Varovanje osebnih podatkov v telemedicinskih storitvah

Personal data security in telemedicine services

Rok Bernik,[1] Marija Petek Šter[2]

[1] Medicinska fakulteta, Univerza v Ljubljani, Ljubljana, Slovenija
[2] Katedra za družinsko medicino, Medicinska fakulteta, Univerza v Ljubljani, Ljubljana, Slovenija

Korespondenca/ Correspondence:
Rok Bernik, e: rokbernik5@gmail.com

Ključne besede:
informacijske nevarnosti; videokonferenca; elektronska pošta; spremljanje na daljavo; varnostni ukrepi

Key words:
data compromising; videoconferencing; electronic mail; remote monitoring; security measures

Prispelo: 13. 7. 2020
Sprejeto: 28. 9. 2020

Izvleček

Telemedicina je hitro razvijajoče se področje, ki na učinkovit način zagotavlja zdravstvene storitve. Ker se pri telemedicini, tako kot v vsakdanji običajni klinični praksi, rokuje z občutljivimi osebnimi podatki, se je treba zavedati nevarnosti spletnega kriminala ter spoznati načine za zaščito pred takimi napadi. Področje varovanja osebnih podatkov je slovenski in evropski pravni prostor dobro opredelil, obstajajo pa odprta še nekatera nerazrešena vprašanja na področju telemedicine. Telemedicinske storitve delimo na sinhrone (v realnem času, npr. videokonference) in asinhrone (z zaostankom v komunikaciji, npr. spletna pošta) ter na spremljanje parametrov zdravja na daljavo (spremljanje arterijskega tlaka, krvnega sladkorja ipd.). Vsako od teh področij ima svoje varnostne značilnosti in posebnosti. Varovanje osebnih podatkov je pri telemedicinskih storitvah potrebno zagotoviti na sistemski in individualni ravni. Vsak zaposleni v zdravstvu, ki izvaja storitve na področju telemedicine, mora pri svojem delu skrbeti za varnost podatkov. Posebej pomembno se je redno izobraževati na temo informacijske varnosti. Tudi v Sloveniji se izvaja že sorazmerno veliko telemedicinskih projektov, med katerimi jih je nekaj tudi prešlo v redno uporabo. Eden najobsežnejših zdravstvenih projektov pri nas je projekt *eZdravje*, ki med drugim vključuje tudi nekatere telemedicinske storitve (*TeleKap, Teleradiologija, ePosvet*).

Abstract

Telemedicine is a rapidly evolving field that presents an effective way of providing healthcare services. As its use, likewise everyday clinical practice, involves handling of sensitive personal data, it is necessary to be aware of the dangers posed by cybercrime and ways of protection against such attacks. The field of personal data protection is well defined in the Slovenian and European legislation, but there are some unresolved issues in the telemedicine field. Telemedicine services are divided into synchronous (real-time, e.g. videoconferencing), asynchronous (with a delay in communication, e.g. e-mail) and remote monitoring of patient health parameters (arterial pressure, blood sugar, etc.). Each of these areas has its own security features and peculiarities. The protection of personal data in telemedicine services must be ensured at the systemic and individual levels. Every healthcare employee who uses telemedicine services must ensure data security at their work. It is especially important to conduct regular training on the topic of information security. A relatively large number of telemedicine projects have already been implemented in Slovenia, some of which have been put into regular use. One of the most extensive healthcare projects in Slovenia is the eHealth project, which also includes some telemedicine services (*TeleKap, Teleradiologija, ePosvet*).

Citirajte kot/Cite as: Bernik R, Petek Šter M. Varovanje osebnih podatkov v telemedicinskih storitvah. Zdrav Vestn. 2021;90(3–4):159–72.

DOI: https://doi.org/10.6016/ZdravVestn.3131

1 Uvod

Informacijsko-komunikacijska tehnologija postaja vse pomembnejši del našega življenja. Zaradi njenih pozitivnih lastnosti (npr. časovna učinkovitost) se uporablja tako v osebnem kot poklicnem življenju. Z manjšo zamudo se vse bolj uveljavlja tudi v zdravstvu, kjer se je za določene dejavnosti uveljavil izraz telemedicina.

Telemedicina pomeni uporabo elektronskih komunikacijskih metod in informacijske tehnologije za izvajanje kliničnih storitev na daljavo. Prvič se je koncept telemedicine pojavil sredi 19. stoletja, ko je odkritje telegrafa in kasneje telefona omogočilo hitro komunikacijo na dolge razdalje. Leta 1924 je ameriška revija Radio News objavila ilustracijo, na kateri je družina preko video ekrana komunicirala s svojim zdravnikom. Telemedicina, kot jo poznamo danes, pa se je verjetno razvila v sredini 20. stoletja na osnovi vojaške tehnologije. Na začetku je bila draga in slabo dostopna. Uporaba se je razširila šele proti koncu stoletja po odkritju interneta in s pospešenim razvojem informacijske tehnologije (1,2).

Zaradi uporabe in obdelave občutljivih podatkov pri kliničnem delu je informacijska varnost v telemedicini izrednega pomena. Z vse širšo digitalizacijo narašča tudi nevarnost zlorab in kraje osebnih podatkov. Po nekaterih anketah je celo več kot 80 % zdravstvenih ustanov priznalo, da so bile v preteklosti že žrtve spletnega napada. Znana sta primera, ko so aprila 2004 na računalniškem strežniku v Maleziji odkrili ukradene zdravstvene podatke stótin prebivalcev ZDA, ali pa, ko je pred nekaj leti neznana oseba objavila seznam več kot 4.000 HIV pozitivnih prebivalcev Floride. Eden največjih napadov nasploh pa se je odvijal leta 2016. Napadalci so z vdorom v strežnik druge največje ameriške zdravstvene zavarovalnice *Anthem* pridobili dostop do zdravstvenih podatkov več kot 80 milijonov zavarovancev. Med ukradenimi podatki so bila imena, priimki, naslovi ter podatki o poteku in zdravljenju bolezni. Podobnih primerov je seveda še mnogo več, primere kraje zdravstvenih podatkov pa beležimo tudi v Sloveniji (3,4,5).

V zvezi z varnostjo osebnih podatkov predstavlja veliko tveganje, ker tudi zdravstveni delavci kršijo predpise s področja varstva osebnih podatkov. Informacijski pooblaščenec v svojem letnem poročilu poudarja zlasti naslednje kršitve (6):

- pošiljanje zdravstvenih podatkov po nezavarovanih (nešifriranih) povezavah (običajna elektronska pošta, nešifrirane spletne povezave);
- posojanje avtentikacijskih sredstev za dostop do podatkov (gesel, kartic) ter njihovo neustrezno varovanje;
- curljanje in prodajanje podatkov iz zdravstvenih ustanov za namene neposrednega trženja;

- omejena preglednost in nadzor nad obdelavami podatkov, ki jih izvajajo zunanji izvajalci;
- še premalo zavedanja o neprimernosti širjenja informacij o bolnikih;
- pomanjkljivo zavarovanje prostorov, v katerih se hranijo zdravstvene kartoteke.

