ARTSS: Perspektīvās tehnoloģijas noturīgiem un drošiem servisiem

VPP-COVID-2020/1-0009

Izvērtējums par attālināto veselības aprūpes pakalpojumiem un to ietekmējošajiem faktoriem

Rekomendācijas normatīvo aktu grozījumiem veselības aprūpes pakalpojumu kvalitātes vadībai

Autori: Ginta Majore, Iveta Reinholde, Juris Binde, Egons Bušs, Ilze Auliciema, Malvīne Stučka, Viesturs Bambāns, Mārtiņš Švirksts

Versija, datums: 2021.gada 10.marts, 6.versija

Satura rādītājs

Kopsavilkums

Projekta „ARTSS: Perspektīvās tehnoloģijas noturīgiem un drošiem servisiem” (VPP-COVID-2020/1-0009) (turpmāk tekstā – Projekts) mērķis ir izstrādāt metodi un tehnoloģiskos risinājumus digitālo pakalpojumu dinamiskai pielāgošanai un drošības nodrošināšanai COVID-19 gadījumā un līdzīgās krīzes situācijās. Izvērtējuma mērķis ir analizēt attālināto veselības aprūpes pakalpojumu sniegšanas drošības ietekmējošiem faktoriem un sniegt rekomendācijas.

Rekomendāciju pamatā ir Projektā izstrādātā ARTSS metode, kā arī secinājumi no literatūras analīzes (IKT izmantošanas tendences krīzes situācijās, risku pārvaldības modeļi u.c.). Metode paredz strukturētu pakalpojuma mērķu, izpildes rādītāju, konteksta (jeb izpildes vides mērījumu) un drošības un noturības pielāgojumu attēlošanu un izmantošanu servisa konfigurēšanā tā izstrādes un izpildes laikā. Tādējādi, izvērtējums par attālināto veselības aprūpes pakalpojumiem un to ietekmējošajiem faktoriem, t.sk. drošumu, potenciālo un reālo efektivitāti, izmaksu lietderību, pieejamību balstās ARTSS metodē.

Izvērtējuma laikā secināts, ka drošības un noturības prasības telemedicīnā primāri izriet no pielietotās IKT drošības un noturības, jo attālinātie medicīnas pakalpojumi tiek sniegti IKT vidē.

Termini un saīsinājumi

Termins	Skaidrojums
AI *Artificial inteligence*	Mākslīgais intelekts
ARTSS metode	Metode paredz strukturētu pakalpojuma mērķu, izpildes rādītāju, konteksta (jeb izpildes vides mērījumu), kā arī drošības un noturības pielāgojumu attēlošanu un izmantošanu servisa konfigurēšanā tā izstrādes un izpildes laikā. Metode ir komponentorientēta, kas nozīmē, ka specifisku projektēšanas un piegādes uzdevumu risināšanai tiek izstrādātas atsevišķas komponentes, kuras vieno vienota konceptuālā bāze.
Digitalizācija	Digitālo tehnoloģiju izmantošana jaunu produktu, pakalpojumu un pievienotās vērtības radīšanai
Digitālais briedums	Mērījums organizācijas digitālo spēju mērīšanai
Digitālais dvīnis *Digital twin*	Reālā servisa nodrošināšanas tīkla attēlojums virtuālajā videi kontrolei un analīzei
Drošības aspekts	Mērķa specializācija, kas attēlo drošības mērķus
Ekosistēma *Ecosystem*	Visu drošu un noturīgu servisu nodrošināšanu ietekmējamo iesaistīto pušu kopums
GDPR *European General Data Protection Regulation*	Vispārīgā datu aizsardzības regula Eiropas Parlamenta un Padomes Regula (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti
HIPAA *Health Insurance Portability and Accountability Act*	Vadlīnijas ASV standartizētai elektronisko veselības datu un pakalpojumu drošībai atbildībai
IKT	Informācijas un komunikāciju tehnoloģijas
ISP *Interner Service Provider*	Interneta pakalpojumu nodrošinātājs
Mācīšanās modulis	Nodrošina apmācību par servisa drošu izmantošanu

Termins	**Skaidrojums**
Pielāgojums *Adjustment*	Algoritmiska rekomendācija spējas pielāgošanai atbilstoši konteksta situācijai
Serviss	Komponente, kas, nodrošina noteiktu funkcionalitāti atbildot uz partnera pieprasījumu
Spēja *Capability*	Varēšana un kapacitāte sasniegt organizācijas mērķus mainīgos kontekstuālos apstākļos
Tīkls	Servisa nodrošinātāju kopums
Termins	**Skaidrojums**

1 Ievads, dokumenta mērķis un izvērtējuma algoritms

Šīs dokuments ietver:

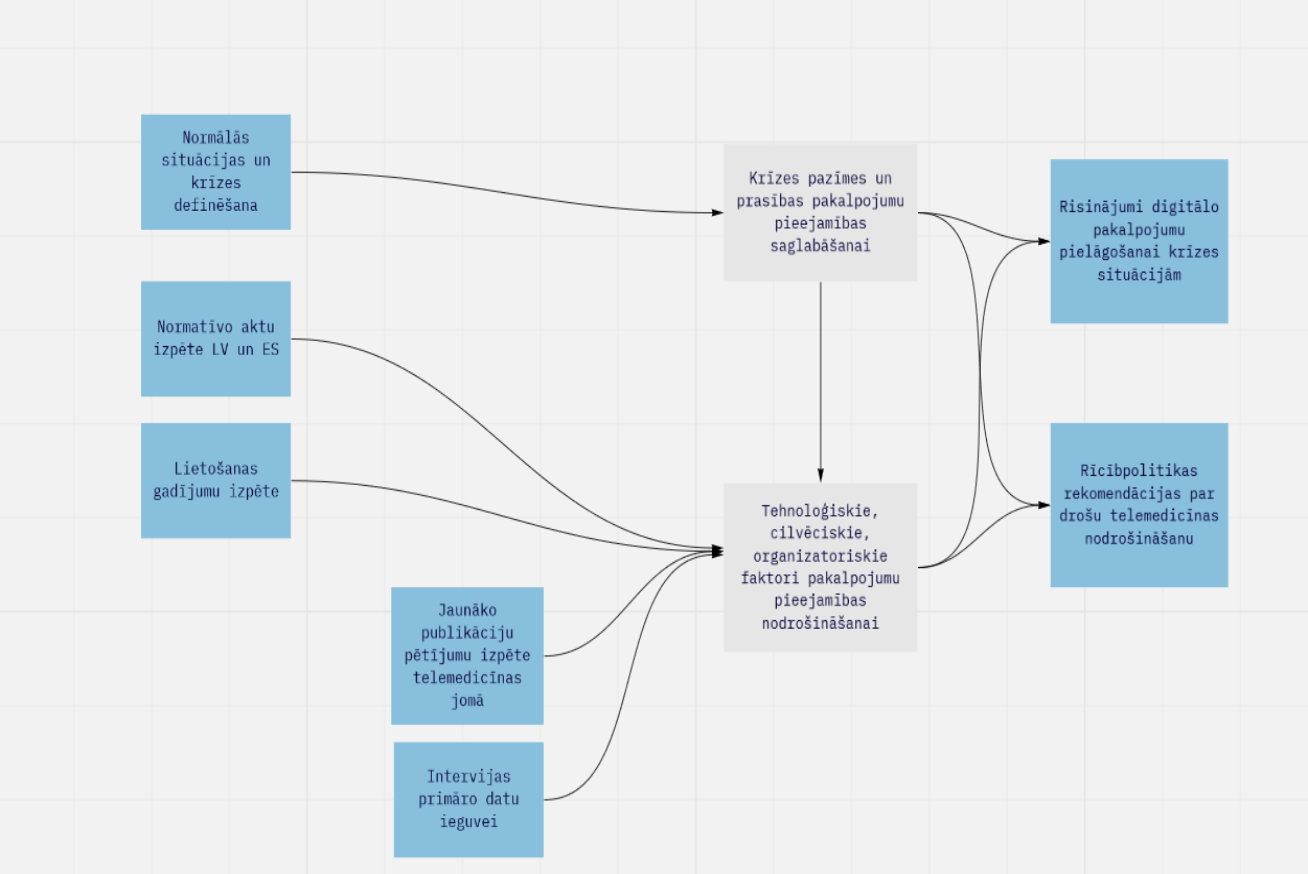
a) *Izvērtējumu par attālināto veselības aprūpes pakalpojumiem un to ietekmējošajiem faktoriem;*

b) *Rekomendācijas normatīvo aktu grozījumiem veselības aprūpes pakalpojumu kvalitātes vadībai.*

Gan izvērtējums, gan rekomendācijas ir sagatavotas VVP projektā "ARTSS: Perspektīvās tehnoloģijas noturīgiem un drošiem servisiem. VPP-COVID-2020/1-0009" kā projektā sasniedzamie papildus rezultāti, kas atbilst Ministru kabineta rīkojuma "*6.8.1. punktu optimālajām attālināto pakalpojumu nodrošināšanas pieejām galvenajās tautsaimniecības nozarēs, kiberdrošībai, lielajiem datiem, kā arī informācijas un komunikācijas tehnoloģiju izmantošanai uzņēmējdarbībā krīzes apstākļos, un sniegt konkrētas rekomendācijas par valsts apmaksāto telemedicīnas pakalpojumu attīstīšanu, optimālām jauna formāta digitalizētām darba vietām, par jaunām individuālā un kolektīvā darba pieejām, sabiedriskā sektora darbu digitālajā formātā, kā arī izstrādāt attālināto pakalpojumu sniegšanas standartus vai pilnveidot esošos standartus pakalpojumu kvalitātes un drošības nodrošināšanai*".

Projekta mērķis ir izstrādāt metodi un tehnoloģiskos risinājumus digitālo pakalpojumu dinamiskai pielāgošanai un drošības nodrošināšanai COVID-19 gadījumā un līdzīgās krīzes situācijās. Izvērtējuma mērķis ir analizēt attālināto veselības aprūpes pakalpojumu sniegšanas drošības ietekmējošiem faktoriem. Izvērtējuma mērķa sasniegšanai tika izmantota vairāku kvantitatīvo metožu kombinācija (intervijas ar nozares ekspertiem, padziļinātās intervijas ar 10 (desmit) ģimenes ārstiem, ģimenes ārstu līdzdalība pakalpojumu modelēšanas sesijās, dokumentu izpēte), lai aptvertu visu pētāmās problēmas apgabalu un iegūtu pēc iespējas lielāku pētījuma rezultātu ticamību.

Rekomendāciju pamatā ir Projektā izstrādātā ARTSS metode, kā arī secinājumi no literatūras analīzes (IKT izmantošanas tendences krīzes situācijās, risku pārvaldības modeļi u.c.). Metode paredz strukturētu pakalpojuma mērķu, izpildes rādītāju, konteksta (jeb izpildes vides mērījumu) un drošības un noturības pielāgojumu attēlošanu (1. attēls).



1.attēls. Izvērtējuma norises algoritms.

Izvērtējums secīgi tika organizēts šādos posmos trīs posmos (1. tabula)

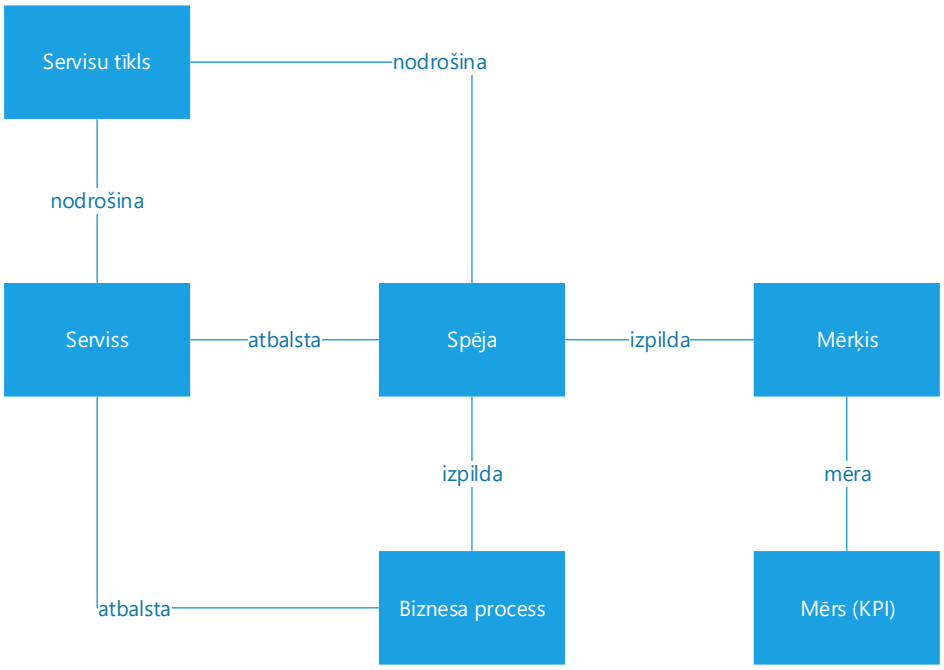
1. tabula. Izvērtējuma norises posmi.

1.posms	Tika veikta normālās situācijas un krīzes definēšana, lai izprastu ar ārkārtas situāciju Latvijā saistītos izaicinājumus. Šajā posmā tika veikta arī normatīvo aktu un politikas plānošanas dokumentu izpēte, kas sniedz būtisku informāciju lietošanas gadījumiem (*use case*).
2.posms	Tika organizētas intervijas ar veselības jomas profesionāļiem. Izvērtējuma laikā tika veiktas šādas ekspertu intervijas: ● Dr. Iliārs Freimanis, ģimenes ārsts; ● Sabīne Keiša, SIA "KIRSH veselības fabrika" īpašniece, menedžere; ● Santa Batuhtina-Banga, telemedicīnas entuziaste; ● Dr. Ņina Gailīte, ģimenes ārste; ● Baiba Kaškina, CERT.LV

	● Edgars Goba, Nacionālais veselības dienests. Papildus, tika veikta padziļinātās strukturētās intervijas ar 10 ģimenes ārstiem, kuri atsaucās pētnieku aicinājumam. Tieši ģimenes ārstu palielinātā slodze bija iemesls, kāpēc tika veiktas padziļinātas strukturētas intervijas, lai iegūtu informāciju par tendencēm nozarē, jo aptaujā netiktu sasniegts reprezentatīvs respondentu skaits. Izmantojot ARTSS metodi tika veikta klātienes modelēšanas sesijas, ar mērķi apzināt specifiskas prasības drošiem un noturīgiem telemedicīnas servisiem ģimenes ārstu privātpraksēs. ARTSS metodes detalizēts apraksts ir publiski pieejams projekta mājas lapā (skat. saiti). ARTSS metodoloģijas semināros piedalījās un rezultātu novērtēja ģimenes ārstu prakšu pārstāvis Dr.Ilārs Freimanis un Dr.Ņina Gailīte. Semināru būtība un mērķis bija strukturēta telemedicīnas pakalpojumu analīze no ģimenes ārstu skatpunkta, konteksta un nepieciešamo pielāgojumu identificēšana un strukturēšana. Turpmāk 7.nodaļā ir detalizēti atspoguļots ARTSS modelis.
3.posms	Tika formulētas rekomendācijas pakalpojumu pielāgošanai un rīcībpolitikas pilnveidošanai.

Organizācijas (t.i., telemedicīnas sniedzēja) līmenis ar tehnoloģiju līmeni tiek sasaistīts, izmantojot spēju modeļus. ARTSS metodes pamatā, kas tika izmantota šajā projektā, ir servisu spēju (*capabilities*) virzīta izstrādes metodoloģija (2. attēls).

Saskaņā ar ARTSS metodi, servisus nodrošina savstarpēji saistītu servisu sniedzēju tīkls. Spēja determinē servisu tīkla un tā dalībnieku varēšanu un kapacitāti nodrošināt servisa noturību un drošību. Servisu tīklam ir vienoti mērķi, un tas apmainās ar kontekstuālo informāciju un zināšanām savstarpējās uzticēšanās ietvaros. Citiem vārdiem, sakot, vienā tīklā esošās ieinteresētās puses apmainās ar savā rīcībā esošo informāciju. Lai nodrošinātu drošus un noturīgus servisus, servisu tīklam ir jāpiemīt atbilstošām drošības un noturības spējām. Savukārt, servisu nodrošinātāji veido drošu un noturīgu servisu ekosistēmu, kurā notiek pakāpeniska savstarpēji bagātinoša spēju attīstīšana, balstoties uz uzkrātajām zināšanām.



2.attēls. ARTSS metodes konceptu modeļa fragments

Turklāt, ARTSS metodes aptver šādus aspektus:

- Organizāciju ekosistēmas modelēšana, lai identificētu dažādus dalībniekus un viņu ieguldījumu pakalpojuma sniegšanā.
- Spēju pārvaldība, lai izstrādātu no konteksta atkarīgu pakalpojumu pielāgošanu un pārvaldību.
- Digitālie dvīņi, lai nodrošinātu, ka korekcijas (lēmumi un darbības) tiek izmantotas pakalpojuma sniegšanā, tostarp pakalpojumu ekosistēmas uzlabošanā;
- Liela apjoma kontekstuālo datu (reālā laika, kā arī vēsturiskā) apstrāde un pārvaldība;
- Atkārtoti izmantojamu krīzes reaģēšanas zināšanu uzkrāšana;

Rīcībpolitikas kontekstā, pakalpojumu un pakalpojuma tīkla attīstību nosaka spēja (*capability*), kuru ir iespējams modelēt un veidot no konteksta atkarīgus un kontekstam pielāgoties spējīgus telemedicīnas pakalpojumus. ARTSS metode neietver finanšu analīzi, un tādēļ, šajā ziņojumā nav veikti aprēķini nepieciešamajam investīciju apjomam telemedicīnas nozarē.

2 Telemedicīnas definējums un ietvars

Populāra izpratne par telemedicīnu ir tāda, ka telemedicīna ir veselības aprūpes pakalpojumu sniegšana, kur tradicionālā pacienta un ārsta mijiedarbība klātienē tiek aizstāta ar distancētu mijiedarbību, izmantojot informācijas un komunikāciju tehnoloģijas.

Tomēr šajā jomā ir virkne terminu, kas tiek lietoti un uztverti atšķirīgi gan no sabiedrības puses, gan no nozares profesionāļu puses. Pētnieks Donalds Šovs[1] (*Donald Shaw*) 2009.gadā definēja *telemedicīnu kā telekomunikāciju pielietošanu medicīniskiem diagnostikas, uzraudzības un terapeitiskiem mērķiem, kad attālums šķir lietotājus*.

Pasaules Veselības organizācija (PVO) 2016.gadā definēja, ka *televeselība*[2] *(telehealth) ir veselības aprūpes pakalpojumu sniegšana, kad attālums ir nozīmīgs faktors starp veselības aprūpes sniedzēju un pacientu, veselības aprūpes speciālistiem, izmantojot informācijas un komunikāciju tehnoloģijas diagnostikai, ārstēšanai un profilaksei, pētniecībai un novērtēšanai, kā arī veselības aprūpes pakalpojumu sniedzēju tālākizglītībai, lai veicinātu indivīdu veselību*.

Cita PVO izmantotā definīcija nosaka, ka televeselība (*telehealth*)[3] – *telekomunikāciju un virtuālo tehnoloģiju izmantošana, lai sniegtu veselības aprūpes pakalpojumus ārpus tradicionālajām veselības aprūpes iestādēm (piem., virtuālā aprūpe mājās).*

Amerikas Ģimenes ārstu akadēmija (*American Academy of Family Physicians)* norāda, ka "*televeselība ir plašāks un aptverošāks jēdziens kā telemedicīna, jo telemedicīna attiecas uz attālinātiem klīniskiem pakalpojumiem, kamēr televeselība var tikt attiecināta arī uz neklīniskiem pakalpojumiem*"[4].

Amerikas Ģimenes ārstu asociācijas piedāvātās definīcijas ir:

- *Televeselība (telehealth) ir plaša informācijas un komunikāciju tehnoloģiju izmantošana, kas nodrošina veselības aprūpi un tās pakalpojumus attālināti. Televeselība ietver tehnoloģijas un virtuālās medicīnas, veselības un izglītības pakalpojumus un cita veida informācijas apmaiņu, lai nodrošinātu efektīvu novērtēšanas, diagnostikas, konsultāciju, ārstniecības, izglītības un aprūpes pārvaldību*[5].
- *Telemedicīna – attālināta medicīnas prakse, izmantojot informāciju komunikācijas tehnoloģijas, kur pacients atrodas vienā vietā, bet ārstniecības persona attālināti, citā vietā.*

---

[1] Shaw, D. K., (2009). *Overview of Telehealth and Its Application to Cardiopulmonary Physical Therapy*. Cardiopulmonary Physical Therapy Journal, 20(2), 13-18

[2] *Telehealth.* Izgūts no https://www.who.int/gho/goe/telehealth/en/, skatīts 21.09.2020.

[3] *Telehealth.* Izgūts no http://www.who.int/sustainable-development/health-sector/strategies/telehealth/en/, skatīts 20.09.2020.

[4] AAFP (2019). *Telemedicine.* Izgūts no https://www.aafp.org/news/media-center/kits/telemedicine-and-telehealth.html un https://www.aafp.org/dam/AAFP/documents/advocacy/health_it/telehealth/BKG-Telemedicine.pdf , skatīts 19.09.2020.

[5] *Telehealth and Telemedicine*. Izgūts no https://www.aafp.org/about/policies/all/telehealth-telemedicine.html , skatīts 18.09.2020.

Visbeidzot, šajā jomā tiek lietoti arī šādi termini:

- e-Veselība *(eHealth)*[6] – informācijas un komunikāciju tehnoloģiju izmantošana veselības aprūpei un sabiedrības veselībai;
- mVeselība (*mHealth*)[7] – mobilo tehnoloģiju izmantošana veselības aprūpei un sabiedrības veselībai;
- digitālā veselība (*digital health*) – drošā veidā elektroniski sasaistīti dažādi veselības pakalpojumu sniegšanas punkti vai vietas[8];
- elektronisks veselības ieraksts (Electronic health record (EHR)) – informācija, ieraksts par pacienta veselības stāvokli (pacienta elektroniskā karte) jebkurā veselības aprūpes iestādē vai datu bāzē.

ASV Pārtikas un zāļu administrācija (*US Food and Drug Administration*)[9] skaidro, ka digitālā veselība iekļauj tādas kategorijas kā mVeselību, veselības informācijas tehnoloģijas, valkājamās ierīces, televeselību, telemedicīnu un personalizēto medicīnu. Respektīvi, digitālā veselība ir visplašākais jēdziens, lai raksturotu IKT (informācijas un komunikācijas tehnoloģijas) daudzveidīgo izmantošanu veselības jomā.

[6] *eHealth at WHO*. Izgūts no http://www.who.int/ehealth/about/en/, skatīts 15.09.2020.

[7] Turpat.

[8] Australian government. *Australian Digital Health agency*. Izgūts no https://www.digitalhealth.gov.au/get-started-with-digital-health/what-is-digital-health, skatīts 10.09.2020.

[9] US Food and Drug Administration. *Digital Health*. Izgūts no https://www.fda.gov/medical-devices/digital-health-center-excellence/what-digital-health , skatīts 22.09.2020.

3 Esošā situācija rīcībpolitika jomā

3.1 Ārkārtas situācijas regulējums Latvijā

Ārkārtas situācijas izsludināšana 2020.gada 12.martā ienesa būtiskas izmaiņas sabiedrības dzīvē kopumā, t.sk. noteica virkni ierobežojumu, kas sekojoši radīja virkni izaicinājumu publiskās pārvaldes institūcijām, uzņēmējiem un ikvienam indivīdam.

Ministru kabinets rīkojumu Nr.103 "Par ārkārtas situācijas izsludināšanu" izdeva atsaucoties uz Pasaules veselības organizācijas 2020.gada 11.marta paziņojumu, ka Covid-19 ir sasniegusi pandēmijas apmērus un pamatojoties uz Civilās aizsardzības un katastrofu pārvaldīšanas likuma 4.panta pirmās daļas 1. punkta "e" apakšpunktu, likuma "Par ārkārtējo situāciju un izņēmuma stāvokli" 5.panta pirmo daļu un 6.panta pirmās daļas 1. punktu un otro daļu, 7. panta 1. punktu un 8. pantu un Epidemioloģiskās drošības likuma 3. panta otro daļu.[10]

Civilās aizsardzības un katastrofu pārvaldīšanas likuma (turpmāk – CAKPL) 4.pants nosaka katastrofu veidus un mērogus. Atbilstoši šī panta pirmās daļas 1. punkta "e" apakšpunktam Covid-19 pandēmija ir klasificēta kā bioloģiskā katastrofa.

