicinske ustanove); ena od rešitev (Slika 4) je arhitektura, ki se poslužuje vmesnega odložišča – posredovalnega strežnika (angl. proxy server). Posredovalni strežnik se nahaja v t. i. demilitarizirani coni (angl. Demilitarized Zone – DMZ) ponudnika. Ker je dostopen z javnega interneta, lahko sprejema podatke od uporabnikov (npr. z mobilnih naprav, spletnih brskalnikov ipd.). Zaradi dodatne varnosti je treba poskrbeti, da se podatki ne

zapišejo na trdi disk, temveč ostanejo shranjeni zgolj v pomnilniku. Ker pa se tudi posredovalni strežnik ne more povezati v varno cono medicinske ustanove, se mora strežnik iz varne cone periodično sam povezati na posredovalni strežnik in zahtevati nove podatke. Takšna rešitev onemogoča vdor v zasebno cono in omejuje količino podatkov, ki so ogroženi ob morebitnem vdoru v posredovalni strežnik.

Za varnostno ozaveščene in zaupanja vredne uporabnike, ki potrebujejo tudi dostop za branje podatkov, pa je mogoča uporaba navideznega zasebnega omrežja (angl. Virtual Private Network – VPN); tako se uporabnik prek šifrirane povezave poveže neposredno v zasebno omrežje zdravstvene ustanove. Vendar je tudi v tem primeru mogoča omejitev regulative, ki v nekaterih državah prepoveduje, da podatki zdravstveno ustanovo zapustijo. Če pa obstaja zgolj omejitev shranjevanja podatkov zunaj zdravstvene ustanove, je dostop še vedno mogoč z uporabo spletnih tehnologij, pri katerih poskrbimo za izklop funkcionalnosti začasne hrambe na napravi (angl. caching).

Informacijska varnost je kompleksen problem, ki ga zapleta hiter napredek tehnologije, tehnik vdorov in posledično tudi evolucije dobrih praks. Ena takšnih praks številnih ponudnikov storitev je uvajanje programov prijave napak (angl. bug bounty program), ki uporabnikom ponujajo plačilo za odkrite ranljivosti strežniškega sistema ali aplikacije [33]. Ker kljub izjemno skrbni zasnovi in izvedbi informacijskega sistema ni zagotovila, da je sistem imun proti napadom, bi to morala postati pomembna praksa tudi v rešitvah digitalnega zdravja.

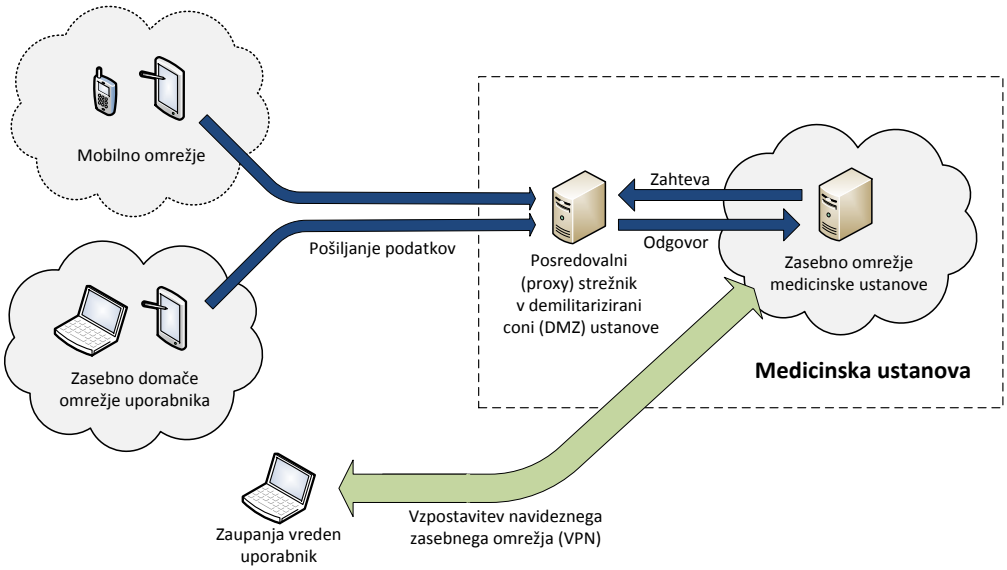
Dodaten problem pa je tudi samo vzdrževanje sistema, saj lahko fizičen dostop do infrastrukture omogoča tudi nepooblaščen dostop do osebnih podatkov; anonimizacija je v tem primeru rešitev le, če IT administratorji nimajo dostopa do celotne infrastrukture oz. vsaj do dela, ki hrani šifrant uporabnikov.

7 SKLEP

Uporaba sodobnih ICT v zdravstvu ima velik potencial, vendar se sooča s številnimi izzivi. Uvajanje novih rešitev je po eni strani oteženo zaradi izjemno močne regulative, po drugi pa zaradi neupoštevanja potreb in zahtev uporabnikov (predvsem zdravstvenega osebja in pacientov).