2 Pravna ureditev telemedicinskih storitev in varovanja osebnih podatkov

2.1 Pravna ureditev telemedicinskih storitev v Evropski uniji

Telemedicina se na ravni Evropske unije definira kot zdravstvena storitev in storitev informacijske družbe. Kot taka spada v področje uporabe Pogodbe o ustanovitvi Evropske skupnosti in področje veljavne sekundarne zakonodaje (evropske direktive) (7,8):

- Direktiva 2000/31/ES (direktiva o elektronskem poslovanju) ureja nudenje storitev informacijske družbe v državah članicah in med njimi, zajema pa tudi telemedicino.
- Direktiva 2002/58/ES o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij postavlja različne zahteve za ponudnike storitev elektronskih komunikacij, ki zagotavljajo zaupnost komunikacije in varnost njihovih omrežij.
- Direktiva o uveljavljanju pravic bolnikov pri čezmejnem zdravstvenem varstvu (Direktiva 2011/24/EU) ureja področje čezmejne mobilnosti bolnikov ter njihove možnosti za dostop do čezmejnih storitev. Komisija mora na podlagi direktive sprejeti ukrepe, ki bodo omogočali interoperabilnost sredstev, potrebnih za nudenje e-zdravstvenih storitev, vključno s telemedicino.
- Direktiva 2015/1535 določa postopek, ki državo članico obvezuje, da pred sprejetjem na nacionalni ravni Komisiji in ostalim državam članicam sporoči vsak osnutek tehničnega predpisa o storitvah informacijske družbe, vključno s telemedicino.

Sodišče Evropske unije je v različnih sodbah (v zadevi C-385/99, Müller in Van Riet, Recueil 2003; v zadevi C-157/99, Smits in Peerbooms, Recueil 2001, in v zadevi C-372/04, Watts, Zodl. 2006) potrdilo, da zdravstvene storitve niti zaradi svojih posebnosti niti zaradi načina organiziranosti ali financiranja niso izvzete iz obsega temeljnega načela prostega pretoka. Uporabniki zdravstvenih storitev torej lahko iščejo in prejmejo zdravstveno pomoč v drugi državi članici, in sicer ne glede na to, kako se storitev opravi, torej tudi s telemedicino (7).

2.2 Pravna ureditev telemedicinskih storitev v Republiki Sloveniji

Državni zbor Republike Slovenije (RS) je leta 2017 sprejel Zakon o spremembah in dopolnitvah Zakona o zdravstveni dejavnosti, s katerim je v pravni red RS prenesel Direktivo 2011/24/EU. S tem je spremenil besedilo 3. člena Zakona o zdravstveni dejavnosti in opredelil pomen telemedicine (9): »Zdravstvene storitve, glede katerih sta lahko ob upoštevanju pravil medicinske doktrine bolnik in izvajalec ali več izvajalcev zdravstvene dejavnosti prostorsko ločena, se lahko opravijo z uporabo informacijskih in telekomunikacijskih tehnologij (v nadaljnjem besedilu: telemedicina). Zdravstvena dokumentacija

se v tem primeru posreduje v skladu s predpisi o varstvu osebnih podatkov, ki se nanašajo na prenos občutljivih osebnih podatkov prek telekomunikacijskih omrežij. V primeru opravljanja zdravstvene dejavnosti v obliki telemedicine se šteje, da je zdravstveno varstvo zagotovljeno v državi, v kateri ima sedež izvajalec zdravstvene dejavnosti, ki opravlja telemedicino.«

Pri izvajanju telemedicinskih storitev je pri prenosu in obdelavi medicinskih podatkov treba upoštevati obstoječo nacionalno zakonodajo, ki to področje ureja, zlasti (10,11):

- Zakon o zdravstveni dejavnosti (ZZDej),
- Zakon o zdravniški službi (ZZdrS),
- Zakon o pacientovih pravicah (ZPacP),
- Zakon o zdravstvenem varstvu in zdravstvenem zavarovanju (ZZVZZ),
- Zakon o zbirkah podatkov s področja zdravstvenega varstva (ZZPPZ),
- Zakon o varstvu osebnih podatkov (ZVOP-1),
- Zakon o informacijski varnosti (ZInFV),
- Zakon o elektronskih komunikacijah (ZEKom-1),
- Zakon o elektronskem poslovanju na trgu (ZEPT),
- Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP).

2.3 Osebni podatki in njihovo varstvo

Zakon o varstvu osebnih podatkov, veljaven za ozemlje Republike Slovenije, opredeljuje osebni podatek kot kateri koli podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen. Med občutljive osebne podatke spadajo vsi podatki o narodnem, rasnem ali narodnostnem poreklu, političnem, verskem ali filozofskem prepričanju, članstvu v sindikatu, zdravstvenem stanju, spolnem življenju, vpisu ali izbrisu v ali iz kazenske evidence ali evidenc, ki se vodijo na podlagi zakona, ki ureja prekrške. Mednje sodijo tudi biometrične značilnosti, če je z njihovo uporabo mogoče določiti posameznika v zvezi s kakšno od prej navedenih okoliščin (12).

Varstvo osebnih podatkov obravnavajo številne odločbe EU že v primarni zakonodaji. Omenjeno je v 16. členu Pogodbe o delovanju Evropske unije. Nadalje se obravnava v Listini Evropske unije o temeljnih pravicah v 7. in 8. členu. Direktivo 95/46/ES o varstvu osebnih podatkov, ki je bila do nedavnega najpomembnejša za to področje, je maja 2018 nadomestila Splošna uredba o varstvu osebnih podatkov (t. i. GDPR oz. Splošna uredba), ki med drugim določa, da morajo podjetja v javnem sektorju ter v nekaterih primerih tudi v zasebnem, določiti odgovorno osebo za varstvo podatkov, ki bo upravljalcu svetovala pri vprašanjih, povezanih z varstvom osebnih podatkov. Prepoveduje tudi obdelavo posebnih vrst osebnih podatkov (tudi podatkov v zvezi z zdravjem), razen če gre za izjeme, naštete v 9. členu Splošne uredbe. Direktiva (EU) 2016/1148 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji določa ukrepe za dvig ravni informacijske varnosti in vzpostavitev mehanizmov za odzivanje na kibernetske grožnje. Državam članicam nalaga, da vzpostavijo nacionalni okvir za varnost omrežij in informacij, ki vsebuje državno strategijo, vsaj en odzivni center in pristojni nacionalni organ, katerega naloga je usklajevati aktivnosti na ravni države. Poleg tega se varstva osebnih podatkov dotikajo tudi številne strategije in smernice, npr. Digitalna agenda

2020, Evropska strategija za podatke, ipd (3,10,13).