CAKPL 1.panta 2.punkts definē katastrofu kā notikumu, kas izraisījis cilvēku upurus un apdraud cilvēku dzīvību vai veselību, nodarījis kaitējumu vai radījis apdraudējumu cilvēkiem, videi vai īpašumam, kā arī radījis vai rada būtiskus materiālos un finansiālos zaudējumus un pārsniedz atbildīgo valsts un pašvaldības institūciju ikdienas spējas novērst notikuma postošos apstākļus. CAKPL 1.panta 3.punkts definē katastrofas draudus kā situāciju, kad risku novērtējums, prognozes, informācija vai citi apstākļi pamatoti liecina par katastrofas iespējamību.[11] Likuma "Par ārkārtējo situāciju un izņēmuma stāvokli" (turpmāk tekstā – LĀSIS) 4.pants definē ārkārtēju situāciju kā īpašu tiesisko režīms, kura laikā Ministru kabinetam ir tiesības likumā noteiktā kārtībā un apjomā ierobežot valsts pārvaldes un pašvaldību institūciju, fizisko un juridisko personu tiesības un brīvības, kā arī uzlikt tām papildu pienākumus. Katastrofa un tās draudi, ja būtiski apdraudēta valsts, sabiedrības, vides, saimnieciskās darbības drošība vai cilvēku dzīvība var būt pamats ārkārtas situācijas izsludināšanai.[12]

Papildus, Epidemioloģiskās drošības likuma (turpmāk – EDL) 3. panta otrā daļa piešķir Ministru kabinetam tiesības noteikt epidemioloģiskās drošības pasākumus atsevišķu infekcijas slimību izplatības ierobežošanai. Epidemioloģiskā drošība EDL izpratnē ietver:

1. pasākumus veselīgas vides nodrošināšanai;
2. infekcijas slimību epidemioloģisko uzraudzību, tajā skaitā:

a) infekcijas slimību reģistrāciju, uzskaiti un saslimstības analīzi,

[10] Ministru kabinets. (pieņemts 12.03.2020) *Ministru kabineta noteikumi Nr. 103* "*Par ārkārtējās situācijas izsludināšanu"*. Izgūts no https://likumi.lv/ta/id/313191-par-arkartejas-situacijas-izsludinasanu, skatīts 21.09.2020.

[11] Saeima. (pieņemts 05.05.2016) *Civilās aizsardzības un katastrofas pārvaldīšanas likums.* Izgūts no https://likumi.lv/ta/id/282333-civilas-aizsardzibas-un-katastrofas-parvaldisanas-likums, skatīts 21.09.2020.

[12] Saeima. (pieņemts 07.03.2013) *Par ārkārtējo situāciju un izņēmuma stāvokli.* Izgūts no https://likumi.lv/ta/id/255713-par-arkartejo-situaciju-un-iznemuma-stavokli, skatīts 21.09.2020.

b) cilvēku, dzīvnieku un vides materiālu laboratoriskās pārbaudes infekcijas slimību izraisītāju cirkulācijas novērošanai,

c) iedzīvotāju imunitātes izpēti.

3. nodrošināšanu ar imūnbioloģiskiem preparātiem un iedzīvotāju vakcināciju;
4. slimnieku un infekciozo personu atklāšanu, uzskaiti, ārstēšanu un, ja nepieciešams, izolēšanu;
5. kontaktpersonu noteikšanu, uzskaiti, laboratoriskās pārbaudes un medicīnisko novērošanu;
6. īpašu piesardzības un ierobežošanas pasākumu noteikšanu, tajā skaitā profesionālās darbības un piedalīšanās mācību procesā ierobežošanu un aizliegšanu, slimniekiem, infekciozajām personām, kontaktpersonām un personām, par kurām ir radušās epidemioloģiski pamatotas aizdomas, ka tās ir atradušās paaugstināta inficēšanās riska apstākļos;
7. infekcijas slimību perēkļu atveseļošanas pasākumus, kā arī pasākumus infekcijas slimību izraisītāju cirkulācijas pārtraukšanai ārējā vidē;
8. sabiedrības veselības aizsardzības pasākumus;
9. iedzīvotāju informēšanu par epidemioloģisko situāciju un izglītošanu infekcijas slimību profilakses jautājumos;
10. likumā noteikto piespiedu līdzekļu piemērošanu par epidemioloģiskās drošības pasākumu nepildīšanu.[13]

LĀSIS 5.panta 1.daļa nosaka, ka Ārkārtas situāciju Ministru kabinets var izsludināt uz laiku ne ilgāku par trīs mēnešiem.

Laiks no 2020.gada 12. martam, kad tika izsludināta krīzes situācija, līdz 2020. gada 10.jūnijam, kad stājās spēkā likums "Epidemioloģiskās drošības pasākumi Covid-19 infekcijas izplatības ierobežošanai" uzskatāmi iezīmē pārejas posmu, kas iezīmē būtiskas izmaiņas sabiedrībā kopumā, t.sk. sabiedrības attieksmē un rīcībpolitikās, kas attiecas uz telemedicīnu.

3.attēls. Analizējamie periodi un atskaites punkti

Ministru kabineta 12.03.2020.rīkojums Nr.103. (turpmāk Rīkojums Nr.103) „Par ārkārtējās situācijas izsludināšanu" paredzēja virkni ierobežojumu epidemioloģiskās drošības nodrošināšanai, kas būtiski ietekmēja uzņēmējdarbību. Tomēr ārkārtas situācija uzlika papildus slogu veselības sistēmai, jo bija jānodrošina tāds pakalpojumu apjoms, lai nepasliktinātos iedzīvotāju veselības stāvoklis. Tādējādi, kā risinājums tika plašāk izmantoti telemedicīnas

[13] Saeima. (pieņemts 11.12.1997) *Epidemioloģiskās drošības likums.* Izgūts no https://likumi.lv/ta/id/52951-epidemiologiskas-drosibas-likums, skatīts 21.09.2020.

pakalpojumi, izmantojot IKT risinājumus, kuru drošība un noturība variē atkarībā no izmantotās IKT tehnoloģijas. Tādējādi, "normalitātes apstākļos" pirms ārkārtējas situācijas telemedicīnas pakalpojumu attīstība notiek bez īpašām regulējošām prasībām pakalpojumiem, reaģējot uz sabiedrības pieprasījumu un tehnoloģisko progresu. Savukārt, ārkārtas situācijā pieaug sabiedrības pieprasījums pēc telemedicīnas pakalpojumiem ierobežojumu dēļ. Vienlaikus, gan pacientiem, gan ārstniecības personālam ir jāpārvar gan tehnoloģiskie šķēršļi (piem., kā risināt drošu saziņu), gan arī organizatoriskie šķēršļi (piem., kā organizēt pacientu pierakstu telemedicīnas konsultācijām) un finansiālie aspekti (piem., telemedicīnas pakalpojumu apmaksa). Attiecīgi, atkopšanas periods, kas ietver arī gatavošanos iespējamām citām krīzēm – ietver nepieciešamību definēt telemedicīnas pakalpojumu prasības rīcībpolitikas līmenī, kas nākotnē ietekmēs telemedicīnas pakalpojumu kvalitāti un investīcijas šajā jomā. Tādēļ, rekomendāciju ziņojums piedāvā ieteikumus dažādu telemedicīnas šķēršļu pārvarēšanai.

3.2 Normatīvais un rīcībpolitikas ietvars

3.2.1 Starptautiskā līmenī

2018.gadā PVO pieņēma **rezolūciju[14] par digitālo veselību** (*digital health*) aicinot valstis pievērst uzmanību vairākiem aspektiem, t.sk.:

- Jānovērtē digitālo tehnoloģiju izmantošana veselības politikas jomā, iekļaujot veselības informācijas sistēmas, lai identificētu potenciālos uzlabojumus un noteiktu prioritārās jomas digitālo tehnoloģiju plašākai izmantošanai, lai veicinātu veselības aprūpes pieejamību.
- Jānovērtē, kā digitālās tehnoloģijas varētu tikt integrētas esošā veselības aprūpes sistēmas infrastruktūrā, lai nodrošinātu uz cilvēku-centrētu veselības aprūpi un samazinātu veselības sistēmas noslodzi.
- Optimizēt un koordinēt resursus reformas un attīstību veselības aprūpes jomā, paredzot digitālo tehnoloģiju izmantošanu;
- Identificējot jomas, kurās prioritāri ir nepieciešams normatīvais regulējums un tehniskais atbalsts digitālo veselības rīku izmantošanai, balstoties uz pierādījumiem, lietderības un ilgtspējas apsvērumiem.
- Jāstrādā, lai nodrošinātu tehnoloģiju savietojamību un spēju sadarboties (angl. *interoperability*);
- Dalīties ar labo praksi un pieredzi digitālās veselības aprūpes sistēmas veidošanā ar citām valstīm un kopienām;
- Stiprināt sabiedrības veselības spēju atjaunoties (angl. *resilience*), veicinot digitālo tehnoloģiju pieejamību un lietošanu arī krīzes situācijās;
- Stiprināt cilvēkresursu digitālās veselības politikas attīstībai, iesaistot gan veselības jomu, gan arī IT jomu.
- Uzlabot iedzīvotāju digitālās prasmes, palielinot sabiedrības uzticēšanos un atbalstu digitālās veselības risinājumu izmantošanai;

[14] Seventy first world health assembly. (26.05.2018.) Agenda item 12.4 *Digital health*. Izgūts no https://apps.who.int/gb/ebwha/pdf_files/WHA71/A71_R7-en.pdf?ua=1, skatīts 30.09.2020.

- Attīstīt un pilnveidot normatīvo bāzi un datu aizsardzību, pievēršot uzmanību tādiem aspektiem kā pieejamība datiem, datu koplietošana, pacienta piekrišana, drošība, privātums, savietojamība un iekļaušana;
- Attīstīt, kur iespējams, partnerību ar citām ieinteresētajam pusēm digitālās veselības veicināšanā.

PVO izstrādāta "Stratēģija digitālajai veselībai 2020-2025.gadam"[15] ietver redzējumu par veselības uzlabošanu ikvienam cilvēkam, veicinot atbilstošu, pieejamu, ilgtspējīgu un uz personas vajadzībām fokusēto digitālo veselības un aprūpes risinājumu izstrādi un ieviešanu, un sasniegtu ar veselību saistītu ilgtspējīgas attīstības veicināšanas mērķi.

Konkrēti, stratēģijas balstās šādiem pamatprincipiem:

- Digitālās veselības institucionalizācija nacionālajā veselības aprūpes sistēmā;
- Digitālās veselības iniciatīvas ir jāuzlūko un jāattīsta kā integrēta stratēģija.;
- Digitālo veselības aprūpes tehnoloģiju lietošanas veicināšana.

2011.gada 28.februārī Eiropas Savienības Padome apstiprināja, un ES dalībvalstis pārņēma līdz 2013.gada 25.oktobrim Eiropas Parlamenta un Padomes direktīvu 2011/24/ES par pacientu tiesību piemērošanu pārrobežu veselības aprūpē. Direktīvas mērķis ir uzlabot piekļuvi drošai un kvalitatīvai pārrobežu veselības aprūpei un veicināt dalībvalstu sadarbību veselības aprūpes jomā, pilnībā ievērojot valstu kompetenci veselības aprūpes organizēšanā un sniegšanā, un tā attiecas uz pacientiem sniegtu veselības aprūpi neatkarīgi no veida, kā tā ir organizēta, sniegta vai finansēta. Lai nodrošinātu precīzu Eiropas Savienības (ES) direktīvas par pacientu tiesību piemērošanu pārrobežu veselības aprūpē piemērošanu Latvijā, Saeima definējusi terminu telemedicīna, veicot grozījumus "Ārstniecības likumā" 2014.gadā.

Papildus, telemedicīnas jomā svarīgas ir arī Eiropas Parlamenta un Padomes Regula (EK) Nr. 883/2004 (2004.gada 29.aprīlis) par sociālās nodrošināšanas sistēmu koordinēšanu[16] un Eiropas Parlamenta un Padomes Regula (EK) Nr. 987/2009 (2009.gada 16.septembris), ar ko nosaka īstenošanas kārtību Regulai (EK) Nr. 883/2004 par sociālās nodrošināšanas sistēmu koordinēšanu.

---

[15] *Draft global strategy on digital health 2020–2025.* Izgūts no https://www.who.int/docs/default-source/documents/gs4dhdaa2a9f352b0445bafbc79ca799dce4d.pdf?sfvrsn=f112ede5_58, skatīts 30.09.2020.

[16] European Commission. *Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare.* Izgūts no https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:088:0045:0065:EN:PDF un http://www.vm.gov.lv/images/userfiles/phoebe/eiropas_savieniba_aktualitates_7483481cd1235986c225742b003e6642/160909_regula_en.pdf, skatīts 02.10.2020.

ES E-Veselības rīcības plāns 2012.-2020.gadam[17] (*eHealth Action Plan 2012-2020*) paredzēja vairākus mērķus:

a) panākt e-Veselības pakalpojumu plašāku pieejamību un sasniegšanu;

b) atbalstīt pētniecību, attīstību un jauninājumus e-Veselības un labklājības jomā, lai nodrošinātu lietotājam draudzīgu rīku, lietotņu un pakalpojumu pieejamību;

c) atvieglot e-Veselības (telemedicīnas) ieviešanu un nodrošināt plašāku ieviešanu;

d) veicināt rīcībpolitikas dialogu un starptautisko sadarbību e-Veselības/telemedicīnas jomā globālā līmenī.

Savukārt , ES Veselības vīzija 2021-207.gadam (EU4Health 2021-2027) paredz trīs prioritātes, no kurām divas vistiešākā veidā ir saistītas ar telemedicīnu un turpina jau uzsāktas aktivitātes. Respektīvi, ES līdz 2027.gadam plāno[18]:

a) palielināt ES gatavību un pārrobežu sadarbību veselības apdraudējumiem;
b) stiprināt veselības aprūpes sistēmas nākotnes pandēmijām un krīzēm, kur veselības aprūpes sistēmas digitālā transformācija ir viena no svarīgākajām rīcībām;
c) padarīt medikamentus un medicīnas ierīces pieejamākas sabiedrībai.

ES veselības jomā 2021.-207.gadā plāno turpināt attīstīt ar veselību saistīto datu apmaiņu platformas, lai nodrošinātu drošu un efektīvu pārrobežu veselības aprūpi, kā arī koncentrēties uz digitālo instrumentu un tehnoloģiju izmantošanu iedzīvotāju pieejamības nodrošināšanai veselības aprūpei.[19]

Atbilstoši Komisijas paziņojumam Eiropas Parlamentam, Padomei, Eiropas Ekonomikas un sociālo lietu komitejai un Reģionu komitejai par telemedicīnu pacientu, veselības aprūpes sistēmu un sabiedrības labā (04.11.2008., COM (2008) 689)[20] telemedicīna ir gan veselības aprūpes pakalpojums, gan arī informācijas sabiedrības pakalpojums, līdz ar to uz telemedicīnas pakalpojumiem ir attiecināmas arī prasības, kas izvirzītas informācijas sabiedrības pakalpojumiem. Komisijas paziņojumā pausts mudinājums dalībvalstīm iekļaut telemedicīnu veselības aizsardzības politikā un pārvarēt šķēršļus, kas kavē telemedicīnas

[17] *eHealth Action Plan 2012-2020 - Innovative healthcare for the 21st century. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committe of the Regions.* Brussels, 6.12.2012 COM(2012) 736 final.

[18] EU4Health 2021-2027 – a vision for a healthier European Union. https://ec.europa.eu/health/funding/eu4health_en, skatīts 04.10.2020.

[19] Proposal for a Regulation of the European Parliament and of the Council on the establishment of a Programme for the Union's action in the field of health –for the period 2021-2027 and repealing Regulation (EU) No 282/2014 ("EU4Health Programme"). Brussels, 28.5.2020 COM(2020) 405 final2020/0102 (COD). https://eur-lex.europa.eu/resource.html?uri=cellar:9b76a771-a0c4-11ea-9d2d-01aa75ed71a1.0001.02/DOC_1&format=PDF, skatīts 02.10.2020.

[20] *Eiropas Ekonomikas un sociālo lietu komitejas atzinums par tematu Komisijas paziņojums Eiropas Parlamentam, Padomei, Eiropas Ekonomikas un sociālo lietu komitejai un Reģionu komitejai par telemedicīnu pacientu, veselības aprūpes sistēmu un sabiedrības labā COM(2008*) 689 galīgā redakcija. Izgūts no https://eur-lex.europa.eu/legal-content/LV/TXT/PDF/?uri=CELEX:52009AE1197&from=LV , skatīts 02.10.2020.

plašāku izmantošanu valstī. Eiropas Komisija iesaka telemedicīnas ieviešanu strukturēt trijos līmeņos:

a) Veidot uzticēšanos telemedicīnas pakalpojumiem (t.i., pārvarēt kultūras, sociālās un tehniskās barjeras);

b) Ieviest juridisku skaidrību – kas nozīmē noteikt telemedicīnas izmantošanas jomas un veidot tām nepieciešamo tiesisko pamatu;

c) Atrisināt tehniskās problēmas un atvieglot tirgus attīstību telemedicīnas jomā – jānodrošina maksimāli lielam iedzīvotāju skaitam pieeja digitālajām tehnoloģijām.

3.2.2 Nacionālā līmenī

"Pamatnostādnes e-Veselība Latvijā", pieņemtas 2005.gada 17.augustā[21]

2005. gadā apstiprinātās e-Veselības pamatnostādnes apkopojušas informāciju un secinājušas, ka tajā laikā tikai 42% pašvaldību tika 100% nodrošinātas ar piekļuvi internetam (Jēkabpils, Krāslavas, Bauskas, Talsu, Dobeles, Preiļu, Rīgas, Jelgavas, Alūksnes, Ogres, Limbažu rajonos), taču 23% pašvaldību nav pieejams interneta pieslēgums, un dominēja dažādu pakalpojumu sniedzēju un interneta tīkla pieslēgumi[22]. Šāds nevienmērīgs sadalījums radīja risku, ka ne visām veselības aprūpes iestādēm ir vienlīdzīga iespēja gan izmantot, gan sniegt e-Veselības pakalpojumus, tādēļ iespējas saņemt pakalpojumus var būt limitētas.

Lai arī 2005.gadā interneta tīkls vēl nebija tika attīstīts kā 2020.gadā, tomēr pamatnostādnes piedāvāja iespējamus risinājumus, kas modernizētu Latvijas veselības aprūpes sistēmu atbilstoši pasaules tendencēm:

- Veselības aprūpes iestāžu informācijas sistēmu (arī elektroniskās slimības vēstures) ieviešana;
- Elektronisko veselības karšu (*Electronical Health Record*) ieviešana;
- Telemedicīnas attīstība;
- Veselības aprūpes pakalpojumu saņemšanas procesa standartizācija un elektronizācija – pakalpojumu saņemšanas ķēžu ieviešana;
- Uzskaites informācijas uzlabošana (veselības aprūpes statistika, zāļu (arī narkotisko un psihotropo zāļu) lietošanas uzskaite);
- Centralizēta veselības aprūpes portāla izveide.

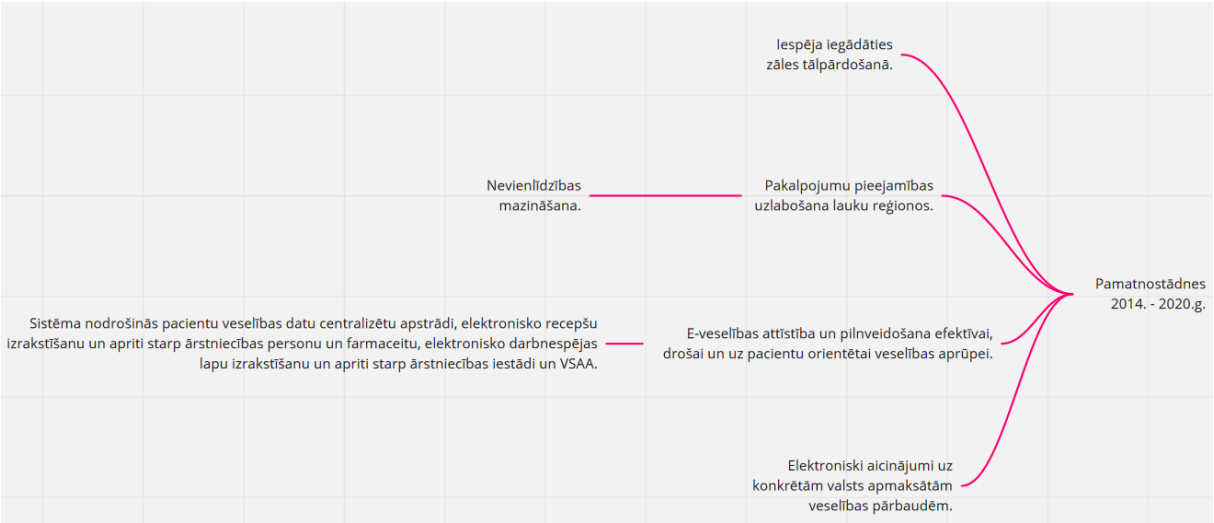
[21] Ministru kabinets (pieņemts 25.08.2005). *Ministru kabineta rīkojums Nr. 560. "Par pamatnostādnēm "e-Veselība Latvijā"*. Izgūts no https://likumi.lv/ta/id/114693-par-pamatnostadnem-ie-veselibai-latvija, skatīts 02.10.2020.

[22] *Pamatnostādnes „e-Veselība Latvijā" (informatīvā daļa)* (2005). Izgūts no https://www.who.int/goe/policies/latvia_ehealth_2005.pdf, skatīts 02.10.2020.

Savukārt, "Pamatnostādņu "E-Veselība Latvijā" ieviešanu 2014.-2017.gadā gala atskaitē"[23] ir secināts, ka 2007.-2013.gada ES struktūrfondu plānošanas periodā veselības jomā ir ieviesta virkne projektu, kas vērsti uz infrastruktūras un e-pakalpojumu attīstību, tostarp, ir izveidots e-Veselības portāls.

Sabiedrības veselības pamatnostādnes 2014-2020.gadam, pieņemtas 2014.gada 14.oktobrī[24].Sabiedrības veselības pamatnostādnes 2014.-2020.gadam faktiski paredz vairākas rīcības e-Veselības jomā[25]. Pamatnostādnes atzīts, ka IKT un e-Veselības attīstības tendences, kopā ar sabiedrības pieprasījumu pēc augstāka līmeņa pakalpojumiem un demogrāfiskās prognozes, nosaka valstīm nepieciešamību turpināt jau izstrādāto e-Veselības risinājumu attīstīšanu un investēt jaunu e-Veselības/telemedicīnas risinājumu izstrādē, panākot digitālās veselības rīku un risinājumu lietošanas aptvērumu sabiedrībā.

Atbilstošu pamatnostādņu redzējumam – laika periodā starp 2007.gadu un 2020.gadu, kas aptver divus ES struktūrfondu plānošanas periodus, e-Veselības informācijas sistēma tiktu attīstīta un sastāvētu no vairākām informācijas sistēmām - e-receptes informācijas sistēmas, elektroniskās veselības kartes informācijas sistēmas, pierakstu/nosūtījumu informācijas sistēmas, kā arī sadarbības platformas, kurā tiktu organizēta datu apmaiņa starp centrālajām valsts sistēmām un ārstniecības iestāžu un aptieku informācijas sistēmām, kā arī datu apriti starp ārstniecības personu un farmaceitu, elektronisko darbnespējas lapu izrakstīšanu un datu/informācijas apriti starp ārstniecības iestādi un VSAA.



4.attēls. Sabiedrības veselības pamatnostādņu 2014-2020.gadam skatījums uz telemedicīnu.

2020.gada pavasarī sākās darbs pie nākamā plānošanas perioda pamatnostādnēm – "**Sabiedrības veselības pamatnostādnes 2021.-2027. gadam**". Jaunās pamatnostādnes[26] paredz izmantot telemedicīnas risinājumus hronisku pacientu aprūpei mājās. Vienlaikus,

[23] *Informatīvais ziņojums "Par pamatnostādņu "E-Veselība Latvijā" ieviešanu 2014.-2017.gadā gala atskaite".* Izgūts nohttp://tap.mk.gov.lv/doc/2018_10/VMzino_220618_eves.1577.docx, skatīts 02.10.2020.

[24] *Sabiedrības veselības pamatnostādnes 2014-2020.gadam.* Apstiprinātas 2014.gada 14.oktobrī. Izgūts no http://polsis.mk.gov.lv/documents/4965, skatīts 02.10.2020.

[25] Pamatnostādnēs tiek lietots jēdziens "e-Veselība", nevis telemedicīna vai digitālā veselība.

[26] Uz 2020.gada 20.decembri pamatnostādnes ir izstrādes stadijā un atrodas sabiedriskajā apspriešanā.