Problem je mogoče prevesti na manjšega in lažje obvladljivega, če določenih deležnikov namerno ne vključimo (npr. rešitve za spremljanje dobrega počutja, fitnes aplikacije, socialna omrežja za povezovanje pacientov ipd.), vendar pa s tem močno zmanjšamo potencialne koristi. Že boljša povezava pacienta in zdravnika bo zadnjemu omogočala, da bo o pacientu brez dodatnega napora pridobil boljšo anamnezo, kar bo vodilo k boljši diagnozi in zdravljenju. Mehanizmi za zajem takšnih informacij postajajo čedalje bolj dostopni in jih določene skupine pacientov že s pridom izkoriščajo (npr. merjenje krvnega tlaka, spremljanje telesne teže, krvnega sladkorja), poleg aktivnih meritev pa obstaja tudi čedalje več pasivnih načinov spremljanja življenjskega sloga in navad, ki so poleg zagotavljanja zdravstvenega konteksta pacienta lahko tudi vzvod za preventivno ravnanje.

Če želimo izboljšati pretok takšnih občutljivih osebnih informacij med pacientom in zdravnikom ter na njihovi podlagi razviti rešitve digitalnega zdravja, ki bodo koristne, uporabne in uporabniku prijazne, bo tesno sodelovanje vseh deležnikov, še zlasti pa zdravstvenega osebja in razvijalcev, ključnega pomena.



Slika 4: Primer visokonivojske arhitekture informacijskega sistema za varno posredovanje podatkov

LITERATURA

[1] E. J. Topol, The creative destruction of medicine: How the digital revolution will create better health care. Basic Books, 2012.

[2] Ministrstvo za zdravje RS, "Nadgradnja zdravstvenega sistema do leta 2020".

[3] K. Peternel, M. Pogačnik, R. Tavčar, and A. Kos, "A Presence-Based Context-Aware Chronic Stress Recognition System," Sensors, vol. 12, No. 11, pp. 15888–15906, 2012.

[4] D. Rudel, M. Breskvar, J. Gašperšič, and T. Vidjen, "Izhodišča za pripravo nacionalne strategije zdravja na daljavo", 2012.

[5] A. Štern and A. Kos, "Mobile phone as a tool in the areas of health protection," Zdr. Vestn., vol. 78, No. 11, 2009.

[6] "Live better, together! | PatientsLikeMe." [Splet]. Dostopno: http://www.patientslikeme.com/. [Citirano: 11.08.2014].

[7] J. Brubaker, C. Lustig, and G. Hayes, "PatientsLikeMe: empowerment and representation in a patient-centered social network," in CSCW'10; Workshop on Research in Healthcare: Past, Present, and Future, 2010.

[8] J. Frost, S. Okun, T. Vaughan, J. Heywood, and P. Wicks, "Patient-reported outcomes as a source of evidence in off-label prescribing: analysis of data from PatientsLikeMe," J. Med. Internet Res., vol. 13, No. 1, 2011.

[9] "EU policy for eHealth | Digital Agenda for Europe | European Commission." [Splet]. Dostopno: http://ec.europa.eu/digital-agenda/en/eu-policy-ehealth. [Citirano: 11.08.2014].

[10] "Message by Neelie Kroes on 'Healthcare in your pocket.'" [Splet]. Dostopno: http://ec.europa.eu/avservices/video/player.cfm?ref=I088539. [Citirano: 11.08.2014].

[11] "Socio-economic impact of mHealth. An assessment report for the European Union."

[12] "FI-STAR project website." [Splet]. Dostopno: https://www.fi-star.eu/fi-star.html. [Citirano: 11.08.2014].

[13] C. Pagliari, "Design and evaluation in eHealth: challenges and implications for an interdisciplinary field," J. Med. Internet Res., vol. 9, no. 2, 2007.

[14] A. Kos, D. Pristov, U. Sedlar, J. Sterle, M. Volk, T. Vidonja, M. Bajec, D. Bokal, and J. Bešter, "Open and scalable iot platform and its applications for real time access line monitoring and alarm correlation," in Internet of Things, Smart Spaces, and Next Generation Networking, Springer, 2012, pp. 27–38.

[15] S. Adibi and G. B. Agnew, "On the diversity of eHealth security systems and mechanisms.," in Conference proceedings:... Annual International Conference of the IEEE Engineering in Medicine and Biology Society. IEEE Engineering in Medicine and Biology Society. Conference, 2007, vol. 2008, pp. 1478–1481.

[16] "Networked medical device cybersecurity and patient safety: Perspectives of health care information cybersecurity executives."