Na nacionalni ravni varstvo osebnih podatkov obravnava že Ustava Republike Slovenije, v kateri 35. člen opredeljuje varstvo zasebnosti, 38. člen pa zagotavlja varstvo osebnih podatkov, prepovedana pa je uporaba osebnih podatkov v nasprotju z namenom njihovega zbiranja (3). Lastnik osebnih podatkov je v skladu s slovensko zakonodajo bolnik, na katerega se posamezni podatki nanašajo. Lastnik nosilcev podatkov je organizacija, ki dokumentacijo hrani. Ta mora poskrbeti za varovanje osebnih podatkov, pri čemer morajo njeni zaposleni spoštovati vsa etična načela in predpise o varovanju osebnih podatkov, vključno z Zakonom o varovanju osebnih podatkov. Zdravnik, ki hrani bolnikovo zdravstveno dokumentacijo, je neposredno odgovoren za izvajanje določil zakona (14). Pomembno vlogo imata tudi Zakon o pacientovih pravicah, v katerem sta bistvena predvsem 43. in 44. člen, ki opredeljujeta zasebnost in pravico bolnika do zaupnosti osebnih podatkov, ter Zakon o informacijski varnosti, ki ureja področje informacijske varnosti in ukrepe za doseganje visoke ravni varnosti omrežij in informacijskih sistemov v RS. Izdane so bile tudi številne smernice, ki pomagajo pri interpretiranju pravnih dokumentov (npr. Smernice za izvajalce zdravstvenih storitev, Smernice za zavarovanje osebnih podatkov v informacijskih sistemih bolnišnic ipd.) (3,15).

3 Vidiki varovanja osebnih podatkov v telemedicinskih storitvah

Telemedicinske storitve morajo za varno izvajanje zadostiti splošnim informacijskim varnostnim zahtevam. Mednje spadajo zaupnost, verodostojnost, nadzor dostopa, celovitost, razpoložljivost ter nezmožnost zanikanja (4,16,17):

- *Zaupnost* (*angl.* confidentiality) je najosnovnejša funkcija varnosti. Zagotavlja, da lahko do podatkov dostopajo samo pooblaščene osebe, katerih istovetnost je bila pred tem potrjena, in le v takem obsegu, da lahko učinkovito opravljajo svoje delo.
- *Verodostojnost* (*angl.* authentication) je storitev ugotavljanja istovetnosti osebe oz. izvora podatkov. Za ta namen uporabljamo gesla, PIN-kode, digitalne podpise, izkaznice, prstne odtise idr.
- *Nadzor dostopa* (*angl.* authorisation) pomeni preverjanje, ali ima neka oseba oz. računalnik pravico za določen poseg.
- *Celovitost* (*angl.* integrity) pomeni točnost in nespremenjenost podatkov. Za zagotavljanje celovitosti je potrebno vzpostaviti sistem za nadzor in beleženje vsake spremembe podatkov.
- *Razpoložljivost* (*angl.* availability) pomeni stalen dostop do podatkov in sicer tudi v primerih električnih izpadov, okvare programske ali strojne opreme ipd. Za vzdrževanje razpoložljivosti je pomembno vzpostaviti različne preventivne ukrepe.
- *Nezmožnost zanikanja* (*angl.* non-repudiation) je pomembna za dokazovanje storjenega dejanja, še posebej pri zanikanju, tj. če se taji.

Grožnje oz. napade glede na vpliv na normalen pretok informacij preko omrežja delimo na prekinitev, prestrezanje, spreminjanje in ponaredbo. Podrobnejše razlage posameznih vrst napadov so dostopne v prispevku Zain J, et al (18).

Vsaka organizacija mora prepoznati svoje varnostne potrebe in izdelati načrt za izpolnjevanje varnostnih zahtev. Pri tem se lahko poslužujejo različnih že pripravljenih priporočil ali standardov (ITIL, COBIT, ISO, CALDICOTT ipd.). Med najbolj uveljavljenimi na tem področju sta mednarodna standarda ISO/IEC 27001 (Informacijska tehnologija – Varnostne tehnike – Sistemi za upravljanje varovanja informacij – Zahteve) in ISO/IEC 27002 (Informacijska tehnologija – Varnostne tehnike – Kodeks za upravljanje varovanja informacij), ki med drugim določata vzpostavitev sistema upravljanja za varovanje informacij (19).

Telemedicinske storitve delimo na (20):

- asinhrone (shrani in pošlji, *angl.* store-and-forward);
- sinhrone (v realnem času, *angl.* real-time);
- spremljanje parametrov zdravja na daljavo (*angl.* telemonitoring, remote monitoring).

Vsako področje ima z vidika informacijske varnosti svoje posebnosti.

3.1 Asinhrone telemedicinske storitve (shrani in pošlji)

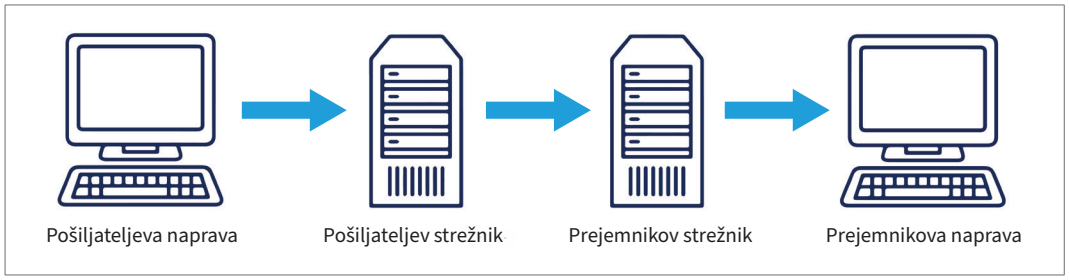
O asinhronih telemedicinskih storitvah govorimo, ko zdravstvene podatke (npr. slike, video posnetje) pošiljamo preko elektronskih omrežij v pregled in oceno, ki se izvedeta kasneje. Metoda se pogosto uporablja v dermatologiji, radiologiji in patologiji (20). Podatki se lahko pošiljajo po elektronski pošti ali pa se naložijo na spletni strežnik, do katerega lahko prejemnik dostopa, ko želi (21). Novejši način pa je posredovanje podatkov preko računalništva v oblaku (*angl.* cloud computing) (22).

3.1.1 Varnost elektronske pošte

Elektronska pošta je, tudi v zdravstvu, eden najbolj razširjenih in priročnih načinov za komuniciranje. Še posebej pogosto se uporablja med specialisti družinske medicine za komunikacijo z bolniki in tudi z ostalimi zdravstvenimi delavci. Tak način komunikacije pa je lahko z vidika varovanja osebnih podatkov zelo tvegan. V ZDA so npr. napadalci samo v obdobju 2009–2015 pridobili dostop do osebnih zdravstvenih podatkov več kot 100 organizacij, ki so uporabljale neustrezno zaščiteno elektronsko pošto. Pomembno je, da uporabniki razumejo nevarnosti take komunikacije ter se znajo pred njimi tudi ustrezno zavarovati (23,24).