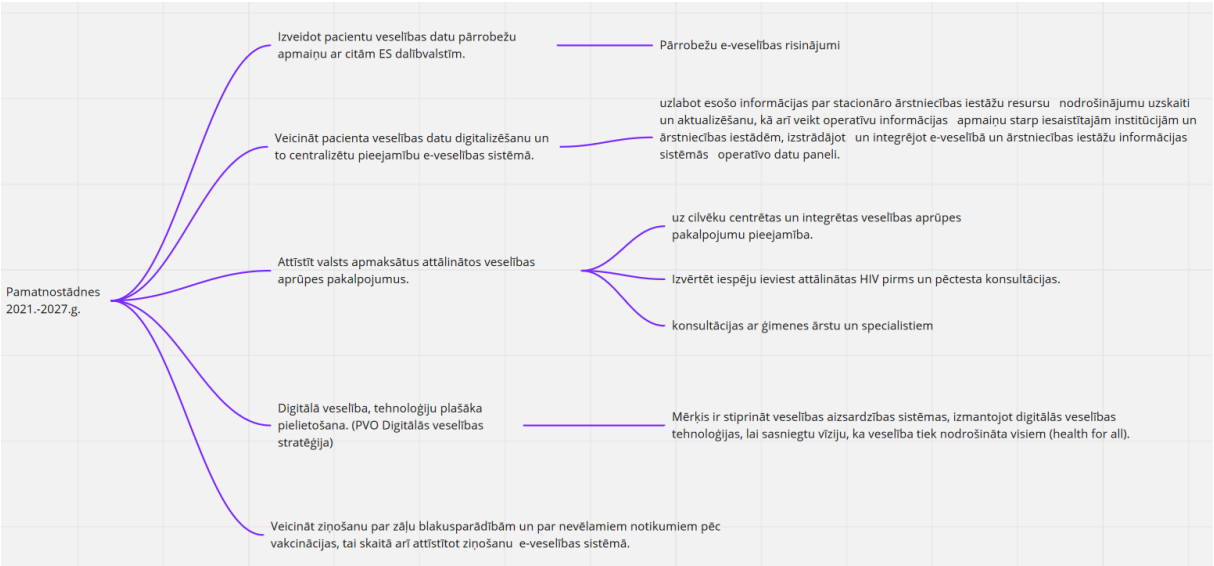
pamatnostādnēs ir paredzētas darbības, lai novērstu vairākas praktiskas nepilnības, kas tika konstatētas arī intervijās un aptaujā. Proti, pamatnostādnēs tiek plānots:

a) veicināt pacienta veselības datu digitalizēšanu un to centralizētu pieejamību e-Veselības sistēmā, atsakoties no t.s., papīra formas pacienta kartiņām;

b) veidot pacientu veselības datu pārrobežu apmaiņu ar citām ES dalībvalstīm;

c) veidot e-Veselību, kā vietu, kur pacients var ziņot par blakusparādībām un par nevēlamiem notikumiem pēc vakcinācijas;

d) uzlabot esošo informācijas par stacionāro ārstniecības iestāžu resursu nodrošinājumu uzskaiti un aktualizēšanu, kā arī veikt operatīvu elektronisku informācijas apmaiņu starp iesaistītajām institūcijām un ārstniecības iestādēm.



5.attēls. Sabiedrības veselības pamatnostādņu projekta 2021.-2027. gadam skatījums uz digitālo veselību

Ārstniecības likums ir uzskatāms par galveno normatīvu aktu veselības politikas jomā.

2014.gada 11.septembrī "Ārstniecības likumā" tika veikti grozījumi un ietverts telemedicīnas definējums[27]:

"***telemedicīna*** *— attālināta veselības aprūpes pakalpojuma sniegšana, izmantojot informācijas un komunikācijas tehnoloģijas. Tā ietver ārstniecībai nepieciešamu medicīnisku datu un informācijas drošu pārsūtīšanu teksta, skaņu, attēlu vai citā formātā*".

Ārstniecības likumā ietvertais telemedicīnas definējums neatspoguļo attīstību nozarē, kas ir notikusi pēdējo gadu laikā. Ņemot vērā, PVO stratēģiju par digitālo veselību 2020.-

[27] Saeima (pieņemts 12.06.1997). *Ārstniecības likums.* Izgūts no https://likumi.lv/doc.php?id=44108, skatīts 02.10.2020.

2027.gadam, ASV Pārtikas un zāļu administrācijas un Amerikas Ģimenes ārstu asociācijas skaidrojumus par IKT lietojumu veselības jomā saistīto terminu un izpratnes attīstību būtu ieteicams ietvert Ārstniecības likumā, citā normatīvajā aktā vai rīcībpolitikas attīstības plānošanas dokumentā precīzāku skaidrojumu, jo šīs asociācijas lietotais definējums ir visaptverošākais.

Likuma "Par prakses ārstiem" 6.pants[28] nosaka, ka prakses ārsts ārstēšanu nedrīkst veikt ar masu saziņas un komunikācijas līdzekļu starpniecību vai sarakstes veidā. Respektīvi, šī likuma norma aizliedz telemedicīnu. Tādējādi, normatīvo aktu starpā (t.i., Ārstniecības likums un likums "Par prakses ārstiem") ir savstarpēja pretruna, kas būtu jānovērš. Ārstniecības likums kā vispārējā tiesību norma un arī jaunākā tiesību norma atļauj telemedicīnu. Tajā pat laikā, Latvijā citos normatīvajos aktos nav izvirzītas specifiskas prasības telemedicīnas pakalpojumiem, kamēr normatīvie akti paredz regulējumu un definē prasības veselības aprūpes pakalpojumiem, kas tiek sniegti neizmantojot telemedicīnu.

Saskaņā ar Pacientu tiesību likuma 5.panta pirmo un otro daļu[29] ārstniecības personai ir jānodrošina veselības stāvoklim atbilstošu, kvalitatīvu un kvalificētu ārstniecību neatkarīgi no slimības rakstura un smaguma pakāpes. Tādēļ, izvēloties sniegt veselības aprūpes pakalpojumu attālināti vai sniegt telemedicīnas konsultāciju, katrā gadījumā ir jāizvērtē, vai ir vispār iespējams attālināti veikt ārstniecību, un vai tiek nodrošināta veselības stāvoklim atbilstoša, kvalitatīva un kvalificēta ārstniecība neatkarīgi no slimības rakstura un smaguma pakāpes. Tādējādi var secināt, ka Pacientu tiesību likuma 5.panta pirmajā daļā noteiktais paredz katras personas tiesības atbilstoši normatīvajos aktos noteiktajai kārtībai saņemt veselības stāvoklim atbilstošu ārstniecību, ir attiecināms arī uz telemedicīnu. Ja attālinātās konsultācijas rezultātā ārstniecības personai lemj izrakstīt recepti, pamatojoties uz telefoniski vai caur videokonferenci sniegtu konsultāciju, nepieciešams pārliecināties par pacienta identitāti, kā arī vai noteiktas receptes izrakstīšana pacientam nodrošinās veselības stāvoklim atbilstošu ārstniecību.

Visbeidzot, visi personas dati, kas satur informāciju par personas veselību, ir personas sensitīvie dati. Saskaņā ar Pacientu tiesību likuma 10.panta pirmo un otro daļu informācija, kas attiecas uz identificētu vai identificējamu pacientu, ir aizsargājama saskaņā ar fizisko personu datu aizsardzību regulējošiem normatīvajiem aktiem. Saskaņā ar Fizisko personu datu aizsardzības likuma 25.pantu[30] personas, kura atbild par personu datu apstrādi un personas, kas veic personas datu apstrādi, pienākums ir lietot nepieciešamos tehniskos un organizatoriskos līdzekļus, lai aizsargātu personas datus un novērstu to nelikumīgu apstrādi. Faktiski šī norma ietver arī nosacījumu nodrošināt tehniski drošu telemedicīnas pakalpojumu.

Rekomendācija:

[28] Saeima (pieņemts 24.04.1997). *Par prakses ārstiem*. Izgūts no https://likumi.lv/ta/id/43338-par-prakses-arstiem, skatīts 02.10.2020.
[29] Saeima (pieņemts 17.12.2009). *Pacientu tiesību likums.* Izgūts no https://likumi.lv/ta/id/203008-pacientu-tiesibu-likums, skatīts 04.10.2020.
[30] Saeima (pieņemts 21.06.2018). *Fizisko personu datu apstrādes likums.* Izgūts no https://likumi.lv/ta/id/300099-fizisko-personu-datu-apstrades-likums, skatīts 04.10.2020.

1. Iesakām papildināt nacionālos normatīvos aktus un/vai politikas plānošanas dokumentos ar precīzākām terminu definīcijām. Normatīvos aktos iesakām ietvert šādus definējumus:
   a) Digitālā veselība – kā visaptverošs termins, kas atspoguļotu IKT izmantošanu visās ar sabiedrības veselību un veselības aprūpi saistītās jomās.
   b) Telemedicīna – ņemot vērā to, ka šis termins tiek plaši lietots sabiedrībā, lai raksturotu un skaidrotu IKT izmantošanu veselības politikā.
2. Izslēgt no normatīvajiem aktiem (konkrēti likuma "Par prakses ārstiem") normas, kas aizliedz IKT lietošanu profilakses, diagnostikas un ārstēšanas procesos.

3.3 Interviju dati

Izvērtējuma laikā tika veiktas arī padziļinātās strukturētas attālinātās intervijas ar 10 ģimenes ārstiem, kuru viedoklis liecina par telemedicīnas attīstības vispārējām tendencēm (2. tabula). Padziļināto interviju laikā ģimenes ārsti pauda vēlmi detalizētāk iepazīties ar drošības aspektiem, kas būtu jāpievērš uzmanība ikdienas darbā un tā rezultātā ir izstrādātas rekomendācijas informācijas drošības pilnveidei ģimenes ārsta praksē (publiski pieejams tiešsaistē).

2. tabula. Konstatētās tendences intervijās.

Kategorija	Konstatētā tendence
Vispārējās tendences elektronisko sistēmu lietošanā	Tendences liecina, ka ikdienā ģimenes ārsti aptuveni pusi laika, kas paredzēts pacienta konsultācijai un vizītei, patērē darbam elektroniskajās sistēmās (piem., Ārsta prakses elektroniskā sistēma, e-Veselība, DataMed, e-pasts, Vadības informācijas sistēma). Visvairāk izmantotās elektroniskās sistēmas ir – e-Veselība, Smart Medical un DataMed, kur SmartMedical tiek novērtēts kā visfunkcionālākais risinājums. Turklāt arvien vairāk ārsti izvēlas informāciju par pacientu iegūt elektroniskajā ierakstā, nevis lasīt informāciju par pacientu papīra kartiņā.
Darba laika organizācija	Tendences liecina, ka visvairāk ģimenes ārstu darbu apgrūtina informācijas trūkums par veiktajām pārbaudēm, izmeklējumiem, analīzēm, veselības stāvokļa izmaiņām, kā arī ierobežota pieejamība pacientu datu kopsavilkumam. Tāpat ikdienas darbu apgrūtina tas, ka dati par veiktajām pārbaudēm, veselības stāvokli un izmaiņām atrodas

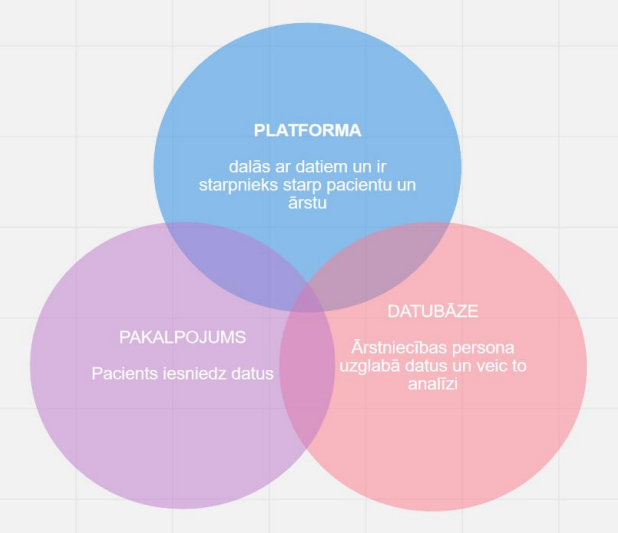
	katrā veselības iestādē atsevišķi, nevis vienotā portālā vai datu glabātuvē. Tādēļ, ģimenes ārsti vēlētos, lai būtu nodrošināta piekļuve visiem pacientu datiem un dažādas sistēmas būtu savstarpēji savietojamas.
Komunikācija ar pacientu	Visbiežāk ģimenes ārsti informāciju no pacientiem saņem ar viedtālruni sūtīta teksta vai attēla veidā, e-pastā un Whatsapp lietotnē. Informācijas saņemšanai tiek izmantotas arī Viber, Signal lietotnes. Savukārt, informācijas nodošanai populārākie rīki ir telefons, Whatsapp lietotne, Zoom un e-pasts.
Tehnoloģiskās problēmas elektroniskajās sistēmās	Ģimenes ārsti norādīja, ka pacientu dati atrodas vairākās elektroniskās sistēmas un šī fragmentācija palēnina un apgrūtina darbu. Turklāt, ir apgrūtināta informācijas apmaiņa starp sistēmām.
Drošības jautājumi	Ģimenes ārsti atzina, ka sūtot datus pacientiem, tos nešifrē[31], jo nav šādu prasmju vai arī nav zinājuši, ka tāda iespēja pastāv. Savukārt, antivīrusu un ugunsmūra programmatūra ir gandrīz visos datoros, kas tiek izmantoti ģimenes ārstu praksēs.

3.4 Telemedicīnas rīcībpolitikas ietvars

Telemedicīnas pakalpojumi bieži tiek saistīti arī ar telekonsultācijām, telediagnostiku vai diennakts zvanu centriem. Lielākoties telemedicīnu īsteno ar kādas lietotnes vai platformas palīdzību, kur iespējams kopīgot datus. Attiecīgi, dati tiek uzkrāti datubāzē, kur ārstniecības persona, cits veselības aprūpes personāls vai programmatūra tos analizē, kā tas attēlots 3.attēlā[32]. Jāmin, ka šāds tehnoloģiskais risinājums: platforma-datubāze-pakalpojums ir visnotaļ izplatīts ES dalībvalstīs uz balstās uz pieņēmumu, ka pacients, saņemot telemedicīnas pakalpojumus, dalās ar saviem veselības datiem. Savukārt, visi pacienta veselības dati tiek uzglabāti platformā, no kuras ārstniecības persona iegūst datus un veic to analīzi.

[31] Vispārīgā nozīmē datu šifrēšana ir datu un ziņojumu apstrādes process, ko veic datu sagatavotājs vai ziņojuma nosūtītājs, lai datus vai ziņojuma saturu nodrošinātu pret nesankcionētu izmantošanu.

[32] European Commission. (2018). *Market study on telemedicine.* Izgūts no https://ec.europa.eu/health/sites/health/files/ehealth/docs/2018_provision_marketstudy_telemedicine_en.pdf, skatīts 10.10.2020.



6.attēls. Telemedicīnas ietvars[33].

Tehniski telemedicīna izmanto vairākus tehnoloģiju tipus:

- Medicīniskās ierīces, kas paredzētas slimības diagnostikai, ārstēšanai, prevencijai, piemēram, pārnēsājams elektrokardiogrāfs, neinvazīvi glikozes līmeņa mērītāji;
- Lietotnes (tai skaitā tiešsaistes) pacientu veselības stāvokļa novērtēšanai attālināti – vizuāli, audiāli, izmantojot veikto izmeklējumu datu analīzi. Lietotne apkopo un kopīgo datus un šāda lietotne izmantojama pacientiem, veselības aprūpes nodrošinātājiem, var tikt instalēta telefonā vai planšetē
- Valkājama ierīce – viedā elektroniskā ierīce, kas var tikt nēsāta kā implants vai aksesuārs. Visbiežāk, ar valkājamo ierīci mērāms pulss, sirds ritms, skābekļa saturs, asinsspiediens, fiziskā aktivitāte vaimiega parametri;
- Telemedicīnas atbalsta programmatūra. Telemedicīna var tik sniegta izmantojot speciālu programmproduktu, kas nodrošina darba plūsmas pārvaldības funkciju, veselības datu pārvaldību, vispārējo datu drošību.
- Lielie dati, mākslīgais intelekts, robotika, datorredze – izmanto liela apjoma datu analīzē, piem., radioloģijā.

Tiesa, PVO definīcija "medicīnas ierīces" ir diezgan plaša, jo medicīnas ierīces var būt ir jebkurš instruments, aparāts, darbarīks, mašīna, ierīce, implants, programmatūra, materiāls vai citi līdzīgi rīki, kurus ražotājs paredzējis lietošanai kopā vai atsevišķi vienam vai vairākiem ar medicīnu un veselības aprūpi saistītos jautājumos[34].

[33] European Commission. (2018). *Market study on telemedicine.* Izgūts no https://ec.europa.eu/health/sites/health/files/ehealth/docs/2018_provision_marketstudy_telemedicine_en.pdf, skatīts 10.10.2020., 28.lpp.

[34] *Medical Devices.* Izgūts no https://www.who.int/health-topics/medical-devices#tab=tab_1, skatīts 10.10.2020.,

Lai arī dažādi telemedicīnas risinājumi tiek attīstīti ES, tomēr tie galvenokārt ir veidoti dalībvalstu nacionālajam tirgum, jo tā kā veselības aprūpe un aizsardzība ir dalībvalstu ekskluzīvas kompetences[35] jautājums, kur ES var veikt visas nepieciešamās darbības, lai atbalstītu un koordinētu dalībvalstu rīcības. Līdz ar to telemedicīnas risinājumus normatīvo ierobežojumu dēļ ir diezgan komplicēti izplatīt citā ES dalībvalstī vai ārpus ES.

Jebkurā gadījumā veselības aizsardzības kontekstā, telemedicīnai ir jānodrošina 4 dimensijas:

1) Prevenciju – risinājumiem ir jābūt kā profilaktiskiem un preventīviem līdzekļiem;
2) Slimību ārstēšanu – sniedzot būtisku ieguldījumu slimību diagnostikā un ārstēšanā;
3) Telemonitorings – slimības norises uzraudzība
4) Labsajūtas un dzīves kvalitātes uzlabojumi – telemedicīna nodrošina ar cilvēka dzīves kvalitāti saistītus veselības aprūpes aspektus.

Kopumā, ES telemedicīnas risinājumus skatās arī pēc mijiedarbības starp iesaistītajām pusēm[36]:

- "Pacients – ārsts": pacients iniciē saziņu ar ārstniecības personu, lai saņemtu padomu vai konsultāciju;
- "Ārsts-pacients": ārstniecības persona iniciē saziņu ar pacientu un izmanto telemedicīnas risinājumu, lai nodrošinātu veselības aprūpi;
- "Pacients-cits medicīnas aprūpes personāls" (piem., māsa vai ārsta palīgs): pacients inicē saziņu ar medicīnas aprūpes profesionāli;
- "Ārsts-ārsts": ārstniecības personāls apmainās ar informāciju vai datiem (piem, Eiropā – eHDSI (*eHealth Digital Service Infrastructre*) un ERNs (*European Reference Networks*). Tiesa, eHDSI infrastruktūra, kas veidota kā pārrobežu e-veselības risinājums, šobrīd neparedz tiešu komunikāciju (t.i., telekonsultācijas) starp ārstiem. Šobrīd infrastruktūra nodrošina tikai e-recepšu un pacienta veselības datu kopsavilkumu pieejamību citā dalībvalstī.
- Ārsts-ārsts": ārstniecības personāls apmainās ar informāciju vai datiem (piem, Eiropā – eHDSI (*eHealth Digital Service Infrastructre*) un ERNs (*European Reference Networks*). Tiesa, eHDSI infrastruktūra, kas veidota kā pārrobežu e-veselības risinājums, šobrīd neparedz tiešu komunikāciju (t.i., telekonsultācijas) starp ārstiem. Šobrīd infrastruktūra nodrošina tikai e-recepšu un pacienta veselības datu kopsavilkumu pieejamību citā dalībvalstī.

[35] Lisabonas Līgums, ar ko groza Līgumu par Eiropas Savienību un Eiropas Kopienas dibināšanas līgumu, parakstīts Lisabonā2007. gada 13. decembrī. Izgūts no https://eur-lex.europa.eu/legal-content/LV/TXT/PDF/?uri=OJ:C:2007:306:FULL&from=LV, skatīts 10.10.2020.,
[36] European Commission. (2018). *Market study on telemedicine*. Izgūts no https://ec.europa.eu/health/sites/health/files/ehealth/docs/2018_provision_marketstudy_telemedicine_en.pdf, skatīts 10.10.2020.

Vienlaikus, ES telpā telemedicīnas jomā attīstās standarti un vadlīnijas, kas vērsti uz to, lai palielinātu telemedicīnas pakalpojumu drošību. Standarti un vadlīnijas aptver šādas telemedicīnas jomas:

a) Personas datu aizsardzības noteikumi (piem., GDPR, starptautiskais standarts veselības informātikas jomā ISO 17975:2015[37]);

b) Tehnoloģiju un aprīkojuma standarti un lietošanas noteikumi;

c) Klīniskās vadlīnijas;

d) Ētiskie standarti un vadlīnijas, datu uzglabāšanas un apstrādes noteikumi, labas darba prakses nodrošinājumam;

e) Organizatoriskās vadlīnijas, kas regulē procesa izpilde, kompetences un atbildības (piem., starptautiskaisvadības sistēmu standarts ISO 9001:2015[38]);

f) Ar cilvēkresursiem saistītās vadlīnijas, tostarp veselības aprūpē nodarbinātā personāla kvalifikācija un tālākizglītība, kompetences.

ES galvenie telemedicīnas risinājumu nodrošinātāji ir[39]:

- Telekomunikāciju kompānijas un mobilie operatori (piem., Vodofone, Deutche Telekom, Orange), kas investē telemedicīnas risinājumos, nodrošinot datu pārraidi un datu glabāšanu, kā arī augstas izšķirtspējas attēlu un video-konferenču risinājumus.
- Lielie informācijas un komunikāciju tehnoloģiju uzņēmumi (piem., Google. Microsoft, IBM, Phillips) izmanto savu pieredzi produktu, programmproduktu un platformu veidošanā, kas nodrošina telemedicīnas lietotājus ar funkcionāliem produktiem.
- Medicīnisko vai monitoringa ierīču vai platformu izgatavotāji (piem., Medtronik, Aerotel) piedāvā tehnoloģijas pacientiem, lai ievāktu datus ar sensoru un platformu palīdzību. Iegūtie dati vēlāk var tik apspriesti ar ārstniecības personām.
- Farmācijas kompānijas (piem., Roche, GlaxoSmithKline) sadarbībā ar informācijas un komunikāciju tehnoloģiju uzņēmumiem veido telemedicīnas risinājumus.
- Jaunuzņēmumi *(Start-up's)* piedāvā un veido mērķa fokusētus risinājumus, ar mērķi vienkāršot pieeju veselības aprūpes pakalpojumiem.

[37] ISO/ TS 17975:2015. Health informatics — Principles and data requirements for consent in the Collection, Use or Disclosure of personal health information. Izgūts no https://www.iso.org/standard/61186.html skatīts 04.01.2021.

[38] ISO 9001:2015. Quality management systems — Requirements. Izgūts no https://www.iso.org/standard/62085.html, skatīts 04.01.2021.

[39] European Commission. (2018). Market study on telemedicine. Retrieved from: https://ec.europa.eu/health/sites/health/files/ehealth/docs/2018_provision_marketstudy_telemedicine_en.pdf, skatīts 10.10.2020.

Lai arī telemedicīnas risinājumu attīstītās, tomēr ir jārēķinās ar iespējamiem draudiem[40],

- Kiberdrošības riski, kas var ietekmēt pacientu datu drošību
- Ierobežotas konkurences dēļ, tehnoloģiskās zināšanas var koncentrēties dažu spēlētāju rokās, tā radot situāciju, ka telemedicīnas risinājumu vairs nav pieejami iedzīvotājiem
- Vecākās paaudzes skepse pret telemedicīnu kombinācijā ar zemām digitālajām prasmēm ierobežo telemedicīnas attīstību.

Faktiski, zemas un nepietiekamas iedzīvotāju digitālās prasmes var būt izšķirošais faktors digitālās transformācijas procesā, t.sk. arī digitālai transformācijai veselības jomā.

[40] European Commission. (2018). *Market study on telemedicine*. Izgūts no https://ec.europa.eu/health/sites/health/files/ehealth/docs/2018_provision_marketstudy_telemedicine_en.pdf, skatīts 10.10.2020.

4 Telemedicīnas tendences un ietekmējošie faktori

Faktori, kas ietekmē telemedicīnas ieviešanu

Laika gaitā ir pieaugusi telemedicīnas izmantošana, tomēr akadēmiskos pētījumos ir novērots arī tas, ka ieinteresētās puses diezgan pasīvi iesaistās telemedicīnas izmantošanā dažādu faktoru ietekmē. Kopumā, galvenie faktori, kuru ietekmē, telemedicīnas ieviešana notiek lēni ir šādi: cilvēciskie faktori[41]; organizatoriskie faktori[42] ;kultūras barjeras vai šķēršļi[43]

Daļa no negatīvās ietekmes faktoriem ir jāaplūko kontekstā ar riskiem pacientu drošībai, kur lielākā nozīme ir cilvēciskajiem faktoriem (3. tabula).

3.tabula. Kopsavilkums par akadēmiskiem pētījumiem, kuros aplūkoti telemedicīnas riski pacientu drošībai[44].