[17] "It's Insanely Easy to Hack Hospital Equipment | Threat Level | WIRED." [Splet]. Dostopno: http://www.wired.com/2014/04/hospital-equipment-vulnerable/. [Citirano: 11.08.2014].

[18] C. S. Turner, "An Investigation of the Therac-25 Accidents," COMPUTER, vol. 18, No. 9I62/93, pp. 0700–001830300, 1993.

[19] M. van Limburg, J. E. van Gemert-Pijnen, N. Nijland, H. C. Ossebaard, R. M. Hendrix and E. R. Seydel, "Why business modeling is crucial in the development of eHealth technologies," J. Med. Internet Res., vol. 13, No. 4, 2011.

[20] J. Li, A. Talaei-Khoei, H. Seale, P. Ray, and C. R. MacIntyre, "Health care provider adoption of ehealth: systematic literature review," Interact. J. Med. Res., vol. 2, No. 1, 2013.

[21] J. G. Anderson, "Social, ethical and legal barriers to e-health," Int. J. Med. Inf., vol. 76, No. 5, pp. 480–483, 2007.

[22] J. E. van Gemert-Pijnen, N. Nijland, M. van Limburg, H. C. Ossebaard, S. M. Kelders, G. Eysenbach, and E. R. Seydel, "A holistic framework to improve the uptake and impact of eHealth technologies," J. Med. Internet Res., vol. 13, No. 4, 2011.

[23] E. Stojmenova, B. Imperl, T. Žohar, and D. Dinevski, "Adapted User-Centered Design: A Strategy for the Higher User Acceptance of Innovative e-Health Services," Future Internet, vol. 4, No. 3, pp. 776–787, 2012.

[24] I. Sommerville and G. Kotonya, Requirements engineering: processes and techniques. John Wiley & Sons, Inc., 1998.

[25] I. Bray, An introduction to requirements engineering. Pearson Education, 2002.

[26] D. Zowghi and C. Coulin, "Requirements elicitation: A survey of techniques, approaches, and tools," in Engineering and managing software requirements, Springer, 2005, pp. 19–46.

[27] V. Mantzana, M. Themistocleous, Z. Irani, and V. Morabito, "Identifying healthcare actors involved in the adoption of information systems," Eur. J. Inf. Syst., vol. 16, No. 1, pp. 91–102, 2007.

[28] S. I. Hashmi and J. Baik, "Software quality assurance in XP and spiral-A comparative study," in Computational Science and its Applications, 2007. ICCSA 2007. International Conference on, 2007, pp. 367–374.

[29] M. Ullah, M. Fiedler, and K. Wac, "On the ambiguity of Quality of Service and Quality of Experience requirements for eHealth services," in medical information and communication technology (ISMICT), 2012 6th international symposium on, 2012, pp. 1–4.

[30] S. Khirman and P. Henriksen, "Relationship between quality-of-service and quality-of-experience for public internet service," in In Proc. of the 3rd Workshop on Passive and Active Measurement, 2002.

[31] B. Pirkovič, "Normativna ureditev ravnanja z občutljivimi osebnimi podatki v zdravstvu."

[32] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," Future Gener. Comput. Syst., vol. 28, No. 3, pp. 583–592, 2012.

[33] M. Finifter, D. Akhawe, and D. Wagner, "An Empirical Study of Vulnerability Rewards Programs.," in USENIX Security, 2013, vol. 13.

Urban Sedlar je doktoriral leta 2010 na Fakulteti za elektrotehniko Univerze v Ljubljani, kjer je trenutno tudi zaposlen. Njegovo področje raziskovanja obsega aplikacije senzorskih in analitskih sistemov v domenah digitalnega zdravja, kritičnih komunikacij in nadzora operaterskih omrežij.

Mojca Volk je raziskovalka z doktoratom in vodja evropskih projektov v Laboratoriju za telekomunikacije na Fakulteti za elektrotehniko Univerze v Ljubljani. Področja njenega dela so raziskave, razvoj, vzpostavitev pilotov, validacija in poslovno načrtovanje rešitev in storitev e-zdravja in e-medicine v kliničnih in uporabniških okoljih ter sistemov in storitev za urgentne komunikacije in specializiranih aplikacij za podporo intervencijam in nadzor kritičnih infrastruktur v okviru javne varnosti in civilne obrambe.

Janez Bešter je profesor in predstojnik Laboratorija za multimedijo na Fakulteti za elektrotehniko Univerze v Ljubljani. Njegovo raziskovalno in razvojno delo obsega načrtovanje, izvedbo in optimizacijo konvergenčnih komunikacijskih sistemov s poudarkom na uvajanju novih interaktivnih multimedijskih storitev v zdravstvu, energetiki in izobraževanju. Je član v številnih mednarodnih tehnoloških povezavah, deluje na projektih sodelovanja med šolstvom, znanostjo in gospodarstvom ter si prizadeva za vzpostavitev ekosistema talentov.