Da bi razumeli, zakaj je pošiljanje podatkov po elektronski pošti lahko nevarno, moramo najprej vedeti, kako elektronska pošta deluje. V nasprotju z navadno pošto se pri elektronski pošti sporočilo ne prenaša od ene točke do druge, temveč se kopira na vsak člen verige prenosa. Sporočilo nastane na pošiljateljevi napravi (računalniku), od koder potuje na strežnik pošiljateljeve elektronske pošte. Od tam se prenese na prejemnikov strežnik elektronske pošte ter končno na prejemnikovo napravo (Slika 1). Napadalci lahko pridobijo dostop do zdravstvenih podatkov med samim prenosom sporočila ali pa z dostopom do posameznih členov komunikacijske verige. Vse našteto je torej potrebno primerno zaščititi (24,25).

Varnost prenosa lahko povečamo na več načinov. Najpomembnejša je uporaba kriptografije. Sporočilo pri tem s pomočjo različnih algoritmov (npr. 3DES, AES) zašifriramo, odšifrira pa ga lahko samo prejemnik z uporabo posebnega ključa. Osebni podatki so tako teoretično zavarovani med celotnim prenosom, vseeno pa so ranljivi, če je ogrožen



Slika 1: Shema prenosa sporočila po elektronski pošti (24).

pošiljateljev ali prejemnikov računalnik. V primeru, da podatke pošiljamo v priponki sporočila, lahko zašifriramo tudi ta del. Kot splošno pravilo velja, da so prosto dostopne internetne rešitve elektronskega sporočanja (Gmail, Hotmail, AOL) neenkriptirane, torej niso dovolj varne za prenos zdravstvenih podatkov. Prav tako je pomembno, da za zaščito naših računov uporabljamo dovolj kompleksna gesla. Geslo mora biti načeloma dolgo vsaj 8 znakov ter mora vsebovati velike in male črke, številke in posebne znake. Kot geslo ne bi smeli uporabljati besed, ki jih lahko najdemo tudi v slovarju. Priporočeno je, da geslo zamenjamo vsaj vsakih 90 dni. V elektronsko pošto je smiselno tudi vključiti ponavljajoči se del, ki bolnika oz. prejemnika opozori, da sporočilo vsebuje zdravstvene podatke in je zato potrebno poskrbeti za njihovo zaščito (24,26).

3.2 Sinhrone telemedicinske storitve (v realnem času)

Pri sinhronih telemedicinskih storitvah prenos zdravstvenih podatkov poteka v realnem času. V veliki večini primerov gre za uporabo videokonferenčnih aplikacij za komuniciranje med dvema ali več uporabniki, ki so lahko bolniki in/ali zdravstveni delavci (27). Takšna vrsta komunikacije je postala še posebej aktualna med pandemijo covida-19, ko se je začela pogosteje uporabljati v ambulantah kot alternativa obiska ordinacije v živo.

Ker telemedicinski videokonferenčni pogovori vsebujejo občutljive osebne podatke, so lahko pogosto tarča spletnega kriminala, ki izrablja šibkost varnosti videokonferenčnih aplikacij. Kot primer navajam varnostne pomanjkljivosti videokonferenčnih aplikacij Webex in Zoom, ki so bile odkrite v začetku leta 2020. Te so nepooblaščenim osebam omogočale vstop na zasebne sestanke in objavljanje neželenih in tudi prepovedanih vsebin (t. i. »Zoom-boombing«). Poleg tega so napadalci ukradli in preko t. i. temnega spleta (*angl.* dark web) prodajali na tisoče uporabniških imen in gesel (v aprilu celo več kot 500.000). Primerov zlorab je sicer še mnogo več (28,29,30).

Ameriška Nacionalna varnostna agencija (*angl.* National Security Agency, NSA) je aprila 2020 objavila analizo največkrat uporabljenih komercialno dostopnih videokonferenčnih aplikacij skupaj s priporočili za njihovo uporabo (Tabela 1). Merila, ki jih je pri tem uporabila, so (31,32):

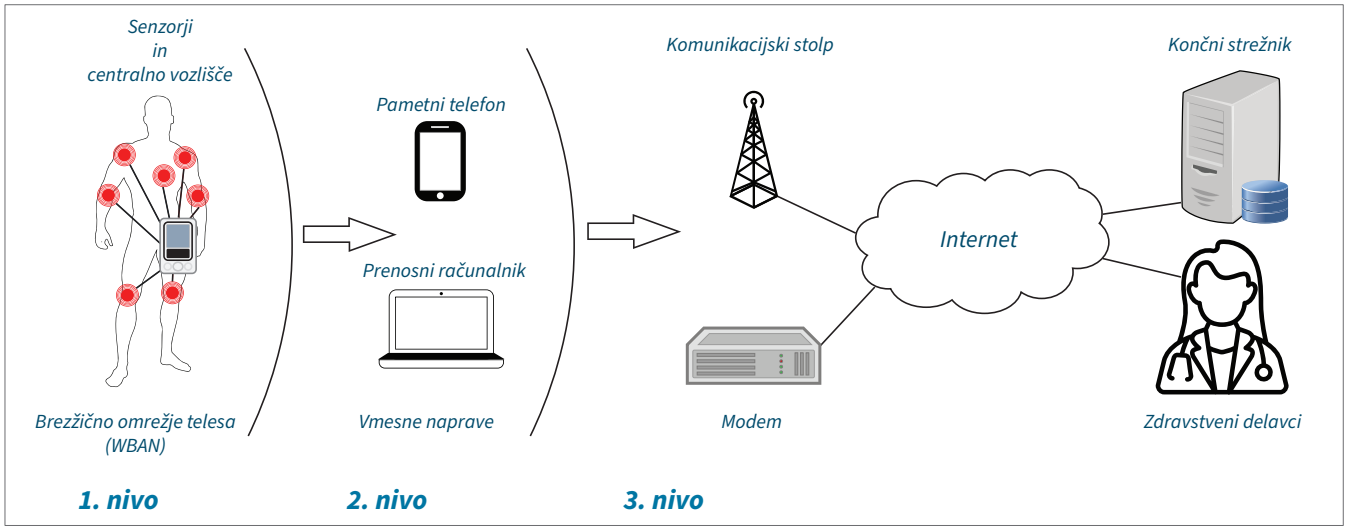
- Ali uporablja aplikacija enkripcijo od pošiljatelja do prejemnika (*angl.* end-to-end encryption, E2E)?
- Ali uporablja močne in dobro uveljavljene standarde enkripcije?
- Ali uporablja multifaktorsko preverjanje istovetnosti?
- Ali lahko uporabniki vidijo in nadzorujejo, kdo se pridruži zasebnemu pogovoru?

Tabela 1: Ocena videokonferenčnih aplikacij (31).