Autors un pētījuma publicēšanas gads	Telemedicīnas pakalpojuma veids	Potenciālā riska avots pacientu drošībai
(de Lusignan et al.) (2001)	Pulsa un asinsspiediena aparāti, ierīces video konsultācijām.	Tehniskas problēmas. Pacientu atkarība no pakalpojuma.
(Essén & Conrick) (2008)	Uz sensoriem balstīta tālvadības sistēma.	Zināšanu trūkums pacientu un personāla vidū. Izmaiņas veselības darbinieku darba slodzē. Vadlīniju trūkums.
(Hibbert et al.) (2004)	Attālināta aprūpe mājās, hroniski obstruktīvās plaušu slimības (HOPS) pacientiem, izmantojot	Tehniskas problēmas. Izmaiņas klīniskās aprūpes darbā.

[41] Demiris, G., Charness, N., Krupinski, E., Ben-Arieh, D., Washington, K., Wu, J., Farberow, B., *The role of human factors in telehealth*. Telemed e-Health. 2010;16(4):446–53. 11.
Gagnon, M.-P., Godin, G., Gagné, C., Fortin, J.-P., Lamothe, L., Reinharz, D., Cloutier, A., *An adaptation of the theory of interpersonal behaviour to the study of telemedicine adoption by physicians*. Int J Med Inform. 2003;71(2–3):103–15.

[42] Cresswell, K., Sheikh, A., *Organizational issues in the implementation and adoption of health information technology innovations: an interpretative review*. Int J Med Inform. 2013;82:e73–86. 13. Jennett, P., Yeo, M., Pauls, M., Graham, J., *Organizational readiness for telemedicine: implications for success and failure.* J Telemed Telecare. 2003; 9(2_suppl):27–30.

[43] Shore, J.H., Savin, D.M., Novins, D., Manson, S.M., *Cultural aspects of telepsychiatry.* J Telemed Telecare. 2006;12(3):116–21.

[44] Veslemøy, G,, Anderson J., Wiig, S., *Patient safety risks associated with telecare: a systematic review and narrative synthesis of the literature.* Izgūts no http://www.biomedcentral.com/1472-6963/14/588, skatīts 15.10.2020.

Autors un pētījuma publicēšanas gads	Telemedicīnas pakalpojuma veids	Potenciālā riska avots pacientu drošībai
	video un uzraugot vitāli svarīgos rādītājus (*vital signs monitoring*)	
(Marziali et al.) (2005)	Medicīnisko simptomu novērošana, izmantojot sinhronizētas tehnoloģijas.	Vadlīniju trūkums.
(Hopp et al.) (2006)	Uzkrāj-un-nosūti (*store-and-forward*) ierīces, videokonferenču ierīces.	Zināšanu trūkums pacientu un darbinieku vidū. Tehniskas problēmas. Pacientu neuzticība, nepaļaušanās. Izmaiņas klīniskās aprūpes darbā. Izmaiņas darbinieku darba slodzē.
(Mair er al.) (2008)	Video saite un pielikumi, fizioloģisku vitālo rādītāju izmaiņu novērošanai.	Izmaiņas klīniskās aprūpes darbā. Darba slodzes izmaiņas.
(Horton) (2008)	Pacientu veselības stāvokļa uzraudzīšana ikdienā, izmantojot ātrās reaģēšanas un/vai neatliekamās palīdzības dienesta zvanu centru.	Tehniskas problēmas. Zināšanu trūkums pacientu un darbinieku vidū.
(Sandberg et al.) (2009)	Attālinātās aprūpes iekārta ar videokonferences režīmu, glikozes un asinsspiediena mērījumu lasījumiem un izglītojošiem materiāliem.	Tehnoloģiskas problēmas. Pacientu zināšanu trūkums. Izmaiņas klīniskās aprūpes darbā.
(Wälivaara et al.) (2009)	Mobilo ierīču attāluma aptveršanas tehnoloģija, lai mērītu vitālās pazīmes.	Slikta pacientu uzticēšanās. Pacientu zināšanu trūkums. Pieejamības trūkums.

Autors un pētījuma publicēšanas gads	Telemedicīnas pakalpojuma veids	Potenciālā riska avots pacientu drošībai
		Izmaiņas klīniskās aprūpes darbā.
(Brewer et al.) (2010)	Tehnoloģiju izmantošana uzraudzībai pieaugušajiem ar attīstības traucējumiem.	Izmaiņas klīniskās aprūpes darbā.
(Zayas-Cabán & Dixon) (2010)	Dažādas IT lietotnes, ieskaitot videotelefonus, ziņapmaiņas sistēmas un veselības monitoringa ierīces.	Tehnoloģiskas problēmas. Nedroša ierīču sasaiste/savienošanās.
(Nilsson et al.) (2010)	Elektronisko ziņu sistēma, lai komunicētu ar pacientiem.	Tehnoloģiskas problēmas.
(Sicotte & Paré) (2011)	Mobilo tehnoloģiju programmatūra, lai plānotu un organizētu mājaprūpes kopšanu.	Tehnoloģiskas problēmas. Slikta sistēmas integrācija. Darba slodzes izmaiņas.
(Skär & Söderberg) (2011)	Lietotne informācijai un saziņai starp hroniski slimiem pacientiem un medmāsu.	Tehnoloģiskas problēmas Izmaiņas klīniskās aprūpes darbā.
(Wälivaara et al.) (2011)	Mobilā attāluma aptveršanas tehnoloģija, komunikācijas un diagnostikas nolūkos.	Pacientu zināšanu trūkums Izmaiņas klīniskās aprūpes darbā
(Young et al.) (2011)	Ziņapmaiņas ierīces, monitoringa un mērīšanas iekārtas, videotelefoni, datori.	Pieejamības trūkums
(Radhakrishnan et al.) (2012)	Centralizēts ikdienas tālvadības modelis, lai novērotu vitālās pazīmes, izmantojot attālinātās aprūpes medmāsas ar klātienes apmeklējumu, ja tāds nepieciešams.	Trauksme pacientiem. Pacientu atkarība no pakalpojuma. Pacientu zināšanu trūkums. Darba slodzes izmaiņas veselības aprūpes darbiniekiem.

Autors un pētījuma publicēšanas gads	Telemedicīnas pakalpojuma veids	Potenciālā riska avots pacientu drošībai
		Izmaiņas klīniskās aprūpes darbā. Vadlīniju trūkums.
(Roberts et al.) (2012)	Mājas skārienekrāns klīniskās uzraudzības iespējai hipertonijas un HOPS pacientiem.	Darba slodzes izmaiņas
(Shea & Chamoff) (2012)	Tālvadība; pacientu sazināšanās ar medmāsām, izmantojot telestaciju (*tele-station*), kas uzkrāj un pārsūta datus pa sakaru līnijām.	Pacientu un darbinieku zināšanu trūkums.
(Hanley et al.) (2013)	Asinsspiediena mērītājs mājās un mobilā tālruņa tehnoloģija asinsspiediena rādījumu pārsūtīšanai, izmantojot SMS, uz drošu vietni.	Trauksme pacientiem Pacientu atkarība no pakalpojuma. Slikta sistēmas integrācija. Izmaiņas darba slodzē. Pieejamības jautājumi.
(Brewster et al.) (2014)	Attālinātās veselības tehnoloģijas, lai uzraudzītu hroniski obstruktīvās plaušu slimības (HOPS) un sirds mazspēju.	Izmaiņas klīniskās aprūpes darbā. Izmaiņas veselības aprūpes darbinieku darba slodzē.
(Lu et al.) (2014)	Tālvadība asinsspiediena un/vai cukura līmeņa asinīs noteikšanai, veselības aprūpes pieejamība konsultācijām, izmantojot datoru vai telefonu.	Pacientu zināšanu trūkums.
(Agarwal et al.) (2014)[45]	Virtuāla iespējamo insulta pacientu izmeklēšana ar video palīdzību, konsultējot pacientus	Centra un perifērijas transporta ceļu savienojums

[45] Agarwal, S., Day, D. J., Sibson, L., Barry, P. J., Collas, D., Metcalf, K., Cotter, P. E., Guyler, P., O'Brien, E. W., O'Brien, A., O'Kane, D., Owusu-Agyei, P., Phillips, P., Shekhar, R., & Warburton, E. A. (2014). Thrombolysis delivery by a regional telestroke network--experience from the U.K. National Health Service. *Journal of the American Heart Association*, *3*(1), e000408. Izgūts no https://doi.org/10.1161/JAHA.113.000408 , skatīts 20.12.2020.

Autors un pētījuma publicēšanas gads	Telemedicīnas pakalpojuma veids	Potenciālā riska avots pacientu drošībai
		Pacienta zināšanu un prasmju trūkums
(Rosenbek Minet et al.) (2015)[46]	Attālinātās veselības tehnoloģijas, lai uzraudzītu, konsultētu un apmācītu smagus hroniski obstruktīvās plaušu slimības (HOPS) pacientus pēc hospitalizācijas.	Pacienta zināšanu un prasmju trūkums Iespējamās cenu atšķirības par attālinātu un klātienes pakalpojumu
(Burke et al.) (2015)[47]	Telemedicīna pediatrijā: teleapmācīšana, telekonsultēšana, teleaprūpe, virtuālās nodarbības u.c.	Pakalpojuma pārrobežu licencēšana un informācijas pārnese. Var netikt nodrošināta datu un slimības vēstures kontinuitāte Izmaiņas veselības aprūpes darbinieku darba slodzē
(Buvik et al.) (2016)[48]	Attālinātas ortopēdiskās konsultācijas ar videozvanu palīdzību.	Pilnā apjomā telemedicīnu nevar izmantot, jo nepieciešama pacienta fiziska apskate
(O'Connor et al.) (2016)[49]	Telemedicīnas barjeras kopumā	Pacienta motivācijas trūkums lietot telemedicīnu, zemas digitālās prasmes un nezināšana par telemedicīnas guvumiem

[46] Rosenbek Minet, L., Hansen, L. W., Pedersen, C. D., Titlestad, I. L., Christensen, J. K., Kidholm, K., Rayce, K., Bowes, A., & Møllegård, L. (2015). Early telemedicine training and counselling after hospitalization in patients with severe chronic obstructive pulmonary disease: a feasibility study. *BMC medical informatics and decision making*, *15*, 3. Izgūts no https://doi.org/10.1186/s12911-014-0124-4, skatīts 20.12.2020.

[47] Burke, B. L., Jr, Hall, R. W., & SECTION ON TELEHEALTH CARE (2015). Telemedicine: Pediatric Applications. Pediatrics, 136(1), e293–e308. Izgūts no: https://doi.org/10.1542/peds.2015-1517, skatīts 20.12.2020.

[48] Buvik, A., Bugge, E., Knutsen, G., Småbrekke, A., & Wilsgaard, T. (2016). Quality of care for remote orthopaedic consultations using telemedicine: a randomised controlled trial. BMC health services research, 16(1), 483.Izgūts no https://doi.org/10.1186/s12913-016-1717-7, skatīts 21.12.2020.

[49] O'Connor, S., Hanlon, P., O'Donnell, C. A., Garcia,S., Glanville J., Mair, F.S., *Understanding factors affecting patient and public engagement and recruitment to digital health interventions: a systematic review of qualitative studies*. BMC Medical Informatics and Decision Making (2016) 16:120 DOI 10.1186/s12911-016-0359-3.

Autors un pētījuma publicēšanas gads	Telemedicīnas pakalpojuma veids	Potenciālā riska avots pacientu drošībai
(Smith et al.) (2016)[50]	Pārvaldības programmas tālruņos un elektoniskajās planšetēs hroniski obstruktīvās plaušu slimības (HOPS) agrīnai konstatēšanai un ārstēšanai.	Trauksme pacientiem
(Weiner et al.) (2017)[51]	Interaktīva balss atbildes sistēma (IVRS), lai samazinātu pirmsdialīzes blakusparādības hroniskas nieru mazspējas gadījumos.	Pacienta zināšanu un prasmju trūkums Komunikācijas problēmas starp pacientu un ārstniecības personālu
(Müller et al.) (2017)[52]	Telemedicīna neakūtu galvassāpju ārstēšanai.	Darba slodzes izmaiņas veselības aprūpes darbiniekiem Komunikācijas problēmas starp pacientu un ārstniecības personālu
(Marien et al.) (2018)[53]	Lietojumprogramma pacientu iesaistei medikamentu saskaņošanas procesā.	Pacienta IT zināšanu un prasmju trūkums (t.i., zemas digitālās prasmes)
(Kruse et.al.) (2018)[54]	Telemedicīnas barjeras kopumā	Pacientu zemas digitālās prasmes.

[50] Smith, H. S., Criner, A. J., Fehrle, D., Grabianowski, C. L., Jacobs, M. R., & Criner, G. J. (2016). Use of a SmartPhone/Tablet-Based Bidirectional Telemedicine Disease Management Program Facilitates Early Detection and Treatment of COPD Exacerbation Symptoms. Telemedicine journal and e-health : the official journal of the American Telemedicine Association, 22(5), 395–399. Izgūts no https://doi.org/10.1089/tmj.2015.0135, skatīts 21.12.2020.

[51] Weiner, S., & Fink, J. C. (2017). Telemedicine to Promote Patient Safety: Use of Phone-Based Interactive Voice-Response System to Reduce Adverse Safety Events in Pre-dialysis CKD. Advances in chronic kidney disease, 24(1), 31–38. Izgūts no: https://doi.org/10.1053/j.ackd.2016.12.004, skatīts 20.12.2020.

[52] Müller, K. I., Alstadhaug, K. B., & Bekkelund, S. I. (2017). A randomized trial of telemedicine efficacy and safety for nonacute headaches. Neurology, 89(2), 153–162. Izgūts no https://doi.org/10.1212/WNL.0000000000004085, skatīts 20.12.2020.

[53] Marien, S., Legrand, D., Ramdoyal, R., Nsenga, J., Ospina, G., Ramon, V., Boland, B., & Spinewine, A. (2018). A web application to involve patients in the medication reconciliation process: a user-centered usability and usefulness study. Journal of the American Medical Informatics Association : JAMIA, 25(11), 1488–1500. Izgūts no https://doi.org/10.1093/jamia/ocy107, skatīts 21.12.2020.

[54] Kruse, C. S., Karem, P., Shifflett, K., Vegi, L., Ravi, K., Brooks, M., *Evaluating barriers to adopting telemedicine worldwide: A systematic review*. Journal of Telemedicine and Telecare 2018, Vol. 24(1) 4–12. Izgūts no https://journals.sagepub.com/doi/pdf/10.1177/1357633X16674087, skatīts 20.12.2020.

Autors un pētījuma publicēšanas gads	Telemedicīnas pakalpojuma veids	Potenciālā riska avots pacientu drošībai
		Pakalpojumu pieejamības trūkums
(Hollander et al.) (2020)[55]	Telemedicīna vīrusa Covid-19 perspektīvā – klātienes medicīnisko pakalpojumu aizstāšana ar telemedicīnu.	Telemedicīna nevar aizstāt nepieciešamību pēc fiziskām procedūrām. Tehnoloģiskas problēmas
(Kichloo et al.) (2020)[56]	Klātienes medicīnisko pakalpojumu aizstāšana ar telemedicīnu.	Pacientu zemas digitālās prasmes Tehnoloģiskas problēmas Atgriezeniskās saites no ārstniecības personām Personas datu drošība
(Bhaskar et al.) (2020)[57]	Klātienes medicīnisko pakalpojumu aizstāšana ar telemedicīnu.	Infrastruktūras trūkums telemedicīnas nodrošināšanai Vienota pārrobežu regulējuma trūkums. Valodas barjeras pakalpojumu sniegšanai
(Kuziemsky et al.) (2020)[58]	Telemedicīnā izmantojamās sistēmas	Juridiskā regulējuma trūkums datu aizsardzībai specifiski telemedicīnai

[55] Hollander, Judd & Carr, Brendan. (2020). Virtually Perfect? Telemedicine for Covid-19. New England Journal of Medicine. 382. 10.1056/NEJMp2003539.

[56] Kichloo, A., Albosta, M., Dettloff, K., Wani, F., El-Amir, Z., Singh, J., Aljadah, M., Chakinala, R. C., Kanugula, A. K., Solanki, S., & Chugh, S. (2020). Telemedicine, the current COVID-19 pandemic and the future: a narrative review and perspectives moving forward in the USA. Family medicine and community health, 8(3), e000530. Izgūts no https://doi.org/10.1136/fmch-2020-000530, skatīts 20.12.2020.

[57] Bhaskar, S., Bradley, S., Chattu, V. K., Adisesh, A., Nurtazina, A., Kyrykbayeva, S., Sakhamuri, S., Yaya, S., Sunil, T., Thomas, P., Mucci, V., Moguilner, S., Israel-Korn, S., Alacapa, J., Mishra, A., Pandya, S., Schroeder, S., Atreja, A., Banach, M., & Ray, D. (2020). Telemedicine Across the Globe-Position Paper From the COVID-19 Pandemic Health System Resilience PROGRAM (REPROGRAM) International Consortium (Part 1). Frontiers in public health, 8, 556720. Izgūts no https://doi.org/10.3389/fpubh.2020.556720, skatīts 20.12.2020.

[58] Kuziemsky, C. E., Hunter, I., Gogia, S. B., Lyenger, S., Kulatunga, G., Rajput, V., Subbian, V., John, O., Kleber, A., Mandirola, H. F., Florez-Arango, J., Al-Shorbaji, N., Meher, S., Udayasankaran, J. G., & Basu, A. (2020). Ethics in Telehealth: Comparison between Guidelines and Practice-based Experience -the Case for Learning Health Systems. Yearbook of medical informatics, 29(1), 44–50. Izgūts no https://doi.org/10.1055/s-0040-1701976, skatīts 20.12.2020.

Autors un pētījuma publicēšanas gads	Telemedicīnas pakalpojuma veids	Potenciālā riska avots pacientu drošībai
(Hare et al.) (2020)[59]	Klātienes medicīnisko pakalpojumu aizstāšana ar telemedicīnu.	Nepietiekoša atlīdzība ārstniecības personālam kā pakalpojuma kvalitāti negatīvi ietekmējošais faktors Datu drošība un datu uzglabāšanas atļaujas
J.Vidal-Alaball et al. (2020)[60]	Hronisko pacientu veselības stāvokļa uzraudzība mājās	Risks nesankcionētai trešo pušu piekļuvei personas medicīnas datiem

Analizējot veiktos pētījumus, kopš 2001.gada par pacientu drošības riskiem telemedicīnā var ievērot vairākas tendences.

Cilvēcisko faktoru spektrā, zināšanu trūkums, prasmju un izpratnes nepietiekamība veicina to, ka attiecīgās telemedicīnas ierīcēs tiek lietotas citādāk nekā tās ir paredzēts. Nepareizi lietotas iekārtas iespējams var izraisīt nopietnas sekas pacientu veselībai un kaitēt emocionālajai labsajūtai. Turklāt, pētījumos ir identificējama tendence, ka prasmju vai izpratnes trūkums par iekārtas lietošanu var būtiski samazināt pacientu un ārstniecības personāla savstarpējo uzticību un motivāciju izmantot šādas iekārtas.

Pacienta un ārsta klātienes tikšanās, ietverot vizuālo novērošanu un verbālo saziņu tiek uzskatīta par būtisku drošas veselības aprūpes sastāvdaļu. Savukārt, telemedicīna maina veidu, kā veselības aprūpes personāls uztver un mijiedarbojas ar pacientiem, radot nepieciešamību pēc jauniem veidiem un vadlīnijām, kā strādāt veselības aprūpes darbiniekiem.

Saskaņā ar Kruse (et al.) veiktā pētījuma datiem, 2018.gadā[61] tika identificētas galvenās barjeras, kas bremzē telemedicīnas plašāku pielietošanu:

- telemedicīnas pakalpojuma izmaksas;
- ierobežots skaits valsts apmaksātās telemedicīnas konsultāciju;
- tiesiskās saistības un privātuma ierobežojumi;
- datu drošība un novecojušas IKT iekārtas;
- lietderība.

[59] Hare, N., Bansal, P., Bajowala, S. S., Abramson, S. L., Chervinskiy, S., Corriel, R., Hauswirth, D. W., Kakumanu, S., Mehta, R., Rashid, Q., Rupp, M. R., Shih, J., & Mosnaim, G. S. (2020). Work Group Report: COVID-19: Unmasking Telemedicine. The journal of allergy and clinical immunology. In practice, 8(8), 2461–2473.e3. Izgūts no https://doi.org/10.1016/j.jaip.2020.06.038, skatīts 22.12.2020.

[60] Vidal-Alaball J., Acosta-Roja R., Hernandez P.N., Luque U.S., Morrison D., Perez S.N., Perez-Llano J., Verges A.S. Segui L.F. (2020) Telemedicine in face of the COVID-19 pandemic. Atencion Primaria. Vol.52 (6) 418-22.

[61] Kruse, C. S., Karem, P., Shifflett, K., Vegi, L., Ravi, K., Brooks, M., *Evaluating barriers to adopting telemedicine worldwide: A systematic review*. Journal of Telemedicine and Telecare 2018, Vol. 24(1) 4–12. Izgūts no https://journals.sagepub.com/doi/pdf/10.1177/1357633X16674087, skatīts 20.12.2020.

No tehnoloģiju perspektīvas tika konstatēts, ka tehnoloģiju attīstītāji ir piesardzīgi attiecībā uz investīcijām telemedicīnas tehnoloģijās, jo viņiem nav pārliecības par investīciju rentabilitāti un atpelnīšanos. Nākamā barjera ir nedrošu tehnoloģiju izmantošana telemedicīnas pakalpojumu sniegšanā, kas palielina personas datu noplūdes risku. Tiesa gan, pētījumā šo risku vistiešākā veidā saista ar pacienta un personāla digitālajām prasmēm un izpratni par drošību telemedicīnas procesā. Izmaksas kā šķērslis pētnieka Kruse pētījumā, saistītas ar izmaksās, kas nepieciešamas digitālo prasmju uzlabošanai un attiecīgās telemedicīnas vai viedierīces iegādei. Turklāt, izmaksu barjera korelē ar pacientu vecumu, jo vecāki pacienti, jo sliktākas ir to digitālās prasmes uz zemāka motivācija un iespējas veikt investīcijas ierīces iegādei. Tiesa, šajā pētījumā ir uzsvērts, ka "pacientu/iedzīvotāju pārliekas cerības uz telemedicīnu" var būt barjera, ja persona ir uztvērusi, ka telemedicīna ir ātra, lēta un vienkārša, bet realitātē persona tāpat ir sastapusies ar pierakstu sistēmu un gaidīšanu uz konsultāciju.

No drošu tehnoloģiju perspektīvas ir jāpievērš uzmanība šādiem aspektiem[62]:

- Neatbilstoša ierīču kvalitāte un funkcionalitāte neļauj ierīces un pakalpojumus izmantot efektīvi;
- Īpaši jānosaka gadījumi, kādos tehnoloģija un ierīce var kļūt nedroša no iekārtu uzticamības vai pacientu veselības viedokļa;
- Riski nesankcionētai piekļuvei personas elektroniskajiem datiem (EHR) vai medicīniskajā ierīcē uzkrātajiem datiem no trešo personu puses (īpaši gadījumos, kad lietojumprogrammas tiek izmantotas uz atšķirīgi konfigurētiem datoriem, operētājsistēmām)[63].

Tādējādi, telemedicīnas ieviešanas veiksme ir atkarīga no tehniskiem, regulējošiem un finanšu jautājumiem, kas ir jārisina kopā ar cilvēkresursu un organizāciju pārmaiņu vadību[64]. Tomēr, vislielākā uzmanība tiek pievērsta tieši cilvēciskajiem faktoriem, kas attur pacientus no telemedicīnas risinājumu izmantošanas (4. tabula).

4.tabula. Faktoru kopums, kas attur pacientus no iesaistes telemedicīnā, kopsavilkums[65]

Personīgā rīcība un motivācija	
1.1.Motivācijas trūkums	Personīgās motivācijas trūkums, lai saprastu un uzlabotu savas veselības stāvokli.

[62] Vidal-Alaball J., Acosta-Roja R., Hernandez P.N., Luque U.S., Morrison D., Perez S.N., Perez-Llano J., Verges A.S. Segui L.F. (2020) Telemedicine in face of the COVID-19 pandemic. Atencion Primaria. Vol.52 (6) 418-22.

[63] Rezaeibagha F., Mu Y. (2018). Practical and secure telemedicine systems for user mobility. Journal of Biomedical Informatics. Vol 78, pp.24-32.

[64] Faife, D., *Reflections on developing an assistive technology/telecare service as a model for change management, creative thinking and workforce development.* Housing Care Support. 2008;11(4):34–42.

[65] Adaptēts no: O'Connor, S., Hanlon, P., O'Donnell, C. A., Garcia,S., Glanville J., Mair, F.S., *Understanding factors affecting patient and public engagement and recruitment to digital health interventions: a systematic review of qualitative studies*. BMC Medical Informatics and Decision Making (2016) 16:120 DOI 10.1186/s12911-016-0359-3.