Storitev	Osnovne funkcije	1 – E2E šifriranje	2 – Preverljivi standardi šifriranja	3 – MFA	4 – Nadzor nad pridruževanjem	5 – Posredovanje podatkov tretjim osebam	6 – Varno odstranjevanje podatkov	7 – Javna dostopnost izvorne kode	8 – Certifikacija storitve (FedRAMP / NIAP)
Cisco Webex®	a, b, c, d, e	D[1]	D	D[12]	D[1]	D	Odjemalec – D Strežnik – N[3]	N	FedRAMP
Dust	a	D	N[3]	N	D	N	Odjemalec – D Strežnik – D	N	N
Google G Suite™	a, b, c ,d	N	D	D[1]	D[1]	D	Odjemalec – D Strežnik –D[2]	N	FedRAMP
GoToMeeting®	a, b, c	D[1]	D	N	D[1]	D	Odjemalec – D Strežnik – N[3]	N	N
Mattermost™	a, b, c,e	D	D	D[2]	D	N	Odjemalec – D Strežnik – N	D	FedRAMP
Microsoft Teams®	a, c, d, e	N	D	D	D	D	Odjemalec – D[1] Strežnik – D[1]	N	FedRAMP
Signal®	a, b, d	D	D	D	D	D	Odjemalec – D Strežnik – D	D	N
Skype for Business™	a, c, d, e	D[4]	D[4]	D	D	N	Odjemalec – D Strežnik –N[3]	N	N
Slack®	a, c, d, e	N	D	D	D	N[3]	Odjemalec – N Strežnik – N	N	FedRAMP
SMS sporočilo	a, d	N	N	N	N	N	Odjemalec – D Strežnik – N	N	N
WhatsApp®	a, c, d	D	D	D	D	D	Odjemalec – D Strežnik – D	N	N
Wickr®	a, c, d, e	D	D	D	D	D	Odjemalec – D Strežnik – D	D	N
Zoom®	a, b, c, e	D[1,4]	D	N	D	D	Odjemalec – D Strežnik – N[3]	N	FedRAMP

Legenda: D = da, N = ne; (a) tekstoven pogovor, (b) zvočna konferenca, (c) videokonferenca, (d) deljenje datotek, (e) deljenje zaslona; MFA (*angl.* multi-factor authentication) – multifaktorsko preverjanje istovetnosti; [1] nastavljivo; [2] brezplačna različica; [3] ni objavljenih podrobnosti; [4] delno.

- Ali politika zasebnosti aplikacije dovoljuje delitev uporabnikovih podatkov s tretjimi osebami?
- Ali imajo uporabniki pravico do izbrisa svojih podatkov iz storitve in njenih hranilnic podatkov?
- Ali je izvorna koda aplikacije javno dostopna (tako je mogoče preveriti, kakšne varnostne mehanizme aplikacija uporablja, ter, ali so ti ustrezni)?
- Ali je aplikacijo ocenjevala in certificirala za uporabo priznana organizacija, usmerjena v informacijsko varnost?



Slika 2: Trinivojska arhitektura sistema za spremljanje parametrov zdravja na daljavo. Povzeto po Partala J, et al (33).

Iz tabele je razvidno, da med aplikacijami, ki se pri nas pogosteje uporabljajo, po merilih poročila, velja za najbolj varno Cisco Webex.

Za varno izvajanje videokonferečnega klica pa smo v veliki meri odgovorni tudi sami. Varnost lahko povečamo s sledenjem naslednjim priporočilom (28):

- Vedno je potrebno zaščititi pogovor z geslom.
- Odsvetuje se deljenje podatkov sestanka po javno dostopnih platformah.
- Priporoča se uporaba gostiteljevih kontrol za zapiranje sobe, ko so se vsi povabljeni pridružili pogovoru ali pa za odstranjevanje neželenih gostov.
- Priporoča se izključitev možnosti pošiljanja datotek znotraj videokonference.
- Vključimo lahko t. i. čakalnico, preko katere gostitelj selektivno sprejema goste v pogovor.
- Potrebno je redno nameščanje najnovejših popravkov in nadgradenj videokonferenčnih aplikacij.

3.3 Spremljanje parametrov zdravja na daljavo

Tukaj govorimo o uporabi različnih tehnoloških naprav za nadzorovanje oz. spremljanje bolnikovih zdravstvenih parametrov. Spremljanje na daljavo se v svetu uporablja predvsem pri zdravstveni obravnavi kroničnih bolnikov s srčno-žilnimi boleznimi (meritve krvnega tlaka), sladkorno boleznijo (meritve sladkorja v krvi) ali z astmo. Tako spremljanje je smiselno, saj je stroškovno učinkovito in omogoča pogostejše kontrole (20). Sistem, ki se pri tem uporablja, je sestavljen iz več komponent in je z vidika varnosti sorazmerno kompleksen (Slika 2). Prvi del ima enega ali več senzorjev oz. merilnih naprav, ki so skupaj s centralnim vozliščem organizirane v t. i. brezžično omrežje telesa ali WBAN (*angl.* wireless body area network). Senzorji komunicirajo s centralnim vozliščem, podatki pa se nato preko vmesne naprave (npr. pametnega telefona, prenosnega računalnika) posredujejo do končnega strežnika. Komunikacija je organizirana na treh ravneh. Prva raven

zajema komunikacijo znotraj WBAN-a, med senzorji oz. merilnimi napravami in centralnim vozliščem, druga med centralnim vozliščem in vmesno napravo, tretja pa od vmesne naprave preko javnega omrežja (npr. interneta) do končnega strežnika, kjer se podatki zbirajo in obdelujejo. Vsak ima z vidika varnosti svoje značilnosti in posebnosti (33).

Brezžično omrežje telesa deluje na zelo kratki razdalji (nekaj metrov). To pomeni, da bi se moral napadalec za prestrezanje radijskih signalov fizično precej približati bolniku, kar pa je manj verjetno. Taki napadi bi lahko postali večji problem v prihodnosti, če se bo uporaba sistemov za spremljanje zdravstvenih parametrov dovolj razširila. V tem primeru bo do napadov verjetno prihajalo predvsem na javnih mestih. Z vidika varnosti je na prvi ravni najpomembnejši novejši standard IEEE 802.15.6, ki skrbi za celovitost, istovetnost ter zaupnost podatkov (33).

Druga raven (med WBAN in vmesno napravo) deluje na precej večjih razdaljah kot prva in je zato izpostavljena tudi napadom prisluškovanja, sledenja in preusmerjanja podatkov. Dodatno ranljivost predstavlja vmesna naprava. Napadalec lahko tako dobi dostop do omrežja preko mobilne naprave, okužene z neželeno programsko opremo ali do prenosnega računalnika. Na tej ravni je z vidika varnosti pomembna tudi vrsta uporabljene komunikacijske tehnologije. Bluetooth prinaša s seboj kar nekaj varnostnih pomanjkljivosti ter tudi zanj specifičnih vrst napadov, kot je t. i. Bluejacking. Za varnejšega velja Zigbee, ki določa tudi skupino visokonivojskih varnostnih protokolov. Na drugi ravni je pomembna tudi uvedba standarda IEEE 802.15.4, ki zagotavlja zaupnost podatkov in njihovo večjo varnost (33).

Na tretji ravni (med vmesno napravo in končnim strežnikom) poteka komunikacija preko javnih omrežij, zaradi česar je izpostavljena napadom prisluškovanja, spreminjanja, preprečevanja dostopnosti, prevzemanja nadzora ipd. Podatki se shranjujejo na končnem strežniku, ki mora uporabljati ustrezne mehanizme za omejevanje dostopa, med katere spada tudi uporaba požarnih zidov. Programska oprema končnega strežnika se mora ažurno nadgrajevati z najnovejšimi popravki. Smiselna je tudi uporaba t. i. navideznega zasebnega omrežja (*angl.* virtual private network, VPN), s katerim je mogoče ustvariti navidezno izolirano povezavo z ostalimi deli sistema za spremljanje na daljavo. Najnevarnejši na tej ravni so verjetno napadi s pomočjo t. i. socialnega inženiringa (npr. pošiljanje lažne elektronske pošte, preko katere napadalec dobi nadzor nad sistemom) (33).

Pregled dostopne literature kaže, da se raziskovalci redko ukvarjajo s problemom varovanja osebnih podatkov ob uporabi tehnologije za spremljanje parametrov zdravja na daljavo. Glavni problem pri tem naj bi bila neinformiranost na področju informacijske varnosti. Prav tako obstaja le malo dokazov o učinkovitem uvajanju varnostnih mehanizmov v sisteme za spremljanje na daljavo. Večina študij predvideva, da je varovanje osebnih podatkov odgovornost proizvajalca medicinske oz. komunikacijske tehnologije (34).

4 Ukrepi za zagotavljanje varnosti osebnih podatkov v telemedicinskih storitvah

Varnost prenosa in obdelave osebnih podatkov lahko pri izvajanju telemedicinskih storitev izboljšamo z različnimi ukrepi. Mednje sodijo (11,17):

- izdelava varnostnih preslikav (rezervnih kopij podatkov);
- določitev natančno definiranih kategorij dostopov (zdravnik, medicinska sestra, upravljalec omrežja ipd.);
- namestitev najnovejše protivirusne zaščite;
- uporaba osebnih požarnih zidov (*angl.* firewall);
- uporaba varnostnih ključev, certifikatov, enkratnih gesel;
- uporaba dovolj kompleksnih gesel;
- uporaba kriptografije za šifriranje poslanih podatkov;
- vzpostavitev sistemov za zaznavanje vdorov v omrežje;
- vzpostavitev sistemov za nadzor podatkovne infrastrukture;
- redno nameščanje popravkov programov in operacijskih sistemov;
- uporaba samo preverjenih programov;
- decentralizirano hranjenje podatkov;
- izobraževanje zaposlenih o dobri varnostni praksi;
- negovanje varnostne kulture med zaposlenimi;
- preprečevanje fizičnega dostopa do opreme.

Tako kot velja pri ostalih omrežjih, je tudi varnost telemedicinskega omrežja odvisna od njegovega najšibkejšega člena. Zato je treba neprestano preverjati varnost ter odkrivati morebitne šibke točke sistema in jih ažurno odpravljati (4).

Pogost problem pri zdravstvenih delavcih so nezakoniti vpogledi v zbirke osebnih podatkov bodisi zaradi radovednosti bodisi zaradi pridobivanja osebnih podatkov za lastne namene. Vpogled v osebne podatke bolnika je dovoljen samo, če zaposleni sodelujejo v procesu zdravstvene obravnave bolnika ali iz drugih zakonitih razlogov (npr. sporočanje o primeru policiji, izdaja računa). Kjer je to le mogoče, je treba omejiti dostop do osebnih podatkov z določanjem kategorij dostopov. V skladu s 24. členom ZVOP-1 je potrebno tudi vzpostaviti sistem za notranjo sledljivost obdelave osebnih podatkov (5).

Pomemben vidik pa je tudi varovanje podatkov pri samih uporabnikih – bolnikih. Potrebno jih je poučiti o možnih tveganjih za varnost podatkov, ki so prisotni ob uporabi telemedicinskih storitev. To je še posebej pomembno pri storitvah spremljanja zdravstvenih parametrov na daljavo, kjer se poslužujemo novejših tehnoloških rešitev, a uporabe bolniki (predvsem starejši) pogosto niso vešči. Če za komuniciranje z zdravstvenimi delavci uporabljajo nezavarovane informacijsko-komunikacijske rešitve, jih je treba na to opozoriti in jim predlagati alternativne tj. varnejše načine komunikacije (35,36).

5 Primeri dobrih praks upravljanja z varovanjem osebnih podatkov pri projektu *eZdravje*

V Sloveniji se je že izvajalo sorazmerno veliko telemedicinskih projektov, med katerimi jih je nekaj že prešlo v redno uporabo. V nadaljevanju so predstavljene nekatere dobre varnostne prakse projekta *eZdravje*, ki med drugim vključuje tudi nekaj telemedicinskih rešitev (npr. *TeleKap*, *Teleradiologija*, *ePosvet*).

Z vidika informacijske varnosti sta v sklopu projekta *eZdravje* najpomembnejša sistem za upravljanje z informacijsko varnostjo (SUVI) in varno zdravstveno omrežje zNET. SUVI je sistem, ki definira standard ISO/IEC 27001. Gre za nabor organizacijskih postopkov, odločitev in tehničnih ukrepov, ki jih izvaja

eZdravje zaradi varovanja podatkov in informacij. Njegov pomembni del so varnostne politike, ki obravnavajo številna področja varovanja podatkov (npr. fizično zaščito, zaščito pred zlonamerno programsko opremo, varnostno kopiranje, revizijske sledi itd.) in so dostopne na spletnem naslovu http://www.ezdrav.si/category/projekti/suvi/ (37). zNET je zasebno zdravstveno računalniško omrežje, ki ga upravlja Nacionalni inštitut za javno zdravje. Omogoča varne in zanesljive povezave med vstopno točko omrežja, drugimi certificiranimi točkami in ključnimi akterji v zdravstvu. Omogoča dostop do storitev *eZdravja* (38,39). Varnost med drugim zagotavlja z uporabo požarnih pregrad, protivirusne zaščite, šifriranja podatkov, sistema za odkrivanje vdorov in njihovo preprečevanje (*angl.* intrusion detection system/intrusion prevention system, IDS/IPS), z uporabo storitev navideznega zasebnega omrežja (VPN) in infrastrukture za avtentikacijo in avtorizacijo uporabnikov. Zagotovljena je tudi fizična zaščita kritičnih prostorov (pisarn, podatkovnega centra itd.) in izdelava ter primerna hramba arhivskih kopij podatkov. Uporabniki morajo za dostop do storitev *eZdravja* uporabljati primerno kompleksna gesla in kvalificirana potrdila, ki se hranijo na prenosnem mediju (pametni kartici). Neprekinjeno delovanje se zagotavlja s podvojeno opremo in z vzpostavitvijo redundantnih povezav do vseh končnih točk. Varnostne pogoje, ki jim morajo zadostiti uporabniki pred vključitvijo v omrežje zNET, določa Pravilnik o pogojih, rokih, načinu vključitve in uporabe *eZdravja* za obvezne uporabnike (39,40,41).