1.2.Izpratne un sapratne	Pacients neizprot vai nesaprot, kā telemedicīna vai digitālā medicīna varētu palīdzēt.
1.3.Personīgā rīcība	Pacients nav informēts un/vai zinošs par alternatīviem veidiem, kā dokumentēt informāciju par veselības stāvokli un slimībām.
Personīgā dzīve un vērtības	
1.4. Personīgais dzīvesveids	Aizņemts dzīvesveids ar vairākām, konkurējošām prioritātēm.
1.5. Prasmes un iekārtas	Pacientam ir sliktas/nepietiekamas digitālās prasmes. Pacientam nav piekļuves iekārtās un ierīcēm un internetam. Pacients nevar atļauties telemedicīnas izmaksas.
1.6.Privātums un drošība	Bažas par drošību un telemedicīnas privātumu vai mijiedarbību.
Iesaistīšanās un veselības veicināšana	
1.7.Veselības veicināšanas politika	Pacientam ir grūtības saprast veselības veicināšanas nozīmi.
1.8.Tiešs atbalsts	Pacientam ir ģimenes locekļu, draugu un paziņu atbalsta trūkums.
1.9. Personīgs padoms	Pacientam ir atbalsta un rekomendāciju trūkums no drošiem, uzticamiem avotiem.
1.10. Veselības aprūpes personāla iedrošinājums	Pacients izjūt iedrošinājumu trūkumu no veselības aprūpes personāla puses
“Telemedicīnas” kvalitāte	
1.11. Negatīva telemedicīnas pieredze (kvalitāte, informācija, mijiedarbība)	Pacients neizjūt telemedicīnu – nepietiekama telemedicīnas komponente pakalpojuma sniegšanā; Pacienta uzticības trūkums telemedicīnas pakalpojumam; Telemedicīna tiek uztverta kā aizskaroša, pazemojoša.
1.12. “Telemedicīnas” izmantošana	Telemedicīnas pakalpojums ir grūti izmantojams.

Faktoru kopums, kas attur pacientus no telemedicīnas izmantošanas ir plašs un aptver gan pacientu iepriekšējo pieredze, gan izglītību, gan arī sociālos faktorus.

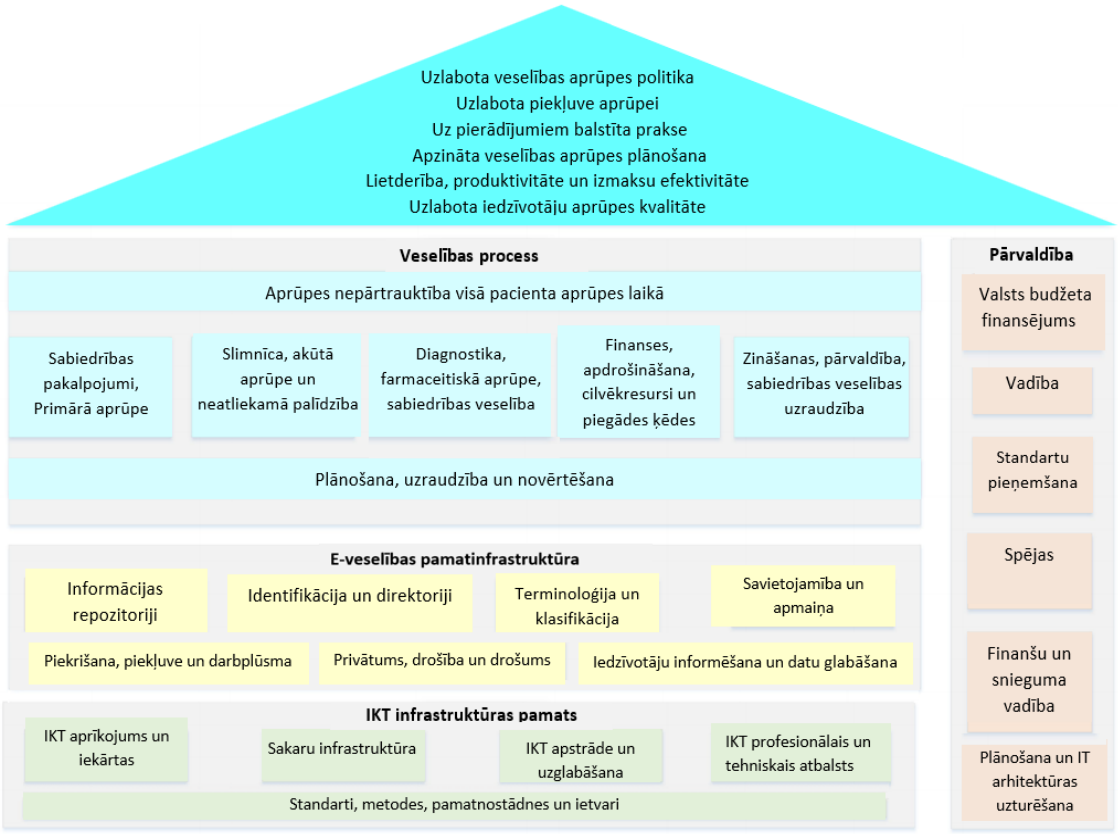
Rekomendācija:

1. Kultūras šķēršļu pārvarēšanai:
   - Veidot komunikācijas un izglītojošas kampaņas par telemedicīnas ieguvumiem un pakalpojuma drošības nosacījumiem;
2. Cilvēcisko faktoru pārvarēšanai:
   - Stiprināt cilvēkresursus veselības aprūpes jomā, izstrādājot vadlīnijas, rekomendācijas un labās prakses piemērus telemedicīnas personālam programmatūras un aparatūras drošai lietošanai;
   - Integrēt praktiskas telemedicīnas zināšanas un prasmes medicīnas studiju procesā dažādos izglītības līmeņos.
   - Izglītot medicīnas personālu, organizējot kursus un seminārus par telemedicīnas rīku drošu izmantošanu.
3. Organizatorisko šķēršļu pārvarēšanai:
   - Telemedicīnas regulējuma paplašināšana, veidojot tiesību aktus, kuros ir paredzētas gan pakalpojumu kvalitātes, gan drošības prasības;
   - Publiskās - privātās partnerības sadarbības izmantošana, lai mudinātu privāto sektoru iesaistīties telemedicīnas attīstībā;
4. Tehnisko un drošības šķēršļu pārvarēšanai:
   - Palielināt valsts atbalstu IKT jomai tieši telemedicīnas attīstībai;
   - Definēt telemedicīnas pakalpojumus IKT drošuma prasības.

5 Telemedicīnas drošums un noturība

Tehnoloģiski telemedicīnai izvirza šādus nosacījumus:

a) lietojamība - lietotne, platforma ir ērti lietojama, gan ārstniecības personālam, gan pacientiem;
b) izmaksas un saderība – telemedicīnas infrastruktūras izmaksas ir pieejamas plašai sabiedrībai un infrastruktūras elementi ir saderīgi ar citiem infrastruktūras elementiem;
c) sniegums – telemedicīnā izmantotā infrastruktūra nodrošina nepieciešamo video un akustiskokvalitāti un izšķirtspēju;
d) privātums – tiek nodrošināta pacientu datu aizsardzība.



7.attēls. Telemedicīnas tehnoloģiskais ietvars[66]

Eiropas Savienības Kiberdrošības aģentūra (ENISA - *European Union Agency for Cybersecurity*) 2020. gada oktobrī publicētajā ziņojumā par būtiskākajiem kiberdrošības incidentiem no 2019. gada janvāra līdz 2020. gada aprīlim[67] norāda, ka COVID-19 pandēmijās laikā veselības aprūpe ir kļuvusi par vienu no krustiskākajam industrijām kiberdrošības jomā. Šifrējošo vīrusu uzbrukumu skaits veselības aprūpei jau agrāk ir bijis augsts un vēl vairāk pieaudzis pandēmijas laikā.

Brno universitātes slimnīca, kas ir otra lielākā slimnīca Čehijas Republikā, 2020. gada martā smagi cieta kiberuzbrukumā[68]. Slimnīcai nācās izslēgt visu savu IT datortīklu un pat atlikt pacientu plānotās operācijas. Minētais incidents kalpoja par pamatu Europas Parlamenta

[66] Taylor A., ,Morris G., Tieman J., Currow D., Kidd M,Carati C. (2015) Building an Architectural Component Model for a Telehealth Service. E-Health Telecommunication Systems and Networks, 2015, 4, 35-44 Published Online September 2015 in SciRes. Izgūts no http://www.scirp.org/journal/etsnhttp://dx.doi.org/10.4236/etsn.2015.4300, skatīts 10.12.2020.

[67] "*ENISA Threat Landscape 2020 – Main Incidents*". (24.11.2020) Izgūts no https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-main-incidents, skatīts 24.11.2020.

[68] "*Brno University Hospital in Czech Republic Suffers Cyberattack During COVID-19 Outbreak*" (2020). Izgūts no https://www.securitymagazine.com/articles/91921-brno-university-hospital-in-czech-republic-suffers-cyberattack-during-covid-19-outbreak, skatīts 24.11.2020.

deputāta L.Mandla rakstiskam jautājumam[69] 2020. gada 19. maijā par Eiropas Savienības[70] kiberdrošības spējām un 2020. gada 22. septembra Eiropas iekšējā tirgus komisāra T.Bretona atbildei[71], kurā viņš paziņo par jaunas darba grupas izveidi un Eiropas kiberdrošības institūciju uzlaboto sadarbības modeli. Tai pat laikā 2020. gada 13. martā Hospitālis arī savā Twitter vietnē publicēja ierakstu, ka hospitālis (kurš ir saistīts ar Covid-19 izplatības mazināšanu kā Covid-19 testa centrs) ir pakļauts kiberuzbrukumam. Hospitāļa pamatfunkcijas tiek uzturētas, bet plānotās medicīniskās manipulācijas ir atliktas, akūtās medicīniskās manipulācijas tiek uzturētas balstoties uz nepieciešamību. Brno hospitāļu sistēmas bija nespējīgas veikt to pamatuzdevumu.[72] Uzbrucēji, iespējams, izmantoja pikšķerēšanas paņēmienu, lai piekļūtu slimnīcas tīklam. Pēc tam tika veikts ļaunprātīga datu šifrēšana lietojot kriptovīrusu Defray. Lai atjaunotu hopitāli pilnā darbības kapacitātē bija nepieciešama nedēļa. Saskaņā ar uzbrukuma analīzi, no incidenta seku likvidētājiem, bija veikts intensīvs monitorings par hospitāļa darbību un personālu. Uzbrucēju darbības veids liecināja par organizētu kriminālu grupu.[73]

Ieteikumi, lai no šādas situācijas izvairītos nākotnē. Šāda uzbrukuma veida preventīvā metodoloģija sagaida no organizācijas daudzpusīgu izglītošanas darbu, lai:

- Izglītotu darbiniekus par pikšķerēšanu un sociālās inženierijas uzbrukuma metodēm;
- Izglītotu IT personālu par to kā tiek veikti kibernoziegumi;
- Izglītot IT un administratīvo personālu par digitālās kriminālistikas gatavības nozīmi ļaunatūras radīto seku mazināšanā;

Tāpat organizācijai vēlams izvērtēt kritisko datu rezerves kopiju veidošanas un glabāšanas opcijas ārpus organizācijas un datu pārraides tīklu segmentāciju.

Kibernoziedznieki uzlauza Somijas psihoterapijas uzņēmuma Vastaamo elektronisko datu bāzi ar vairāk kā 40,000 pacientu datiem un šantažējuši pacientus, pieprasot izpirkuma maksas 200-500 EUR apmērā no katra pacienta. Minētā incidenta rezultātā tika publiskoti Internetā brīvi pieejami arī 300 pacientu dati (EHR). Vastaamo preses relīzē 2020. gada 26. oktobrī uzņēmuma direktoru padome atzīst un atvainojas, ka ielaušanās ir bijusi iespējama informācijas drošības pārvaldības trūkumu dēļ.[74]

---

[69] *"EU cyber defence during and beyond the COVID-19 pandemic"*. Izgūts no https://www.europarl.europa.eu/doceo/document/E-9-2020-003061_EN.html, skatīts 24.11.2020.

[70] "Personal data of 16 million Brazilian COVID-19 patients exposed online". Izgūts no https://www.zdnet.com/article/personal-data-of-16-million-brazilian-covid-19-patients-exposed-online/, skatīts 30.11.2020.

[71] *Answer given by Mr Breton on behalf of the European Commission*. Izgūts no https://www.europarl.europa.eu/doceo/document/E-9-2020-003061-ASW_EN.html, skatīts 22.09.2020.

[72] Twitter. Izgūts no https://twitter.com/FNBrno/status/1238465484053524482, skatīts 24.11.2020.

[73] Horák, J. (20.03.2020) *Na nemocnici v Brně zaútočil vyděračský virus, špitál povolal krizového IT manažera.* Izgūts no https://zpravy.aktualne.cz/, skatīts 24.11.2020.

[74] "*Press release October 26, 2020: Investigation into the Vastaamo data system break-in – shortcomings in information security in the background*" Izgūts no https://vastaamo.fi/ajankohtaista/en.html, skatīts 25.11.2020.

2020. gada 10.septembra agrā rīta, Diseldorfas Universitātes slimnīcas iekšējie informācijas tīkli pārstāja pildīt savas pamatfunkcijas – atspoguļot plānotās medicīniskās manipulācijas, fiksēt dienas stacionāra pacientu pieņemšanu, un neatliekamās palīdzības sniegšana, kā arī nodrošināt pacientu atveseļošanās atbalsta funkciju. Slimnīcas vadība datu un informācijas atjaunošanas procesā iesaistīja IT ekspertus un likumsargus. Vēl 14.septembrī slimnīcas darbība nebija atjaunota, taču tika norādīts, ka dati nav iznīcināti un ir iesaistītas atbildīgās iestādes. 17.septembrī tika publicēts sekojošs atzinums par cēloni.Saskaņā ar izmeklēšanas rezultātiem, iemesls kādēļ hakeri spēja veikt šo uzbrukumu bija viņu spēja izmantot programmatūras ievainojamību. Slimnīca savā IT vidē lietoja programmatūru, kurai bija pieļauta ievainojamība no tās ražotāja puses. Pirms programatūras ražotājs spēja novērst problēmas un publicēt programmatūras atjauninājumu, pagāja pietiekami ilgs laika posms, lai sistēma varētu tiktu uzlauzta. Līdz ar to sistēma nefunkcionēja un dati nebija pieejami. Diseldorfas Universitātes slimnīcas informācijas tīkls un tā iekārtas zaudēja veiktspēju uzturēt visas nepieciešamās funkcijas, kuru pamatuzdevums sniegt atbalstu medicīnas un telemedicīnas pakalpojumiem, tāpat tika zaudēta pieeja visu tipu datiem. Atsaucoties uz Heise.de publicēto informāciju[75], hakeru grupējums, kuru Vācijas likumsargi saista ar Krieviju, iefiltrēja "DoppelPaymer" ar kura palīdzību tika ievainota programma. Iepriekš minēta darbība bija veikta pirms 2019./2020. gadu mijas. Slimnīca pilnībā atjaunoja savu darbību sākot ar 2020. gada 23. septembri.

Ieteikumi, lai no šādas situācijas izvairītos nākotnē. Iebrukuma metodoloģija norāda uz iespējamo informācijas apmaiņu par virtualizācijas programmatūras CITRIX (CVE-2019-19781) ievainojamību ilgi pirms tā iespējams bija pieejama neindeksētās interneta vietnēs. Tāpat tas norāda ka Universitātes IT personāls nesekoja informācijas plūsmai horizontālā līmenī, paļaujoties, ka preventīvie mēri ir pietiekoši. Universitātes vadība nebija iedzīvinājusi kontroles mehānismu, kas veic preventīvu funkciju, ja IT personāls neveic kontroli pār informācijas plūsmu organizācijā. Tāpat no sekojošā incidenta izriet, ka testa funkcija un auditācijaspierakstu analīze ir nepietiekama un nav iedzīvināts mehānisms, kurš ļauj personālam fokusēt savu uzmanību uz iepriekš ar AI atlasītajiem auditācijasierakstiem. Caurmērā tie ir aptuveni 2% no kopējo auditācijaspierakstu apjoma. Tāpat šis incidents liecina par nepilnīgu heiristiku un citu filtru ieviešanu un izmantošanu.

2020. gada novembrī ZDNet rakstīja, ka Brazīlijā vairāk kā 16 miljonu personu dati ir noplūduši. Par iemeslu noplūdei kalpojusi kāda darbinieka neuzmanība padarot pieejamus lietotāju vārdus, paroles, piekļuves kodus un citu sensitīvu informāciju programmatūras izstrādes platformā GitHub.

Plaši pielietota ikdienas saziņas tehnoloģija WhatsApp ir ienākusi veselības aprūpē kā telemedicīnas[76] rīks, neskatoties uz to, ka paši medicīnas darbinieki pētījuma dalībnieki atzīst, ka WhatsApp nav drošs. 2020. gada februārī Eiropas Komisija darbiniekiem ieteica lietot

[75] Düsseldorf, U. (11.09.2020). *Update 16 Uhr - Uniklinik Düsseldorf: Massiver Netzwerkausfall.* Izgūts no https://www.uniklinik-duesseldorf.de/ueber-uns/pressemitteilungen/detail/update-16-uhr-uniklinik-duesseldorf-massiver-netzwerkausfall, Universitätsklinikum Düsseldorf, skatīts 25.11.2020.

[76] De Benedictis, A., Lettieri, E., Masella, C., Gastaldi, L., Macchini, G., Santu, C., & Tartaglini, D. (2019). *WhatsApp in hospital? An empirical investigation of individual and organizational determinants to use.* PloS one, 14(1), e0209873.

Signal[77] saziņas rīku, nevis WhatsApp vai Apple iMessage. Plašu WhatsApp pielietojumu Latvijas ģimenes ārstu praksēs apstiprina arī intervijās sniegtās atbildes.

Telemedicīna ir joma, kas aizvien plašāk attīstās jo īpaši COVID-19 pandēmijas laikā un ietver gan speciālās medicīnas iekārtas, gan pacienta individuāli valkājamas ierīces (piemēram, Holtera monitors, viedais glikozes mērītājs), gan periodiski izmantojamas iekārtas (piemēram, viedais asinsspiediena mērītājs, viedie svari), gan saziņas programmatūras un citus IKT rīkus izmantojamus veselības aprūpes pakalpojumu attālinātai nodrošināšanai un pacientu veselības stāvokļa uzraudzībai [78].

Medicīnas iekārtu saturošu datortīklu risku vadības standarts "IEC 80001-1:2010 *Application of risk management for IT-networks incorporating medical devices — Part 1: Roles, responsibilities and activities*" nosaka lomas, pienākumus un darbības, kas nepieciešamas datortīklu pārvaldībai, kuros tiek lietotas medicīnas iekārtas. IEC 80001-1: 2010 attiecas uz atbildīgajām organizācijām, medicīnas ierīču ražotājiem un citu IKT pakalpojumu sniedzējiem, taču neattiecas uz lietojumiem personīgai lietošanai. ISO mājās lapā tiek minēts, ka IEC 80001-1:2010 standarts tiek pārskatīts un tiks aizvietots ar IEC/DIS 80001-1[79].

IKT pārvaldībā Latvijā tiek plaši pielietots LVS EN ISO/IEC 27001 "Informācijas tehnloģija. Drošības paņēmieni. Informācijas drošības pārvaldības sistēmas. Prasības (ISO/IEC 27001:2013 ieskaitot Cor 1:2014 un Cor 2:2015)". Standarta popularitāti apliecina iespēja starptautiski sertificēt organizācijas vai uzņēmumus atbilstoši šim standartam. Valsts aģentūras "Latvijas Nacionālais akreditācijas birojs" 2020. gada decembrī ir publicētas 4 (četras) institūcijas[80], kuras ir akreditētas LVS ISO/IEC 27001:2013 auditam un sertifikācijai. Medicīnas jomā Latvijā atbilstoši šim standartam 2015. gadā ir sertificējusies[81] Valsts zāļu aģentūra.

Starptautiskās kriminālpolicijas organizācijas Interpol Ģenerālsekretārs Jurgens Stoks preses paziņojumā[82] 2020. gada augustā norāda uz satraucoši pieaugošo kiberuzbrukumu skaitu Covid-19 pandēmijas laikā "Kibernoziedznieki attīsta un pastiprina uzbrukumus satraucošā tempā, izmantojot Covid-19 radītās bailes un nenoteiktību sakarā ar nestabilo sociālo un

---

[77] "*EU Commission to staff: Switch to Signal messaging app"* Izgūts no https://www.politico.eu/article/eu-commission-to-staff-switch-to-signal-messaging-app/ skatīts 25.11.2020.

[78] Vidal-Alaball J., Acosta-Roja R., Hernandez P.N., Luque U.S., Morrison D., Perez S.N., Perez-Llano J., Verges A.S. Segui L.F. (2020) Telemedicine in face of the COVID-19 pandemic. Atencion Primaria. Vol.52 (6) 418-22.

[79] "*IEC/DIS 80001-1. Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software — Part 1: Application of risk management"*, Izgūts no https://www.iso.org/standard/72026.html, skatīts 27.11.2020.

[80] *"Akreditētās institūcijas".* Izgūts no https://www.latak.gov.lv/index.php?option=com_institucijas&view=institucijas&task=myForm&Itemid=151&lang=lv, skatīts 24.11.2020.

[81] "*Noslēdzies ISO 9001 un ISO 27001 sertifikācijas uzraudzības audits Zāļu valsts aģentūrā"* Izgūts no https://www.zva.gov.lv/lv/jaunumi-un-publikacijas/jaunumi/nosledzies-iso-9001-un-iso-27001-sertifikacijas-uzraudzibas-audits-zalu-valsts-agentura-0, skatīts 27.11.2020.

[82] *"INTERPOL report shows alarming rate of cyberattacks during COVID-19",*Izgūts no https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19, skatīts 27.11.2020.

ekonomisko situāciju". Interpols identificējis šādus būtiskākos uzbrukuma veidus pandēmijas laikā:

- Pikšķerēšana – uzbrukuma veids, kas, izmantojot e-pastu vai ziņu apmaiņas programmas, mēģina jūs apmuļķot un mudina veikt darbības, kas kaitē jums pašiem, piemēram, nospiest kādu saiti, atklāt savu paroli vai atvērt inficētu e-pasta pielikumu;
- Šifrējošie vīrusi – ļaunatūra, kas šobrīd aktīvi izplatās internetā, apdraudot upuru dokumentus un citus failus;
- Datu ieguves ļaunatūra – ļaunatūra, kura vāc tādu svarīgu informāciju no upura kā banku pieejas, saglabātus lietotāja vārdus, paroles, u.c.
- Ļaunprātīgi izveidoti domēni, dezinformācija un mājas lapas, kuros iemānīt upuri un mēģināt inficēt ar ļaunatūru.

CERT.LV (Informācijas tehnoloģiju drošības incidentu novēršanas institūcija) 2020. gadā "Kiberlaikapstākļu" un "OUCH!" publikācijās norāda uz Interpol minētajiem kibernoziegumu veidiem, tos precizējot Latvijas iesaistīto banku un citu komersantu vārdiem.

5.1 Drošības un noturības prasības telemedicīnas servisiem

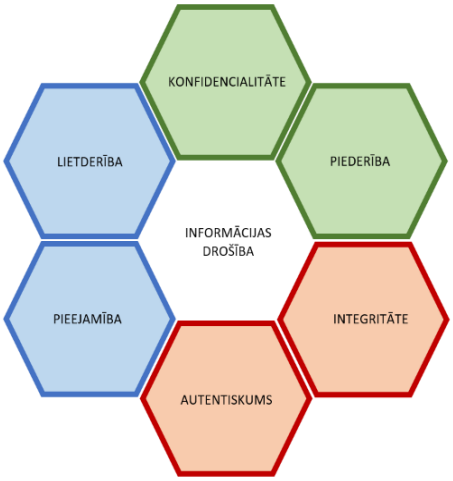
Drošības un noturības prasības telemedicīnā primāri izriet no pielietotās IKT drošības un noturības, jo attālinātie medicīnas pakalpojumi tiek sniegti IKT vidē. Telemedicīnas sistēmu izaicinājums ir savienot medicīnas riskus IKT vidē, pie tam apzinot tehnoloģisko risinājumu veiktspējas fluktuācijas, kuras, savukārt, var ietekmēt medicīnas datu kvalitāti un pat pašu attālināto veselības aprūpi[83].

Latvijas Ministru kabineta noteikumos Nr.442. "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām"[84] 13.panta piektā daļā nosaka, ka sistēmu drošības risku izvērtē attiecībā uz pieejamības, integritātes un konfidencialitātes risku vērtējumu. Zinātniskā literatūrā mēdz apskatīt paplašinātu pamatprasību kopu atbilstoši Pārkera heksādes kategorijām[85]: konfidencialitāte, piederība, integritāte, autentiskums, pieejamība un lietderība.

[83] Larburu, N., Bults, R. G., & Hermens, H. J. (2014, June). *Making medical treatments resilient to technological disruptions in telemedicine systems.* In IEEE-EMBS International Conference on Biomedical and Health Informatics (BHI) (pp. 285-288). IEEE.