6 Zaključek

Telemedicinske storitve doživljajo pravi razcvet in so po mnenju mnogih prihodnost zdravstva. Kljub mnogim prednostim pa pri uvedbi ne smemo pozabiti na vzdrževanje standardov za varovanje osebnih podatkov. To se je pokazalo kot resnično pomembno tudi med pandemijo covida-19, ko se je močno povečalo število spletnih napadov na zdravstvene ustanove. Nekatere organizacije so tako poročale o kar štirikratnem povečanju števila napadov, pri čemer je večinoma šlo za pošiljanje zlonamerne elektronske pošte s povezavo na lažne spletne strani (*angl.* phishing) ter za onemogočanje dostopa do podatkov zaradi kriptiranja z zlonamerno programsko kodo (t. i. izsiljevalski virus, *angl.* ransomware) (5,42,43). Nujno je torej treba uvesti ukrepe tako na sistemski kot tudi na individualni ravni, ki bodo varnost zagotavljali v skladu z veljavno zakonodajo. Pri tem je eden najpomembnejših ukrepov zagotoviti redno izobraževanje za vse zaposlene v zdravstvu, ki pri delu uporabljajo osebne podatke. Predstaviti je potrebno nevarnosti ter ukrepe za njihovo preprečevanje in obvladovanje. Samo z motiviranjem in razvijanjem dobre varnostne kulture bo namreč mogoče zagotoviti okolje za uspešno uporabo telemedicine.

Literatura

1. Russell D, Boisvert S, Borg DJ, Burke ME, McCord D, Heathcote S, et al. Telemedicine Risk Management Considerations. Chicago (IL): American Society for Health Care Risk Management; 2018 [cited 2020 Jun 3]. Available from: https://www.ashrm.org/sites/default/files/ashrm/TELEMEDICINE-WHITE-PAPER.pdf.

2. American Telemedicine Association. Telemedicine, Telehealth, and Health Information Technology. Geneva: World health organization; 2006 [cited 2020 Jun 8]. Available from: https://www.who.int/goe/policies/countries/usa_support_tele.pdf?ua=1.
3. Baloh T. Veliko podatkovje in zasebnost v medicini: (magistrsko diplomsko delo). Ljubljana: Pravna fakulteta; 2018.
4. Das S, Mukhopadhyay A. Security and Privacy Challenges in Telemedicine. CSI Commun. 2011;35:20-2.
5. Prelesnik M. Letno poročilo informacijskega pooblaščenca za leto 2019. Ljubljana: Informacijski pooblaščenec Republike Slovenije; 2019 [cited 2020 Aug 26]. Available from: https://www.ip-rs.si/fileadmin/user_upload/Pdf/porocila/LetnoPorocilo2019.pdf/.
6. Prelesnik M. Letno poročilo informacijskega pooblaščenca za leto 2016. Ljubljana: Informacijski pooblaščenec Republike Slovenije; 2016 [cited 2020 Aug 26]. Available from: https://www.ip-rs.si/fileadmin/user_upload/Pdf/porocila/Letno_porocilo_2016_web.pdf.
7. Sporočilo Komisije Evropskemu parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij o koristih telemedicine za paciente, zdravstvene sisteme in družbo. Ljubljana: EUR-Lex; 2008 [cited 2020 May 15]. Available from: https://eur-lex.europa.eu/legal-content/sl/ALL/?uri=CELEX:52008DC0689.
8. Direktiva (EU) 2015/1535 Evropskega parlamenta in Sveta z dne 9. septembra 2015 o določitvi postopka za zbiranje informacij na področju tehničnih predpisov in pravil za storitve informacijske družbe. Ljubljana: EUR-Lex; 2008 [cited 2020 May 15]. Available from: https://eur-lex.europa.eu/legal-content/SL/TXT/?uri=CELEX%3A32015L1535.
9. Zakon o spremembah in dopolnitvah Zakona o zdravstveni dejavnosti. UL RS. 2017(64).
10. Nacionalni odzivni center za kibernetsko varnost. Ljubljana: Si-cert; 2017 [cited 2020 May 15]. Available from: https://www.cert.si/.
11. Lihtenvalner J, Flerin U, Dinevski D. Varnost osebnih podatkov v (tele)medicini. Infor Med Slov. 2014;19(1-2):29-43.
12. Zakon o varstvu osebnih podatkov. UL RS. 2004(94).
13. Ilovar E. Vpliv razvoja tehnologije na zdravstveni sistem v Sloveniji. (Magistrsko delo). Ljubljana: Pravna fakulteta; 2018.
14. Kersnik J, Tušek-Bunc K. Zdravnik kot lastnik in posrednik zdravstvene dokumentacije. Med Razgl. 2007;47(1):155-62.
15. Zakon o informacijski varnosti. UL RS. 2018(30).
16. Pesante L. Introduction to Information Security. Pittsburgh: Carnegie Mellon University; 2008. Available from: https://us-cert.cisa.gov/sites/default/files/publications/infosecuritybasics.pdf.
17. Hudomalj E. Varnost informacij. Lecture presented at: Uvod v medicino - informatika. Ljubljana: Medicinska fakulteta; 2019 [cited 2020 May 15]. Available from: https://pouk.mf.uni-lj.si/mod/resource/view.php?id=19.
18. Zain J, Clarke M. Security in Telemedicine: Issues in Watermarking Medical Images. In: SETIT 2005: 3rd international conference: Sciences of Electronics, Technologies of Information and Telecommunications; 2005 March 27-31; Susa, Tunisia. New Jersey: IEEE; 2005 [cited 2020 May 21]. Available from: https://www.researchgate.net/publication/228576599_Security_in_Telemedicine_Issues_in_Watermarking_Medical_Images.
19. Potokar M. Telemedicina z vidika varstva osebnih podatkov. In: Štrancar Fatur K, Golob P, eds. Telemedicina – Izzivi v urgenci in na čezmejnem območju; 2014 Jun 20. Portorož, Slovenija. Izola: Splošna bolnišnica Izola, projekt InergAid; 2014. pp. 44-52.
20. Smith Y. Types of Telemedicine. S.l.: News Medical Life Sciences; 2005 [cited 2020 May 26]. Available from: https://www.news-medical.net/health/Types-of-Telemedicine.aspx.
21. Schlachta-Fairchild L, Rocca M, Elfrink Cordi V, Haught A, Castelli D, MacMahon K, et al. Telehealth and Applications for Delivering Care at a Distance. In: Nelson R, Staggers N, eds. Health Informatics - E-Book: An Interprofessional Approach. St. Louis: Elsevier Health Sciences; 2014. pp. 125-46.
22. Wainstein L. Cloud-Based Telehealth Defined: Advantages, Applications, and Security. Arizona: University of Arizona Health Sciences; 2018 [cited 2020 May 27]. Available from: https://telemedicine.arizona.edu/blog/cloud-based-telehealth-defined-advantages-applications-and-security.
23. Royal Australian College of General Practitioners. Using email in general pracice. Melbourn: RACGP; 2020 [cited 2020 May 27]. Available from: https://www.racgp.org.au/FSDEDEV/media/documents/Running%20a%20practice/Security/Using-email-in-general-practice-fact-sheet.pdf.
24. Security Metrics Inc. Sending HIPAA Compliant Emails 101. Orem (UT): SM Inc; 2019 [cited 2020 Jun 3]. Available from: https://www.securitymetrics.com/static/resources/orange/HIPAA_Compliant_Emails_White_Paper.pdf.
25. Kreindler DM. Email security in clinical practice: ensuring patient confidentiality. Open Med. 2008;2(2):e54-9. PMID: 21602943