[84] Ministru kabinets (2015). Ministru kabineta noteikumi Nr.442. Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām. Pieņemti 28.07.2015. https://likumi.lv/ta/id/275671-kartiba-kada-tiek-nodrosinata-informacijas-un-komunikacijas-tehnologiju-sistemu-atbilstiba-minimalajam-drosibas-prasibam, skatīts 28.11.2020.

[85] Pender-Bey, G. (2016). *The Parkerian Hexad.* Information Security Program at Lewis University.



8.attēls. Pārkera heksādes kategorijas.

Ņemot vērā strukturētas attālinātās intervijas rezultātus ar ģimenes ārstiem, tika konstatēts, ka daudzi no viņiem lieto tiešsaistes rīkus tādus kā ZOOM, WebEx, WhatsApp, Signal saziņai ar pacientu. Tomēr, šo rīku izmantošanā ir arī identificēti:

- konfidencialitātes riski saistībā ar pacientu datu nesankcionētu izmantošanu,
- pārliecības riski par pacienta datu autentiskumu (piemēram, vai tiešsaistes konsultācijai ir pieslēgusies atbilstošā persona, kur klātienes konsultācijā par to var gūt pārliecību pieprasot uzrādīt personu apliecinošu dokumentu);
- pieejamības riski no pakalpojumu sniegšanas viedokļa.

Projekta ARTSS ietvaros ir veikta padziļināta drošības risku analīze.

Pamatojoties uz pašreizējiem pētījumiem un pieejamo lietotņu analīzi, autoru ieteikums ir veselības aprūpē pašreizējā brīdī izmantot Zoom programmatūras speciāli veselības aprūpei paredzēto moduli. WebEx nodrošina pārāk šaurus datu centrus bez iespējām apstrādāt sapulču datus. Ziņojumapmaiņai ne lietotne WhatsApp, ne Signal nav piemērotas telemedicīnas vajadzībām, to izmantošana potenciāli pārkāpj Vispārīgās datu aizsardzības regulas nosacījumus (GDPR) (nedodot iespēju lietotājam pārliecināties par personīgā informācijas uzglabāšanu un apstrādi). Kā alternatīvu var izpētīt Tiger Connect (https://tigerconnect.com/about/) vai izveidot vietējo ziņojumapmaiņas lietotni, kas varētu iekļaut pašreizējo ziņojumapmaiņas lietotņu labākos aspektus un kuras ieviešanā tiktu ņemti vērā Latvijas Republikas un Vispārīgās datu aizsardzības regulas likumdošanas aizsardzības pasākumi. Tomēr, ir nepieciešams fiziski novērtēt Zoom un potenciāli Tiger Connect. Šādam novērtējumam ir nepieciešama sadarbība ar attiecīgo produktu īpašniekiem/ izstrādātājiem un līguma noslēgšana par to produktu testēšanu.

Videokonferenču nodrošināšanai ir pieejami vairāki risinājumi, kas varēti tikt lietoti pacienta un ārsta saziņai tiešsaistē: Zoom, WebEx, WhatsApp, Telegram, Signal, Skype, Tiger Connect. Šajā pārskatā galvenā uzmanība tiks pievērsta Zoom, WebEx, WhatsApp un Signal programmām, kā tas tika prasīts no projekta atbildīgo iestāžu puses.

Viens no rādītājiem, ko var izvērtēt, lai noteiktu konkrētas lietojumprogrammas uzticamību, ir tas, cik labi programmatūra/aparatūras ražotājs ir izstrādājis atjauninājumus.

Otrkārt, vai ražotāja ieviestie drošības pasākumi vai drošības risinājumi apgrūtina lietotāju pieredzi un ierobežo produkta lietošanas mērķi.

Lietojumprogramma Zoom piedāvā divus dažādus risinājumus lietotājiem – vienu, kur gala lietotājs var mainīt drošības iestatījumus, un otru, kur gala lietotājs nevar mainīt drošības un HIPAA atbilstības iestatījumus. Pieminētais otrais variants ir Zoom izstrādātāju pielāgots konkrētai medicīnas pakalpojumu sniedzēju grupai, vai arī to pārvalda individuāls administrators konkrētai struktūrvienībai, kurš tad ir arī ieteikts telemedicīnas pakalpojumam Latvijā

Zoom nodrošina pielāgotus produktus konkrētu reģionu vajadzībām – ES, ASV. Atbilstoši reģiona prasībām ir ieviesti uzstādījumi Zoom programmatūras darbības aprakstā:

- HIPAA prasību funkcionālā īstenošana Zoom vidē (aplūkots 2020.g. 31. oktobrī: https://zoom.us/docs/doc/Zoom-hipaa.pdf)
- FERPA prasību funkcionālā īstenošana Zoom vidē (aplūkots 2020.g. 31. oktobrī: https://zoom.us/docs/doc/FERPA%20Guide.pdf)
- PHIPA prasību funkcionālā īstenošana Zoom vidē (aplūkots 2020.g. 31. oktobrī: https://zoom.us/docs/doc/PIPEDA_PHIPA%20Canadian%20Public%20Information%20Compliance%20Guide.pdf)
- GDPR prasību funkcionālā īstenošana Zoom vidē (aplūkots 2020.g. 31. oktobrī: https://zoom.us/gdpr)

5.1.1 Zoom

Funkcionalitātes "E2E šifrēšana Zoom sanāksmēm" Zoom vidē , 2.3. versija ir publicēta 2020. gada 14. oktobrī [86]. Kad Zoom sanāksmes klients (Zoom application) piekļūst Zoom sanāksmei, tas saņem 256 bitu atslēgu (ko izveido un nosūta Zoom serveris), kuru izmanto, lai iegūtu plūsmas atslēgu, apvienojot sanāksmes atslēgu ar neslēptu straumes ID, izmantojot HMAC funkcija. Vienu no HMAC definīcijām sniedz Microsoft, (Microsoft):

"Hash" balstītu ziņojumu autentifikācijas kodu (HMAC) var izmantot, lai noteiktu, vai ziņojums, kas nosūtīts pa nedrošu kanālu, ir sagrozīts, ar nosacījumu, ka sūtītājs un saņēmējs koplieto slepeno atslēgu. Sūtītājs aprēķina sākotnējo datu jaukšanas vērtību un nosūta gan sākotnējos datus, gan HMAC kā vienu ziņojumu. Uztvērējs pārrēķina saņemtā ziņojuma jaukšanas vērtību un pārbauda, vai aprēķinātā jaukšanas vērtība sakrīt ar pārraidītās jaukšanas vērtību."

[86] Josh Blum, S. B., Gal, O., Krohn, M., Len, J., Lyons, K., Marcedone, A., Maxim, M., Mou, M. E., O'Connor, J., Steele, M., Green, M., Kissner, L., Stamos, A., (14.10.2020.). *E2E Encryptoon for Zoom Meetings.* Z. V. Communications. Izgūts no https://github.com/zoom/zoom-e2e-whitepaper/blob/master/archive/zoom_e2e_v2_3.pdf, skatīts 24.10.2020.

Lai mazinātu iekšējos/ārējos draudus, Zoom izmanto CIA triādi- konfidencialitāti, integritāti un pieejamību (*confidentiality, integrity, availability*) pielāgotus pamatprincipus[87]:

• "Konfidencialitāte: Tikai autorizētiem sanāksmes dalībniekiem ir piekļuve sanāksmes audio un video straumēm. Personām, kas izraidītas no sanāksmes, vairs nav tai piekļuves.

• Integritāte: Personām, kas netiek ielaistas sapulcē, nav iespējas ietekmēt sapulces saturu.

• Pieejamība: Kad autorizēti sapulces dalībnieki veic ļaunprātīgas darbības, ir pieejams efektīvs mehānisms, kā par tiem ziņot Zoom drošības komandai, lai palīdzētu novērst turpmākas ļaunprātīgas darbības tādējādi reizē nodrošinot arī programmatūras pieejamību."

Zoom nodrošina sava produkta iespējas, kā arī HIPAA (Veselības apdrošināšanas pārnesamības un atbildības noteikumi[88], Attiecībā uz atbilstību HIPAA Zoom sniedz šādu kopsavilkumu [89] (5. tabula).

5.tabula. ZOOM drošības izvērtējums

HIPAA standarts	Kā Zoom atbalsta standartu
Piekļuves kontrole: ● Īstenot tehnisko politiku un procedūras elektroniskām informācijas sistēmām, kuras saglabāt elektroniski aizsargātu veselību informācija, kas ļauj piekļūt tikai pilnvarotas personas vai programmatūras programmas ● Unikāla lietotāja identifikācija: piešķiriet unikālu nosaukums un / vai numurs identifikācijai un lietotāja identitātes izsekošana/-ai ● Ārkārtas piekļuves procedūra: izveidojiet (un pēc nepieciešamības īstenojiet) procedūras, lai saņemtu nepieciešamo Elektronisko medicīnas ierakstu, krīzes laikā. ● Automātiska atvienošanās: ieviest elektronisko procedūras, kas izbeidz	● Dati kustībā tiek šifrēti lietojuma slānis, izmantojot uzlaboto šifrēšanu Standarts (AES). ● Daudzslāņu piekļuves kontroles ieviešana īpašniekam, administratoram un sapulces dalībniekiem ● Piekļuve tīmeklim un Zoom lietotājprogrammai aizsargā pārbaudīta e-pasta adrese un parole ● Pieeja sapulcei ir aizsargāta ar paroli un/vai uzgaidāmo telpu ● Zoom nepublicē publiskā telpā informāciju par sapulcēm; ● Zoom īsteno duplicētu un sadalītu arhitektūru, lai pieejamība programmai un nepieciešamajiem resursiem būtu augsta un duplicēta.

[87] Josh Blum, S. B., Gal, O., Krohn, M., Len, J., Lyons, K., Marcedone, A., Maxim, M., Mou, M. E., O'Connor, J., Steele, M., Green, M., Kissner, L., Stamos, A., (14.10.2020.). *E2E Encryptoon for Zoom Meetings.* Z. V. Communications. Izgūts no https://github.com/zoom/zoom-e2e-whitepaper/blob/master/archive/zoom_e2e_v2_3.pdf, skatīts 31.10.2020.

[88] Plašāka informācija https://www.healthit.gov/topic/privacy-security-and-hipaa/hipaa-basics, skatīts 31.10.2020.

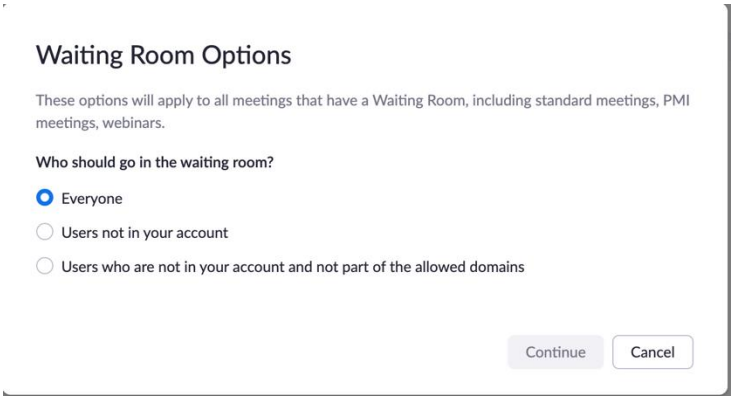
[89] Zoom. (2020a). *New updates for April 16, 2020.* Zoom. Izgūts no https://support.zoom.us/hc/en-us/articles/360041994612-New-updates-for-April-16-2020, skatīts 31.10.2020.

HIPAA standarts	Kā Zoom atbalsta standartu
elektronisko sesiju pēc iepriekš noteikta laika posma neaktivitātes. ● Šifrēšana un Atšifrēšana: ieviest mehānismu, kurš atļauj šifrēt un atšifrēt elektronisko medicīnisko ierakstu (EHR), kurš ir aizsargāts.	● Zoom lietotāj organizācija/uzņēmums var izvēlēties Zoom datu centru, datu apstrādei sapulces laikā saistītiem organizācijas/uzņēmuma kontu. Šie uzstādījums neizmainīs datu glabāšanas/arhivācijas lokāciju. ● Zoom sapulces vadītājs var ērti vai nu atvienot no sapulces dalībniekus, vai pārtraukt sapulces sesijas. ● Sapulces vadītājs var noslēgt notiekošo sapulci (lai ne tikai nokavējošās personas, bet arī trešās puses personas nevar pieslēgties sapulcei) ● Sapulces beidzas automātiski atbilstoši noteiktajam laikam (timeouts). ● Zoom Privātuma funkcijas ļauj kontrolēt sekojošas funkcionalitātes: pieeju sapulcei, gan individuāli, gan kā grupai; lietojot uzgaidāmo telpu; lietojot piespiedu tikšanās testa pieejas kodus; lietojot noslēgtas tikšanās telpas funkciju.
Audita kontrole ● Izstrādāt/ieviest aparatūras, programmatūras līmenī un/vai procesuālā līmenī, kuru uzdevums reģistrēt un pārbaudīt informācijas sistēmu darbības, kurās glabā vai lieto (ar likumu) aizsargāto digitālā formātā medicīnu saistītu informāciju	● Zoom sapulču ģenerētie dati kuri ir kustībā (*data in motion*) via Zoom aizsargātā sadalītā infrastruktūrā ● Pakalpojumu kvalitātes (kuri ir saistīti ar audio un pakalpojuma kvalitāti) nolūkos Zoom vides savienojuma punkti ir pierakstīti auditācijas pierakstos. ● Zoom kontu administratoriem ir nodrošināta droša pieeja, lai pārvaldītu indivīdus, grupas, vai organizācijas.
Integritāte: ● Īstenot vadlīnijas un procedūras, lai aizsargātu EHR ar medicīnu saistīto (ar likumu) aizsargāto informāciju no neatļautām izmaiņām vai to iznīcināšanu.	● Aizsardzība, kura balstās daudzslāņu integrācijā un kurai ir piemērota arhitektūra kura aizsargā datu līmeni un pakalpojuma līmeni. ● Ieviesta kontrole (pārvaldība), kura aizsargā un šifrē sapulču datus.
Integritātes mehānisms:	

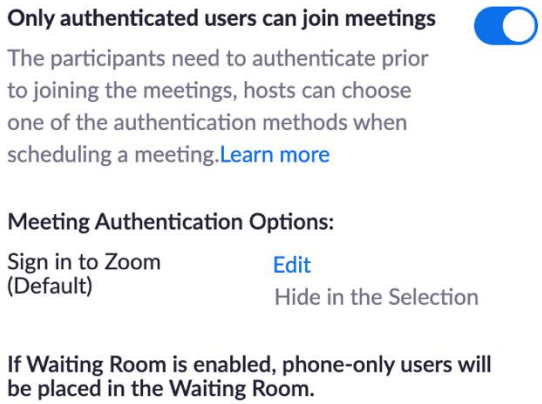
HIPAA standarts	Kā Zoom atbalsta standartu
● Ieviest (programatūriskā/iekārtu līmenī/-os) autentifikācijas mehānismu, kurš attiecināts digitālajiem (ar likumu aizsargātiem) medicīnisko datiem. ● Ieviest metodoloģiju/-as kuras (savstarpēji) apstiprina, ka informācija nav tikusi iznīcināta vai izmainīta.	● (Zoom) lietotnes izpildāmie faili ir digitāli parakstīti. ● Datu savienojumi izmanto TLS 1.2 šifrēšanu un PKI sertifikātus, kuri ir tikuši uzdoti no uzticama privāta sertifikātu pārvaldītāja. (šāds ieraksts iepriekš nav tulkots) ● Pieeja internetam un (Zoom) aplikācijai ir aizsargāta var verificētu e-pasta adresi un paroli
Personas vai organizācijas autentifikācija: ● Ieviest pārbaudi, ka persona vai organizācija/uzņēmums kurš vēlas īstenot piekļuvi ir tas par ko sevi apliecina..	● Pieeja internetam un (Zoom) aplikācijai ir aizsargāta var verificētu e-pasta adresi un paroli. ● (Zoom) Sapulces vadītājam ir jāpieslēdzas Zoom (lietotnei) ar unikālu e-pastu un (Zoom) konta parole. ● (Zoom) Sapulces vadītājs var bloķēt sapulces dalībnieka piekļuvi pie ekrāna koplietošanas, lai neatļautu (patvaļīgu) ar (Operētājsistēmas) darbavirsmas vai mapes dalīšanos. ● Zoom Privātuma funkcionalitāte atļauj pieeju pie sapulces gan kā indivīdam, gan kā organizācijai/uzņēmumam – lietojot uzgaidāmās telpas, pieprasītos reģistrācijas kodus, un noslēgtas (bloķētas) uzgaidāmās telpas iestatījumus.
Pārraides drošība: ● Aizsargāt digitālo medicīnas datus, kuri tiek glabāti Zoom vidē (platformā). ● Integritātes kontrole: Garantēt, ka (ar likumu) aizsargātie medicīniskie dati nav ļaunprātīgi (tīšī/netīši) izmainīti un, ka šādas izmaiņas nav neatpazītas (lietojot datu pārvaldi). • (Datu) Šifrēšana. (Nepieciešams) Šifrēt (ar likumu) aizsargātos medicīniskos datus.	● Konfidencialitāti no aktīviem un pasīviem uzbrukumu veidiem. ● Zoom Datu savienojumi izmanto TLS 1.2 šifrēšanu un PKI sertifikātus, kuri ir tikuši uzdoti no uzticama privāta sertifikātu pārvaldītāja ● Zoom ievieš (visā infrastruktūrā) AES-GCM šifrēšanas standartu datiem, kuri saistīti un (ar likumu) aizsargāti medicīniskiem datiem.

Ja Zoom programma ir pielāgota medicīnas pakalpojumu sniedzēja vajadzībām, tad, piemēram, tiek liegta iespēja lietotājam mainīt drošības iestatījumus, tādējādi Zoom lietojumprogramma var tikt izmantota telemedicīnas vidē. Šādas iespējas ir pieejamas Zoom pielāgotajā versijā veselības aprūpes nozarei, nevis standarta Zoom versijā (Zoom). Arī individuālam konta administratoram ir iespējams pielāgot Zoom programmu (standarta versiju) telemedicīnas vajadzībām. Dažas no funkcijām, kas var uzlabot kiberdrošības situāciju (šādā scenārijā katrs ģimenes ārsts veic Zoom administrātora funkcijas savai ārstu praksei).

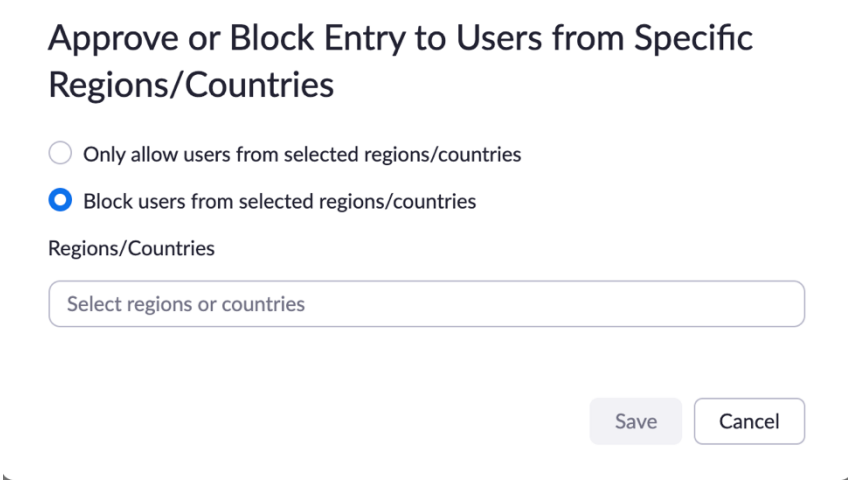
- "Uzgaidāmās telpas pielāgošana" ļauj izvēlēties iespēju, ka visi, kas saistīti ar sapulci, vispirms ir spiesti doties uz uzgaidāmo telpu. Šāda iespēja var novērst problēmas gadījumā, ja ir kāda persona, kas nav uzaicināta uz sapulci un ir ļaunprātīgā veidā ieguvusi sapulces saiti. Uzgaidāmā telpa ļauj redzēt, kura persona pievienojas sapulcei, un sapulces vadītājs var izvēlēties, vai atļaut konkrētam lietotājam pievienoties sapulcei:



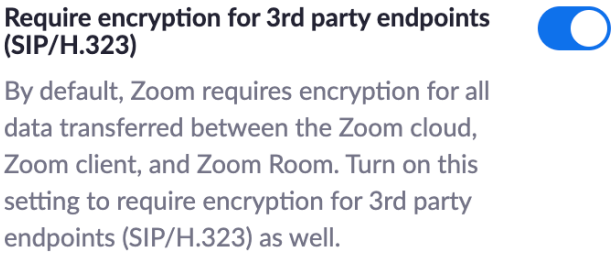
- "Tikai autentificēti lietotāji var pievienoties sapulcēm", pirms pievienošanās sapulcei personai būs nepieciešams Zoom programmas konts un pierakstīšanās:



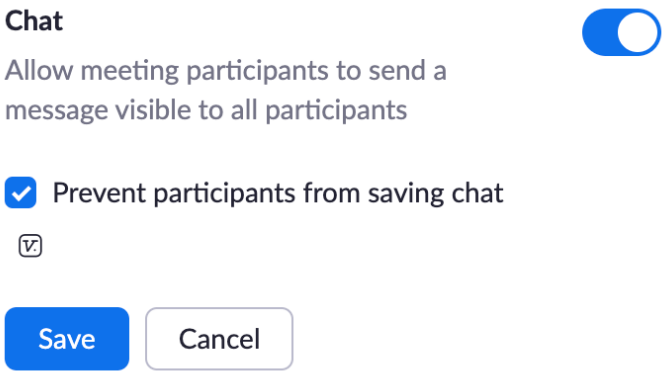
- "Apstiprināt vai bloķēt pieeju sanāksmēm lietotājiem no noteiktiem reģioniem/ valstīm", šis iestatījums ir būtisks. Tam ir divas iespējas, viena no tām – "Atļaut pieeju tikai lietotājiem no izvēlētiem reģioniem/ valstīm" – atlasot tikai Latviju, tas automātiski bloķēs personas no citiem reģioniem; otra iespēja – "Bloķēt lietotājus no izvēlētiem reģioniem/ valstīm", šis iestatījums ir arī svarīgs, lai samazinātu videokonferenču/ telemedicīnas sesiju ļaunprātīgas pārņemšanas risku:



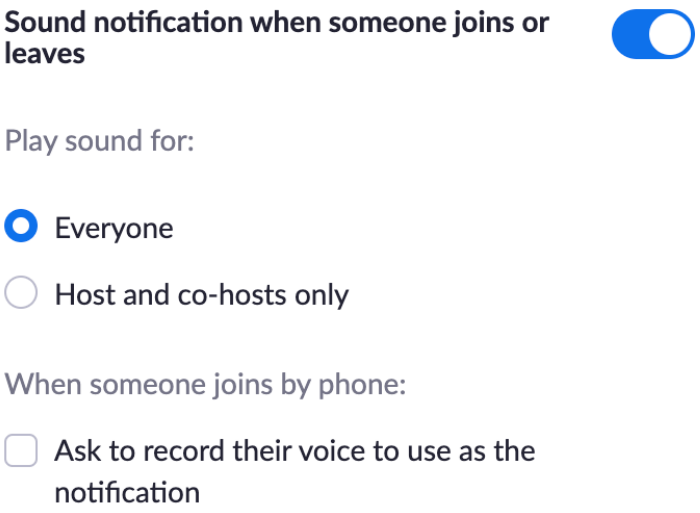
- Sapulces (pamata) apakšiestatījums "Pieprasīt trešo pušu galapunktu šifrēšanu (SIP/H.323); kad šis iestatījums ir iespējots, tad "Pēc noklusējuma Zoom programma pieprasa visu datu, kas pārsūtīti starp Zoom mākoni, Zoom klientu un Zoom telpu, šifrēšanu. Ieslēdziet šo iestatījumu, lai pieprasītu šifrēšanu arī trešo pušu galapunktiem (SIP / H.323)." Šis iestatījums neļauj trešajām pusēm un pašai Zoom programmai piekļūt video/ audio saturam:



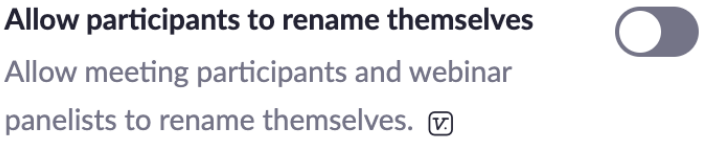
- Tērzēšanas apakšiestatījums "Neļaut dalībniekiem saglabāt tērzēšanas saturu" ļaus saglabāt privātumu un integritāti telemedicīnas vidē:



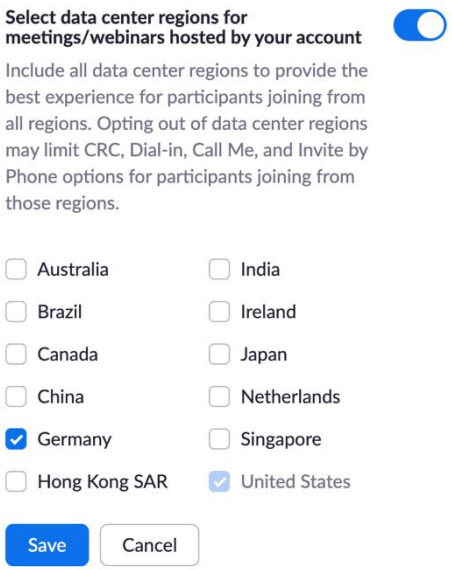
- "Skaņas paziņojums, kad kāds pievienojas vai aiziet", šāds paziņojums vērsīs uzmanību, ja kāds cits, neskaitot autorizētos lietotājus, ir ieguvis sapulces saiti un mēģina pievienoties sapulcei:



- "Ļaut dalībniekiem pārsaukt sevi" - šāds iestatījums neļaus personai uzdoties par autorizētu un zināmu sapulces dalībnieku:

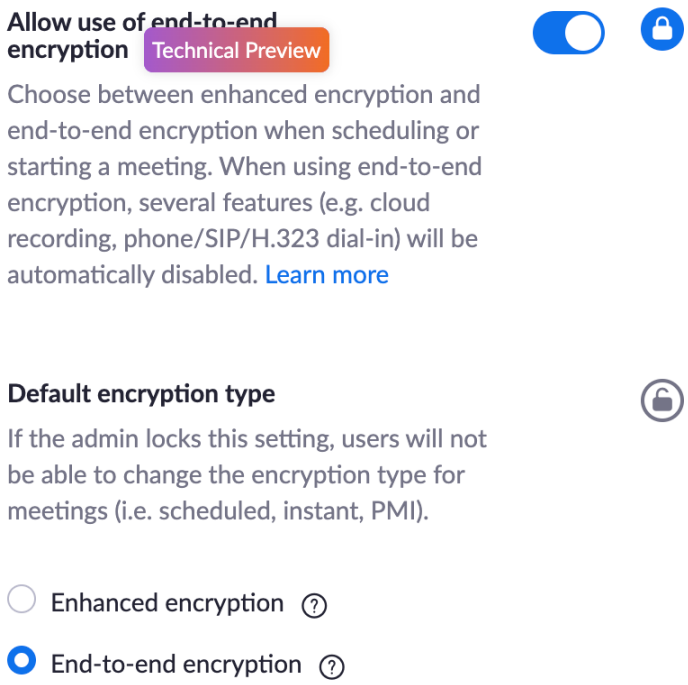


- Iestatījumos "Sapulcē (Papildu)" ir iespēja izvēlēties, kurā no datu centriem tiks vadīta sanāksme. Tas ir atrodams sadaļā "Datu centra reģionu atlase sapulcēm/ vebināriem", izvēloties konkrēto reģionu, kurā tiks vadītas sanākmes:

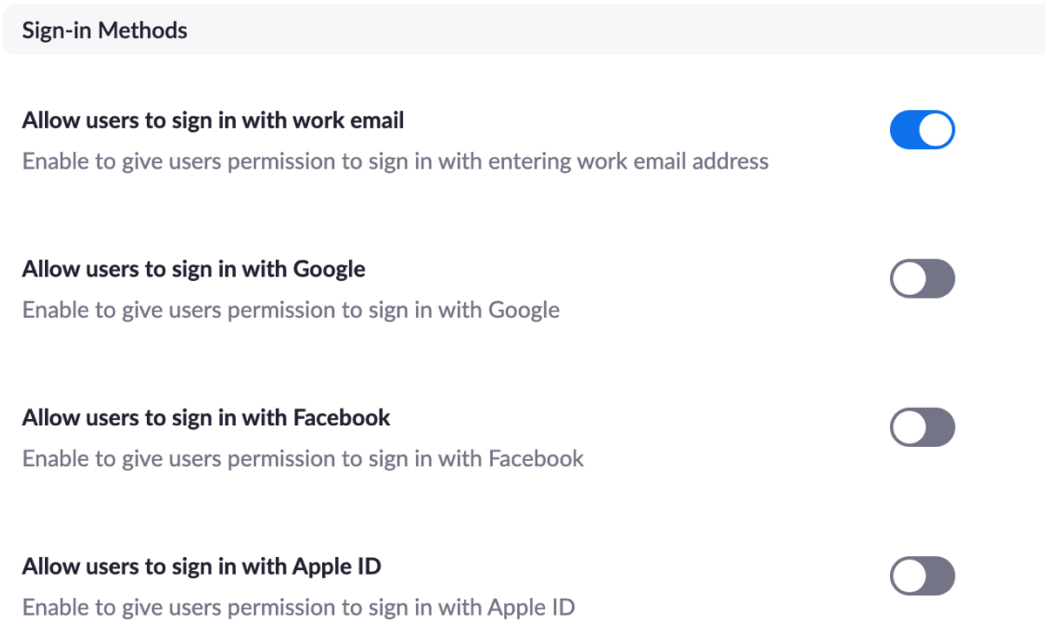


- Sadaļā Administrēšana – Konta pārvaldība – Drošība – Zoom tehniskais priekšskatījums var iespējot pilnīgu datu šifrēšanu. Iestatījums atspējos Zoom mākoņa ierakstīšanu, bet

ļaus maksimāli palielināt telemedicīnas lietošanas integritāti, privātumu un konfidencialitāti:



- Sadaļā Administrēšana – Papildu iestatījumi – Drošības pierakstīšanās var mainīt pieteikšanās iespējas, ļaujot pieteikties ar darba e-pastu un atspējojot pieteikšanos ar Google, Facebook, Apple ID:



- Izvēloties iepriekš minēto iestatījumu, tiks nodrošināts sanāksmes privātums. Tajā pašā vietā var ievietot atrunu pacientiem par telemedicīnas sesiju:

Zoom programmā regulāri tiek veikti atjauninājumi, lai uzlabotu Zoom programmu un mazinātu ievainojamības. Kā piemēru var minēt šādus atjauninājumus. 2020. gada aprīlī atjauninājumi tika veikti:

- 16. aprīlī, (Zoom, 2020a);
- 19. aprīlī, (Zoom, 2020b);
- 20. aprīlī, (Zoom, 2020c);
- 21. aprīlī, (Zoom, 2020d);
- 22. aprīlī, (Zoom, 2020e);
- 25. aprīlī, (Zoom, 2020f);
- 26. aprīlī; (Zoom, 2020g).

Tāpat 2020.g. oktobra mēnesī atjauninājumi tika veikti:

- 5. oktobrī, (Zoom, 2020h);
- 12. oktobrī, (Zoom, 2020i);
- 18. oktobrī, (Zoom, 2020j);
- 21. oktobrī, (Zoom, 2020k);
- 25. oktobrī, (Zoom, 2020l);
- 26. oktobrī, (Zoom, 2020m);
- 28. oktobrī. (Zoom, 2020n).

Šāds atjaunināšanas ātrums norāda uz vēlmi mazināt ievainojamības un ieviest uzlabojumus/ jaunas funkcijas Zoom vidē.

Drošības apsvērumi. Vidusmēra patērētāja maršrutētājs "neredz" filtru portus virs 1024 TCP/ UDP. Lai telemedicīnas vajadzībām ieviestu Zoom programmu vai jebkuru citu videokonferenču/ziņojumapmaiņas risinājumu, būtu vēlams vai nu standartizēt IPS [90]nodrošinātāju ģimenes ārstiem, piemēram, LMT, Bite u.tml., vai arī definēt minimālās tehnoloģiju prasības ģimenes ārstu praksēm, kuras ievērojot var sniegt telemedicīnas pakalpojumus. Abi risinājumi nodrošinās standartizētu tīkla piekļuvi ar zināmu kiberdrošības bāzi un stabilu piekļuvi tīklam. Visu maršrutētāju pārdevēju produkti ir jāpārbauda no ievainojamību viedokļa. Īstenojot šos iepriekš minētos risinājumus, tiks nodrošināta vienota pieeja, kuru var vienkārši uzlabot un risināt problēmas, lai panāktu stabilu telemedicīnas risinājumu.

2020. gada 9. novembrī tika publicēts FTC dokuments par Zoom programmas ievainojamībām, līdz 2020. gada rudenim Zoom programmā nav ieviesta pilnīgā datu šifrēšana.

[90] Ar interneta pakalpojumu sniedzēja standartizāciju ir saprasts, ka tas ir viens pakalpojumu sniedzējs, pie kura vēršas problēmu vai krīžu situācijā. Tas nodrošina savlaicīgu un vienotu risinājumu.

5.1.2 WebEx

WebEx kopumā ir apjomīgs, bet reizē arī ērts rīks tiešsaistei. Tomēr, testējot to ilgstoši darbībā, izaicinājumus rada intelektuālie algoritmi attēla un balss korekcijai atkarībā no fona trokšņiem un interneta tīkla ātruma. WebEx programmas administrators var iestatīt prasības pēc noklusējuma šādiem gadījumiem (CISCO, 2020. gada 30. aprīlis):

- Stingras prasības paroļu iestatījumiem, papildus standarta prasībām ir nepieciešams "neļaut nevienu rakstzīmi atkārtot trīs vai vairāk reizes";
- Pieprasīt pierakstīšanos pirms pievienošanās sapulcei;
- Neļaut piekļūt sapulcei pirms sapulces vadītāja;
- Noteikt laiku, pēc kura Personīgā istaba tiek izslēgta;
- "Dalībnieki, kuri ir pierakstījušies, var iekļūt neaizslēgtā telpā, bet neautentificētiem dalībniekiem jāgaida vestibilā, līdz sapulces vadītājs viņus manuāli ielaiž."

WebEx ir saderīgs ar HIPAA, tomēr līdzīgi kā Zoom tajā ir nepieciešama iestatījumu pielāgošana, lai īstenotu HIPAA atbilstību [91].

WebEx programma ir ierobežota, salīdzinot ar Zoom, attiecībā uz datu centru pārvaldību - lietotājs nevar izvēlēties datu centru, kas apstrādās sapulci, tādējādi nevar nodrošināt personas datu glabāšanu Eiropas Savienības ietvaros. WebEx ir datu centri šādās vietās [92]:

- Amsterdama, Nīderlande;
- Bengalūru, Indija;
- Kalifornija, ASV;
- Honkonga, Ķīna;
- Londona, Apvienotā Karaliste;
- Ņujorka, ASV;
- Singapūra, Singapūra;
- Teksasa, ASV;
- Tokija, Japāna;
- Toronto, Kanāda;
- Virdžīnija, ASV;

WebEx Interneta klātbūtnes punkti atrodas šādās vietās (CISCO, 2020.g. aprīlis):

- Amsterdama, Nīderlande;
- Kalifornija, ASV;
- Ilinoisa, ASV;
- Ņujorka, ASV;
- Sidneja, Austrālija;
- Teksasa, ASV.

[91] Journal, H. (18.02.2018). *Is WebEx HIPAA Compliant*. Izgūts no https://www.hipaajournal.com/cisco-webex-hipaa-compliant/, skatīts 31.10.2020.

[92] CISCO. (30.04.2020). *Cisco WebEx Best Practices for Secure Meetings: Site Administration.* CISCO. Izgūts no https://help.webex.com/en-us/v5rgi1/Cisco-Webex-Best-Practices-for-Secure-Meetings-Site-Administration, skatīts 31.10.2020.

Pastāvot prasībai par pilnīgu datu šifrēšanu, tiks atspējotas šādas WebEx funkcijas, iespējojot pilnīgu datu šifrēšanu [93]:

- Personīgās istabas sanāksmes;
- Pievienošanās pirms sanāksmes vadītāja;
- Videoierīces iespējotas sanāksmes;
- Cisco WebEx sanāksmju tīmekļa lietujumprogramma;
- Linux klients;
- Tīkla ierakstīšana (NBR);
- WebEx asistents;
- Sesijas datu atšifrējumu, sanāksmju piezīmju saglabāšana;
- PSTN iezvanīšana (Call-in)/atzvanīšana (Call-back);

Pilnīga datu šifrēšana ir Vispārējās datu aizsardzības regulas atbilstības un veselības aprūpes vides nodrošināšanas stūrakmens. Tomēr tam būs nepieciešama papildu infrastruktūra telemedicīnas sesijas ierakstu datu uzglabāšanai, lai saglabātu pierādījumu par pacienta ārstēšanu/ diagnozi un nodrošinātu atbilstošus drošības pasākumus.

Attiecībā uz WebEx izmantoto portu diapazonu, līdzīgi kā Zoom gadījumā ir nepieciešams maršrutētāju novērtējums, vai tie spēj ne tikai redzēt/ atpazīt, bet arī filtrēt portu diapazonus.

5.1.3 WhatsApp

Facebook apraksta IP diapazonus rakstā "Tīkla prasības", kas tika atjaunināts 2019. gada 8. augustā un stājās spēkā 2019. gada 17. augustā [94], skatīt C pielikumu.

Apkopojot autoru pieredzē un padziļinātā pētījumā balstīto informāciju (detalizēts pētījuma apskats ir pievienots ARTSS zinātniskās atskaites pielikumā), WhatsApp nenodrošina iestatījumus/funkcijas, kas atbilst Vispārējās datu aizsardzības regulas un HIPAA prasībām [95]:

- Paroles autentifikācijas trūkums katrai sesijai;
- Iepriekšējo sarunu ierakstu uzturēšanas trūkums;
- Netiek sniegts audita atbalsts;
- Facebook/ WhatsApp nenodrošina BAA iespēju, lai saglabātu datu integritāti un īstenotu drošības pasākumus.
- Zoom integrē (visā infrastruktūrā) AES-GCM šifrēšanas standartu datiem (kuri saistīti) ar (likumu aizsargāto) medicīniskiem datiem.

Turklāt WhatsApp nodrošina atbilstošu vidi datu vākšanai un izmantošanai trešo pušu interesēs. Ja mēs skatāmies uz WhatsApp privātuma politiku, kas datēta ar 2018. gada 25. aprīli

[93] CISCO. (2020). *Cisco WebEx Meetings Security.* https://www.cisco.com/c/dam/en/us/products/collateral/conferencing/webex-meeting-center/white-paper-c11-737588.pdf, skatīts 31.10.2020.

[94] CISCO. (2020). *Cisco WebEx Meetings Security.* https://www.cisco.com/c/dam/en/us/products/collateral/conferencing/webex-meeting-center/white-paper-c11-737588.pdf, skatīts 31.10.2020.

[95] Watson, K. (23.04.2020). *Is WhatsApp (R) a HIPAA compliant telemedicine software?* Bridge Patient Portal LLC. Izgūts no https://www.bridgepatientportal.com/blog/Is-Whatsapp-a-HIPAA-compliant-telemedicine-software/, skatīts 31.10.2020.

attiecībā uz Eiropas reģionu (Facebook, 2018. gada 24. aprīlis), sadaļā "Mūsu apkopotā informācija" var atrast šādu informāciju:

- "Jūsu konta informācija. Lai izveidotu WhatsApp kontu, jūs norādāt sava mobilā tālruņa numuru un pamatinformāciju (ieskaitot profila vārdu). Saskaņā ar spēkā esošo likumdošanu, jūs mums regulāri sniedzat informāciju par tālruņa numuriem savā mobilajā adrešu grāmatā, ieskaitot gan mūsu pakalpojumu lietotāju, gan citu jūsu kontaktu numurus. Jūs varat mums norādīt e-pasta adresi. Jūs varat pievienot savam kontam arī citu informāciju, piemēram, profila attēlu un informāciju sadaļā "Par mani"".
- "Jūsu ziņojumi. Mēs nesaglabājam jūsu ziņas mūsu pakalpojumu sniegšanas gaitā. Kad jūsu ziņojumi (ieskaitot tērzēšanas sarunas, fotoattēlus, videoklipus, balss ziņojumus, failus un informāciju par atrašanās vietu) ir piegādāti, tie tiek izdzēsti no mūsu serveriem. Jūsu ziņojumi tiek glabāti jūsu ierīcē. Ja ziņojumu nevar piegādāt uzreiz (piemēram, ja esat bezsaistē), mēs varam to glabāt mūsu serveros līdz 30 dienām, kamēr mēģinām to piegādāt. Ja pēc 30 dienām ziņojums joprojām netiek piegādāts, mēs to izdzēšam. Lai uzlabotu veiktspēju un efektīvāk nosūtītu multivides ziņojumus, piemēram, kad daudzi cilvēki kopīgo populāru fotoattēlu vai videoklipu, mēs varam šo saturu paturēt savos serveros ilgāku laiku. " -
- "Jūsu kontakti. Lai palīdzētu jums organizēt saziņu ar citiem, mēs varam palīdzēt jums identificēt jūsu kontaktpersonas, kuras arī izmanto WhatsApp, un jūs varat izveidot, pievienoties grupām un saziņas sarakstiem, un šādas grupas un saraksti tiek saistīti ar jūsu konta informāciju. Jūs piešķirat savām grupām nosaukumu. Jūs varat pēc izvēles sniegt grupas profila attēlu vai aprakstu ". Šāda iespēja ir potenciāls drauds medicīnas pakalpojumu sniedzējam, kurš pacienta tālruņa numurus ir glabājis savā tālrunī, kā rezultātā tie ir negribot darīti pieejami Facebook/ WhatsApp.

Automātiski apkopota informācija:

- "Informācija par lietošanu un žurnālu;
- Informācija par ierīci un savienojumu;
- Informācija par atrašanās vietu;
- Sīkdatnes.

No minētās informācijas var secināt vai savlaicīgi pamanīt nesankcionētas pieejas mēģinājumu vai iekārtas darbības nepilnības vai kļūdas.

5.1.4 Signal

Signal programma savā privātuma politikā norāda, ka apkopo par saviem lietotājiem šādu informāciju (Signal, 2020):

- "**Informācija par ierīci**, piemēram, IP adrese un ierīcei piešķirtie unikālie identifikatori (piemēram, iOS identifikators reklāmai (IDFA), Android reklamēšanas ID (AAID vai GAID)."
- "**Informācija par jūsu tiešsaistes uzvedību**, piemēram, informācija par jūsu veiktajām darbībām un saturu, kuru skatāt datu avotos, kuros tiek izmantota mūsu tehnoloģija, piemēram, laiks, kas pavadīts tīmekļa lapā, un tas, vai ritināt vai noklikšķināt uz reklāmas vai tīmekļa lapas, sesijas sākuma/ beigu laiks, jūsu novirzošās vietnes adresi, ģeogrāfiskās atrašanās vietas dati, veiktie meklējumi un pirkumu vēsture. "
- "**Informācija par rādītajām, apskatītajām vai noklikšķinātajām reklāmām**, piemēram, reklāmas veids, kur reklāma tika rādīta, vai esat uz tās noklikšķinājis, un cik reizes esat to redzējis."

Par sensitīviem datiem un to izmantošanu Signal Digital Inc. sniedz šādu informāciju [96]

"Mēs neapkopojam nekādus "sensitīvos" vai "īpašu personas datu kategoriju" datus, kā noteikts Eiropas datu aizsardzības likumos.

Mēs varam arī uzlabot lietojuma datus, izmantojot informāciju, kas apkopota no trešajām personām, piemēram, no citiem tīmekļa un mobilajiem tīkliem, apmaiņas un vietnēm ("Partneri") vai mūsu klientiem (piemēram, viņi platformā var augšupielādēt noteiktus "bezsaistes" datus). Turklāt informācija, kuru mēs automātiski apkopojam, var būt saistīta ar profila informāciju, kuru mēs izsecinām par jums. Šī informācija var ietvert, piemēram, dažādus identifikatorus, kas iegūti no citiem informācijas avotiem (piemēram, e-pasta adreses), mobilo ierīču ID, demogrāfiskajiem vai interešu datiem un skatītā satura vai darbībām, kas veiktas datu avotā. "

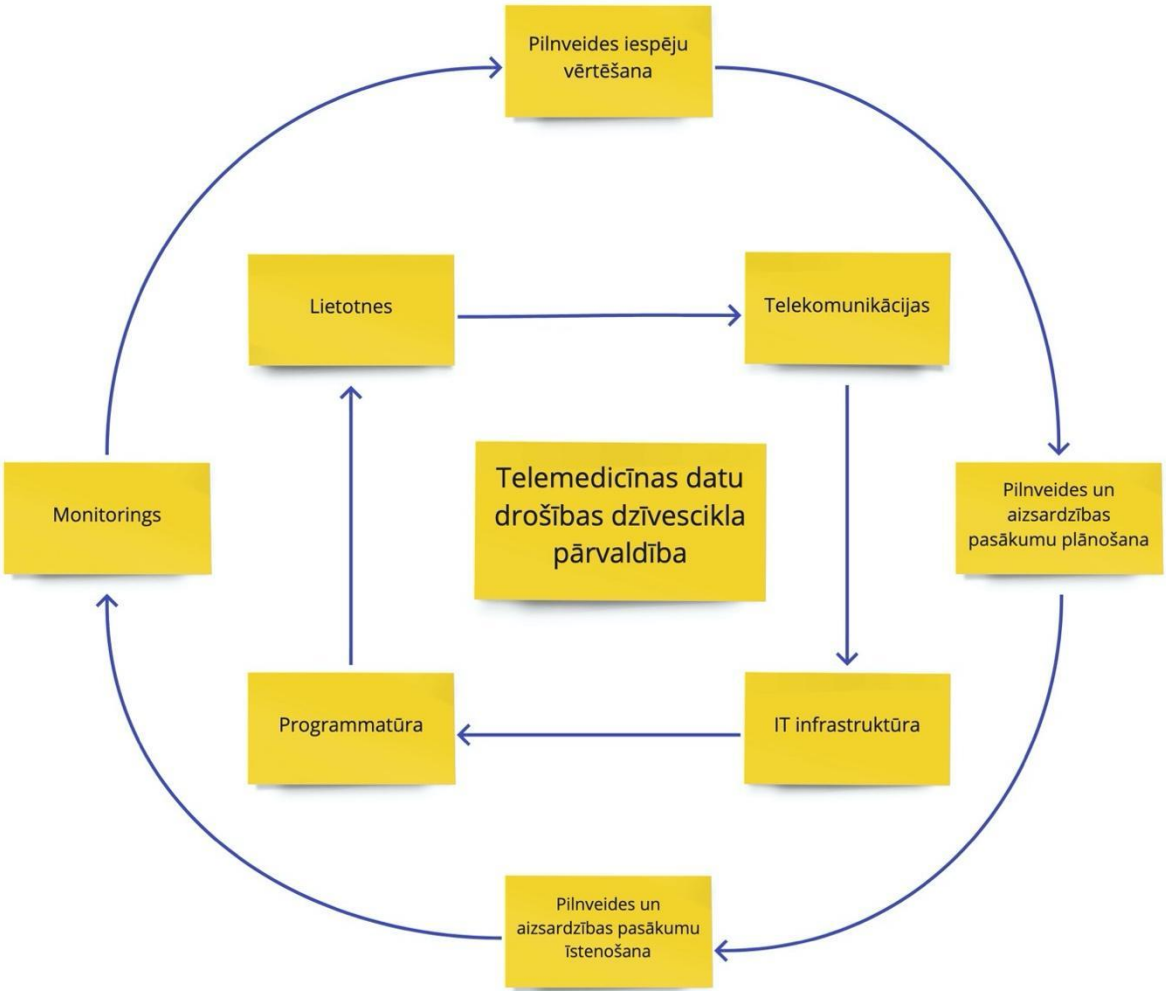
Būtībā nav nekādu precizējumu, kāda veida "Eiropas datu aizsardzības likumi" tika izmantoti, lai iestrādātu drošības pasākumus Signal programmas privātuma politikā, tāpat nav skaidri definēts termins "sensitīvs". Šāda pieeja un datu vākšanas prakse uzskatāma par nepiemērotu, lai izmantotu Signal programmu veselības aprūpes vidē vai telemedicīnā.

Turklāt Signal Digital Inc. ir neskaidri norādījumi par portu diapazonu (Signal.org, ugunssienas un interneta iestatījumi). Pieprasījums "Visiem UDP portiem būs jābūt atvērtiem" rada nedrošu vidi telemedicīnas un veselības aprūpes videi, turklāt rada lielisku vidi datu vākšanai un izmantošanai. Tāpēc Signal programma nav piemērota telemedicīnas un/ vai veselības aprūpes lietošanai un vajadzībām.

5.2 Drošas un noturīgas telemedicīnas nodrošināšanas pieeja

Telemedicīnas datu pārvaldības dzīvesciklā visos etapos (9.attēls) ir nepieciešama laba pārvaldība. IT infrastruktūra nodrošina saziņu ārstam ar pacientu caur programmatūru un lietotni, lietojot atbilstošu telekomunikāciju vidi, savukārt, drošu un noturīgu telemedicīnas vidi nodrošina pasākumu komplekss ar atbilstošu pārvaldību, kuras ietvaros tiek izvērtētas pilnveides iespējas, plānoti un īstenoti aizsardzības pasākumi, kā arī nepārtraukti monitorēta patreizējā situācija.

[96] Signal. (2020). Signal Digital, Inc. Platform Privacy Policy. Signal Digital Inc. Izgūts no https://signal.co/privacy-policy/#informationwecollect, skatīts 28.11.2020.