26. Li Y. Thinking of Emailing Medical Records? Think Again. Electronic health reporter. 2014 Dec 2 [cited 2020 Jun 3]. Available from: https://electronichealthreporter.com/thinking-of-emailing-medical-records-think-again/.
27. Hadeed GJ, Holcomb M, Latifi R. Communication Technologies: An Overview of Telemedicine Connectivity. In: Latifi R, ed. Telemedicine for Trauma, Emergencies, and Disaster Management. Norwood (MA): Artech House; 2011. pp. 37-50.
28. Trend Micro Incorporated. How to Secure Video Conferencing Apps. Irving: TMI; 2020 [cited 2020 May 24]. Available from: https://www.trendmicro.com/vinfo/us/security/news/security-technology/how-to-secure-video-conferencing-apps.
29. Winder D. Zoom Gets Stuffed: Here's How Hackers Got Hold Of 500,000 Passwords. Jersey City (NY): Forbes; 2020 [cited 2020 May 24]. Available from: https://www.forbes.com/sites/daveywinder/2020/04/28/zoom-gets-stuffed-heres-how-hackers-got-hold-of-500000-passwords/#7938b2165cdc.
30. Bode K. Zoom Is Full of Security Flaws — But You Can Protect Yourself. San Francisco (CA): Medium; 2020 [cited 2020 May 26]. Available from: https://onezero.medium.com/zoom-is-full-of-security-flaws-but-you-can-protect-yourself-f153f078ecbf.
31. National Security Agency (US). Selecting and Safely Using Collaboration Services for Telework. Fort Meade (MD): NSA (US); 2020 [cited 2020 May 26]. Available from: https://www.nsa.gov/News-Features/News-Stories/Article-View/Article/2163484/working-from-home-select-and-use-collaboration-services-more-securely/.
32. Cimpanu C. NSA security guide: How to choose safe conferencing and collaboration tools. San Francisco (CA): CBS Interactive; 2020 [cited 2020 May 26]. Available from: https://www.zdnet.com/article/heres-the-nsas-guide-for-choosing-a-safe-text-chat-and-video-conferencing-service/.
33. Partala J, Keranen N, Sarestoniemi M, Hamalainen M, Iinatti J, Jamsa T, et al. Security threats against the transmission chain of a medical health monitoring system. In: 2013 IEEE 15th International Conference on e-Health Networking, Applications and Services; 2013 Oct 9-12. Lisbon, Portugal. New Jersey: Institute of Electrical and Electronics Engineers; 2013 [cited 2020 May 26]. Available from: https://ieeexplore.ieee.org/document/6720675?arnumber=6720675&tag=1. DOI: 10.1109/HealthCom.2013.6720675.
34. Ondiege B, Clarke M, Mapp G. Exploring a New Security Framework for Remote Patient Monitoring Devices. Computers. 2017;6(1):11. DOI: 10.3390/computers6010011
35. Evropski ekonomsko-socialni odbor. Mnenje Evropskega ekonomsko-socialnega odbora o Sporočilu Komisije Evropskemu parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij o koristih telemedicine za paciente, zdravstvene sisteme in družbo (COM(2008) 689 konč.). Brussels: EUR-Lex; 2020 [cited 2020 May 22]. Available from: https://eur-lex.europa.eu/legal-content/SL/TXT/?uri=CELEX%3A52009AE1197.
36. Miliard M. Telehealth privacy and security: Investment and education are key, attorney says. Portland (OR): Healthcare IT News; 2020 [cited 2020 May 25]. Available from: https://www.healthcareitnews.com/news/telehealth-privacy-and-security-investment-and-education-are-key-attorney-say.
37. SUVI. Ljubljana: Ministrstvo za zdravje; 2019 [cited 2020 Aug 28]. Available from: http://www.ezdrav.si/category/projekti/suvi/.
38. zNET. Ljubljana: Ministrstvo za zdravje; 2019 [cited 2020 Aug 28]. Available from: http://www.ezdrav.si/category/projekti/znet/.
39. Pravilnik o pogojih, rokih, načinu vključitve in uporabe eZdravja za obvezne uporabnike. UL RS. 2015(69).
40. Drnovšek S, Bucaj Ž, Šinkovec M, Ladinik J, Černe M, Breznik K, et al. Študija izvedljivosti projekta eZdravje – predinvesticijska zasnova in investicijski program s študijo izvedbe: Definicije podprojektov. Ljubljana: Ministrstvo za zdravje; 2019 [cited 2020 Aug 29]. Available from: http://mz.arhiv-spletisc.gov.si/fileadmin/mz.gov.si/pageuploads/eZdravje/predstavitev/studija/definicija_projektov.pdf.
41. Žele M. Predstavitev varnostnih politik [PowerPoint slides]. Lecture presented at: Informativni dan informacijske varnosti; Jun 2010. Ljubljana: Medicinska fakulteta; 2010 [cited 2020 Aug 29]. Available from: http://mz.arhiv-spletisc.gov.si/fileadmin/mz.gov.si/pageuploads/eZdravje/predstavitev/Predstavitev_politik.pdf.
42. Keown A. Cyberattacks on Health Care Groups Increase During COVID-19 Pandemic. Urbandale: Biospace; c1985-2020 [cited 2020 Jun 22]. Available from: https://www.biospace.com/article/pandemic-creates-opportunities-for-cyberattacks-on-healthcare-groups-report-shows/.
43. European Union Agency for Cybersecurity. Cybersecurity in the healthcare sector during COVID-19 pandemic. Athens: The Agency; c2005-2020 [cited 2020 Jun 22]. Available from: https://www.enisa.europa.eu/news/enisa-news/cybersecurity-in-the-healthcare-sector-during-covid-19-pandemic.