9.attēls. Telemedicīnas datu pārvaldība

Rekomendācija:

Ņemot vērā ģimenes ārstu darba specifiku, it īpaši Covid-19 krīzes laikā, lai paaugstinātu ģimenes ārsta laiku tiešam pacienta kontaktam vizītes laikā un nodrošinātu drošu vidi kā arī lai pasargātu pacienta datus, nepieciešams izveidot vienotu IT ekosistēmu ārstu praksēm, kura ietvertu centralizētu datortehnikas apkalpošanu, programmatūras atjauninājumu pārvaldību komplektā ar valsts nodrošinātu pārvaldītu medicīnas datu mākoņpakalpojumu ģimenes ārstiem. Datortehnikas apkalpošanai un programmatūras atjauninājumu pārvaldībai par saprātīgām izmaksām ir nepieciešams izstrādāt vienotu datortehnikas un programmatūras bāzes standartu. Katrs ģimenes ārsts saņemtu valsts apmaksātu datoru, kura specifikācijas un funkcionalitāte paredzētu::

- augstas kvalitātes datoru, kuru iespējams lietot vismaz 4 gadus ģimenes ārstu praksē;
- vismaz Full HD spēja ekrāna kvalitātei, lai nodrošinātu iespējamu strādāt ar rentgena, ultrasonogrāfijas, datortomogrāfijas un citiem vizualizētajiem izmeklējumu attēliem;
- spēja lietot gan jaunāka tipa WiFi standartus un 4G/5G mobilo internetu;
- kvalitatīva kamera un mikrofons spējai lietot videokonferences programmas;

- centralizēta programmatūra datortehnikas un programmatūras atjauninājumu pārvaldībai.

Operētājsistēmai rekomendējam atbilstību šādām spējam un funkcijām:

- maksimāli ierobežotai Telemetrijas funkcijai, lai pasargātu pacientu datu noplūdi uz programmatūras ražotāja vidi, analīzei kuru neparedz Latvijas likumdošana;
- programmatūras atjaunojumi nedrīkst izjaukt darba vidi ārsta praksē. Atjaunojumi jātestē, lai pārliecinātos par to saderību ar ģimenes ārstu vidi. IT dienests šādus testus varētu veikt centralizēti un, pēc sekmīgiem testiem, nosūtīt atjaunojumu uz ģimenes ārstu datoriem.

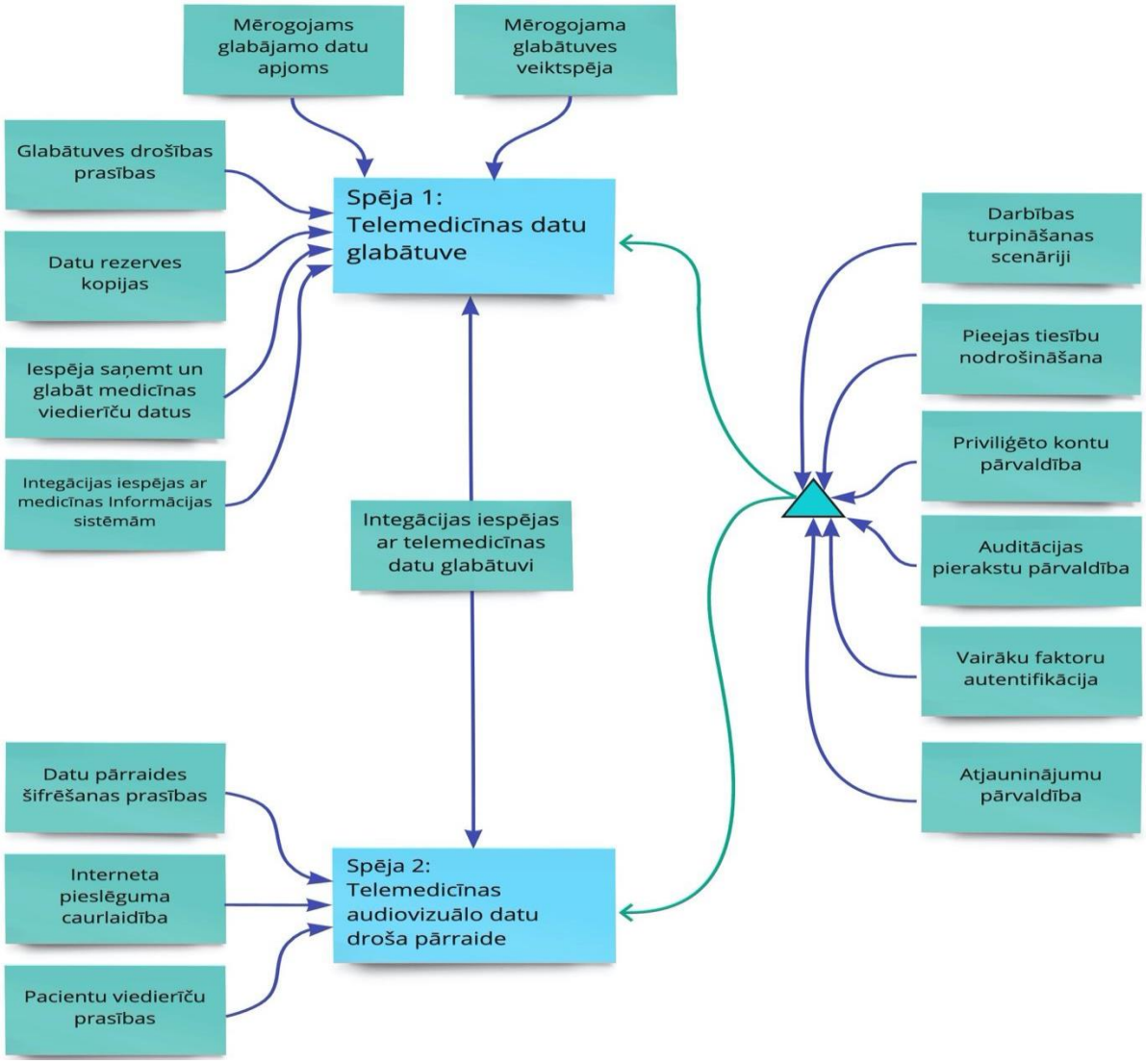
Tuvākais analogs ir Microsoft Windows 10 Enterprise 2019 LTSC.

Veidojot vienotu iekārtas un programmatūras platformu tiktu samazināts nesankcionētas piekļuves risks veselības aprūpes IKT infrastruktūrai un datiem, uzlabota vispārējā ārsta prakses efektivitāte, pacientu apkalpošanas kvalitāte, kā arī panākta veselības aprūpes sistēmas stiprināšana no informācijas drošības aspekta. Tas savukārt samazina valsts un ģimenes ārsta prakses neplānotus izdevumus, kuri ir saistīti ar nevienmērīgu IT nodrošinājuma platformu.

5.3 Servisu drošības un noturības nodrošināšanas paņēmieni

Telemedicīnas servisu drošības un noturības spējas (10.attēls) sastāv no datu uzglabāšanas un datu pārraides spējām. Datu glabātuves nozīmība ir tās spēja pievienot tai jaunus datus, nodrošinot integrāciju ar tādiem ārējiem datu avotiem, kā ārsta prakšu lietotām medicīnas informācijas sistēmām un viedierīču datiem. Lai nodrošinātu ilgtspējīgu datu glabātuves dzīves ciklu, nepieciešams paredzēt mērogošanas spēju kā datu apjomiem, tā veiktspējai. Audiovizuālu datu pārraidē ir nepieciešams nodrošināt aizsardzību pret nesankcionētu piekļuvi datiem ar kriptogrāfijas metodēm jeb šifrēšanu, pie tam ņemot vērā pacientu un ārsta prakšu interneta pieslēguma caurlaidību un pielietoto viedierīču tehniskās iespējas. Kriptogrāfijas matemātiskās metodes papildus konfidencialitātei nodrošina arī pārraidāmo datu kompresiju jeb apjoma samazināšanu, kas pieļauj iespēju mazināt interneta pieslēguma caurlaidības prasības.

Telemedicīnas datu glabātuvei un tās audiovizuālo datu droša pārraidei jānodrošina datu pieejamība, konfidencialitāte un integritāte visā dzīvescikla laikā. IKT industrijas labā prakse tam veic aizsardzības pasākumu kompleksu, kura sastāv no plānošanas, īstenošanas un uzraudzības. Plānošanas stadijā svarīgākās ir drošības, veiktspējas un darbības turpināšanas prasību definēšana. Drošības un noturības īstenošanai nepieciešama laba pārvaldība, kura ietver definētajām drošības prasībām atbilstošu pieejas tiesību nodrošināšanu, administratora jeb priviliģēto kontu pārvaldību, lietotāju vairāku faktoru autentifikāciju, piemēram, parole un īsziņa vai lietotne viedtelefonā, kā arī atjauninājumu pārvaldība ar regulāru monitoringu, uzraudzību un atbilstošu instalācijas procesu.



10.attēls. Telemedicīnas datu drošuma un noturīguma nodrošināšanas paņēmieni

5.4 Telemedicīnas pakalpojumu kvalitāte

Akadēmiskajā literatūrā uzsvērts, ka noteikt un izvērtēt attālināto telemedicīnas konsultāciju kvalitāti ir sarežģīti, jo nereti ir ierobežota informācija par sasniegto rezultātu[97]. Tādēļ, lai definētu telemedicīnas konsultāciju kvalitāti, tiek pievērsta uzmanība konsultāciju procesam un konsultāciju rezultātam. Respektīvi:

1. Kāda bija komunikācijas kvalitāte un vai pacients ir apmierināts ar komunikāciju?;
2. Cik noderīga rezultātu ziņā ir bijusi telemedicīnas konsultācija?

Vienlaikus, telemedicīnas konsultāciju kvalitāti ir jāaplūko no četriem aspektiem: vērtība pacientam, vērtība ārstējošajam ārstam, vērtība organizācijai vai ārstniecības iestādei un vērtība sabiedrībai kopumā. Ja telemedicīnas konsultāciju vērtību un kvalitāti pirmajās trijās perspektīvās (pacients, ārstniecības persona, ārstniecības iestāde) var noteikt jebkurš profesionālis telemedicīnā, tad pievienoto vērtību sabiedrībai noteikt ir salīdzinoši komplicēti. Telemedicīnas konsultāciju kvalitāti ietekmē tādi faktori kā attiecīgās valsts veselības aprūpes sistēmas darbības nosacījumi, tostarp pakāpe, kādā telemedicīna ir pienācīgi integrēta veselības aprūpes pakalpojumu ķēdē98.

No ekonomiskās perspektīvas, telemedicīnas pakalpojumu kvalitāti var novērtēt ar pieejas rentabilitāti un veikt salīdzinājumu starp klātienes konsultāciju un telemedicīnas konsultāciju. Tomēr telemedicīnas jomā, kur liela nozīme ir IKT tehnoloģijām, pastāv bažas par resursu izšķērdēšanu[99]. Tiesa, šo pierādīt ir grūti, jo pacients pēc pirmās telemedicīnas konsultācijas var vairāk nevērsties pie ārsta vai gluži pretēji pacientam var veidoties atkarība no šādiem pakalpojumiem. Detalizētāk iespējamās telemedicīnas barjeras ir aprakstītas šajā ziņojumā iepriekš.

6.tabula. Jautājumi, kas nosaka konsultācijas kvalitāti un vērtību no procesa viedokļa:

Jautājums:	**Iespējamās atbildes**
1.Vai jautājums, ko uzdeva ārstējošais ārsts, bija skaidrs?	Jā / varbūt /nē /nezinu
2.Vai ārstējošais ārsts sniedza pietiekamu informāciju par ārstēšanas taktiku?	Jā / varbūt /nē /nezinu
3.Vai tika veikti izmeklējumi pirms konsultācijas?	Jā/nē
4.Ja jā, vai izmeklējumi bija pietiekami?	Jā / varbūt /nē /nezinu
5.Ja nē, kādi papildus izmeklējumi būtu palīdzējuši?	Jā / varbūt /nē /nezinu
6.Vai konsultācijas pierakstu un koordināciju var uzlabot?	Jā / varbūt /nē /nezinu

[97] Wootton R., Liu J., Bonnardot L. (2014). *Assessing the quality of teleconsultations in a store-and-forward telemedicine network.* Frontiers in Public Health.
[98] Turpat.
[99] Turpat.

6., 7. 8.tabulā iekļautie jautājumi ir piemērojami gan vispārīgi konsultācijām, gan telemedicīnas konsultācijām, lai identificētu iespējamas atšķirības starp abiem konsultāciju tipiem.

7.tabula. Jautājumi, kas nosaka konsultācijas kvalitāti un vērtību no procesa viedokļa un ārsta perspektīvas:

Jautājums:	**Iespējamās atbildes**
1.Vai pacienta kartiņa tika nosūtīta atbilstošam citas jomas ārstam/ekspertam?	Jā / varbūt /nē /nezinu
2.Vai atbilde tika sniegta pietiekami ātri?	Jā / varbūt /nē /nezinu
3.Vai atbilde bija atbilstoša situācijai?	Jā/nē

8.tabula. Jautājumi, kas nosaka telemedicīnas konsultācijas kvalitāti un vērtību no pacienta un ārsta perspektīvas:

Jautājums:	**Iespējamās atbildes**
1.Vai telemedicīnas konsultācija precizēja diagnozi?	Jā / varbūt /nē /nezinu
2. Vai ieteiktā darbība palīdzēja ārstam vadīt pacienta slimības gaitu?	Jā / varbūt /nē /nezinu

Intervijās tika norādīts, ka nepieciešams definēt jomas, kurās ir iespējama telemedicīnas konsultācija un kurās jomās tā nav iespējama. Ir jomas, kurās pacienta un ārsta sadarbība klātienē ir galvenais priekšnoteikums kvalitatīva medicīnas pakalpojuma sniegšanai. Vienlaikus, nosakot telemedicīnas konsultāciju jomas, jāparedz, ka, iespējams,obligāti nepieciešama pirmā pacienta vizīte klātienē, bet turpmāko monitoringu ārsts var veikt attālināti.

Balstoties uz intervijām un literatūras izpēti var identificēt šādu iespējamo kvalitātes kritēriju listi:

a) Telemedicīnas konsultācijas **medicīniska kvalitāte** – cik ārsts objektīvi var izvērtēt pacienta stāvokli, ko ārsts redz videorežīmā, kādi ir pieejamie attēli, dati un analīžu rezultāti.

b) Telemedicīnas konsultācijas **komunikācijas kvalitāte** – cik lietišķi, profesionāli izturas ārsts. Šajā gadījumā, svarīga ir emocionālā inteliģence – ārsta un pacienta ķermeņa valoda un uzvedības pazīmes. Piemēram, ārsts pieraksta pacienta sniegto informāciju, bet pacients to var neredzēt un viņam likties ka ārstam ir garlaicīgi vai ārsts neklausās.

c) Pacienta kā klienta telemedicīnas **konsultācijas kvalitātes novērtējums** – piemēram, pēc konsultācijas pacients aizpilda kvalitātes novērtējumu konsultāciju vietnē punktos. Piešķirtie punkti var būt publiski redzami vai arī pieejami tikai ārstam un ārstniecības iestādes vadībai.

d) Telemedicīnas konsultācijas **tehnoloģiskā kvalitāte** – izmantoto tehnoloģiju drošība. Komisijas paziņojumā Eiropas Parlamentam, Padomei, Eiropas Ekonomikas un

sociālo lietu komitejai un Reģionu komitejai par telemedicīnu pacientu, veselības aprūpes sistēmu un sabiedrības labā (04.11.2008., COM (2008) 689)[100] ir uzsvērts, ka jo īpaši telemedicīnas manipulāciju veikšanā jāparedz informācijas sniegšana par tehniskajiem datu pārraides līdzekļiem.

e) **Netiešo datu** izmantošana – izmantot datus par izlietotajām receptēm, lai identificētu apmierinātību ar konsultāciju kvalitāti, t.sk. ar telemedicīnas konsultāciju.

Pēdējos gados kvalitātes novērtēšanas koncepcijas un stratēģijas veselības aprūpes jomā ir būtiski pārveidotas, izmantojot nepārtrauktas kvalitātes vadības (TQM) modeli. Turklāt, telemedicīnā ir identificētas trīs problēmzonas[101]:

a) Pārmērīgs aprūpes apjoms (*overuse of care)* – piemēram, nevajadzīgas telemedicīnas konsultācijas

b) Nepietiekams aprūpes apjoms (*underuse of care)* – piemēram, pacients netiek sūtīts uz papildus izmeklējumiem vai konsultācijām pie citiem speciālistiem, pieņemot ka telemedicīnas konsultācijā ir saņemts pietiekams informācijas apjoms no pacienta, lai noteiktu diagnozi;

c) Nepietiekama tehniskā vai personiskā veiktspēja (*poor technical or interpersonal performance)* – neprecīza datu interpretācija vai nepietiekama uzmanība pacienta izteiktajām bažām.

Tādējādi, telemedicīnas konsultāciju kvalitāti var aplūkot no visaptverošās kvalitātes vadības perspektīvas:

- tehniskās iespējas – vai tehnoloģija ir droša, precīza un uzticama atbilstoši tehnoloģiju standartiem;
- diagnostikas precizitāte – vai tehnoloģija veicina pareizas un precīzas diagnozes noteikšanu;
- diagnostikas ietekme – vai tehnoloģija sniedz diagnostisku informāciju, kas ir noderīga, lai noteiktu diagnozi (piemēram, vai pēc telemedicīnas konsultācijas joprojām ir nepieciešama konsultācija klātienē vai gluži pretēji – telemedicīnas konsultācijas rezultātā var turpināt pacienta monitoringu, uzraugot atsevišķus pacienta veselības rādītājus);
- terapeitiskā ietekme – vai tehnoloģija ietekmē pacienta slimības gaitas vadību vai terapiju;
- ietekme uz pacienta veselību – vai tehnoloģija uzlabo pacienta veselību un labsajūtu ilgtermiņā.

---

[100] *Eiropas Ekonomikas un sociālo lietu komitejas atzinums par tematu Komisijas paziņojums Eiropas Parlamentam, Padomei, Eiropas Ekonomikas un sociālo lietu komitejai un Reģionu komitejai par telemedicīnu pacientu, veselības aprūpes sistēmu un sabiedrības labā COM(2008) 689 galīgā redakcija.* Izgūts no https://eur-lex.europa.eu/legal-content/LV/TXT/PDF/?uri=CELEX:52009AE1197&from=LV, skatīts 31.10.2020.

[101] Field M.J. (eds). *Telemedicine: A Guide to Assessing Telecommunications in Health Care.* Institute of Medicine (US) Committee on Evaluating Clinical Applications of Telemedicine; Washington (DC): National Academies Press (US); 1996.

Savukārt, vērtējot telemedicīnas konsultāciju kvalitāti rīcībpolitikas kontekstā, jāpievērš uzmanība šādiem telemedicīnas rezultatīvajiem rādītājiem:

a) telemedicīnas konsultāciju skaita izmaiņas noteiktā laika periodā (piemēram, 1 gada laikā);

b) klātienes pacientu konsultāciju skaita izmaiņas noteiktā laika periodā (piemēram, 1 gada laikā);

c) Gaidīšanas/pieraksta pie ārsta laika izmaiņas (piemēram, samazinās gaidīšanas laiks)

d) Pacienta neapmeklēto vizīšu skaita izmaiņas skatot klātienes konsultāciju modeli pret telemedicīnu noteikta laika periodā (piemēram, 1 gada laikā);

e) Pacientu vēlme un pieprasījums pēc telemedicīnas konsultācijām (nosaka ar sabiedriskās domas aptauju);

f) Pacienta un ārsta attieksmes maiņa par telemedicīnas konsultācijām (piemēram, abas grupas atbalsta telemedicīnas konsultācijas);

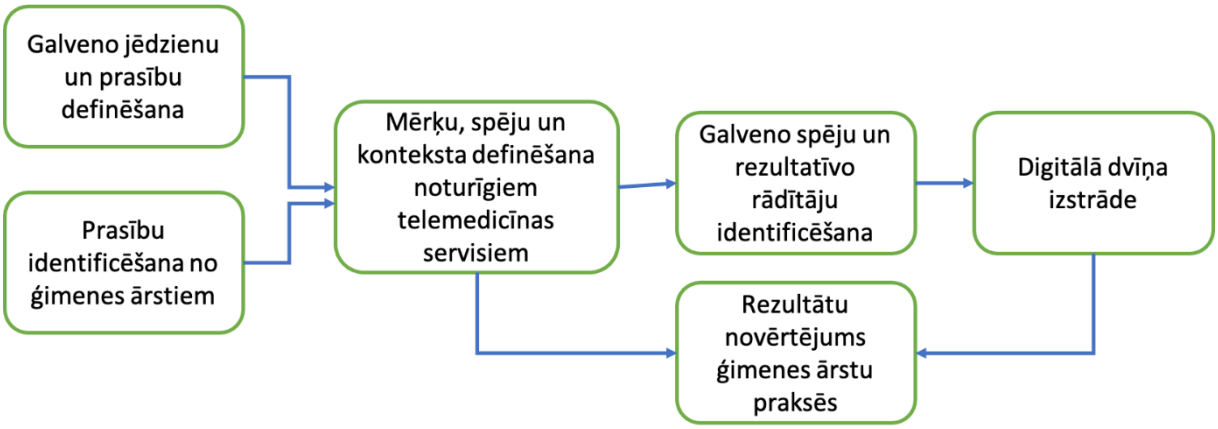
g) Administratīvā sloga salīdzinājums klātienes konsultācijām un telemedicīnas konsultācijām

6 Droša un noturīga telemedicīnas servisa piemērs (*use cases*)

Izstrādājot droša un noturīga servisa piemēru (pamatojoties uz ARTSS metodi), tika iesaistīti gan kiberdrošības nozares profesionāļi, gan arī ģimenes ārstu pārstāvji (dr.Ilārs Freimanis un dr.Ņina Gailīte) un IT jomas eksperti (PhD Jānis Stirna, Dr.oec. Juris Binde, Dr.sc.ing. Ginta Majore, Egons Bušs, Viesturs Bambāns), lai identificētu galvenās prasības telemedicīnas pakalpojumiem tieši ģimenes ārstu praksēm. Fokuss ir izvēlēts balstoties gan uz nozares literatūrā sastopamajām atziņām par telemedicīnas pakalpojumu ieviešanas posmiem, gan arī praktisko nozares vajadzību un risinājumu nepieciešamību pandēmijas laikā, kas saistīts ar distancēšanos un attālinātām konsultācijām Covid-19 saslimšanas izplatības mazināšanai.

Analizējot kopējo situāciju nozarē un tās vajadzības tika īstenoti 11.attēlā parādītie soļi. Analīzes laikā tika identificētas šādi izaicinājumi:

- normatīvie akti telemedicīnas pakalpojumiem vāji atspoguļo un regulē šīs jomas darbību kopumā un ģimenes ārstiem nav skaidras norādes par to, kā pakalpojumi būtu veicami;
- normatīvai bāzei ir jāiekļauj drošības aspekti, kas būtu ievērojami ģimenes ārstu praksēs;
- ģimenes ārstu visaptverošas zināšanas par to, kā būtu droši glabājami un izmantojami pacientu medicīniskie dati tieši IT ietvarā.



11.attēls. Drošu un noturīgu telemedicīnas servisu izstrādes piemērs

Aktivitātes rezultātā identificētie drošu un noturīgu telemedicīnas servisu piemēri sniedz ieguldījumu un pievienoto vērtību:

- ģimenes ārstu prakses noslodzes mazināšanai, reizē palielinot apkalpoto pacientu skaitu;
- spēju nodrošināt pakalpojuma nepārtrauktību arī pandēmijas laikā;
- vēršot uzmanību un uzsverot unificētas un standartizētas savstarpēji savietojamas platformas nepieciešamību, kuru medicīnas personāls var izmantot bez būtiskiem darbības traucējumiem un efektīvi ietaupot vizītei atvēlēto laiku darbā ar pacientiem;
- plānojot telemedicīnas servisus jāņem vērā GDPR regulējums;
- sensori un citi biometriski dati dotu precīzākus ieejas datus precīzāka modeļa īstenošanai.

Lietošanas gadījumu mērķis ir:

- izanalizēt esošo situāciju un iespējamos risinājumus telemedicīnas pakalpojumu elastības un drošuma nodrošināšanai pandēmijas situācijā;
- ieinteresēto pušu iesaiste (ģimenes ārstu pārstāvju kā arī citu telemedicīnas pakalpojumu nodrošinājumā iesaistīto organizāciju pārstāvju);
- definēt šablonus un pielāgojumus elastīgu un drošu pakalpojumu nodrošināšanai;
- nodefinēt ietvaru digitālā dvīņa izstrādei.

Izstrādājot un definējot lietošanas gadījumus, autori izmantoja ARTSS metodi servisu noturības un drošības, kā arī esošās situācijas analīzes, ierobežojumu un iespēju izvērtējumam. Metode nodrošina mērķu, darbības rādītāju, konteksta, drošības un noturības faktoru strukturētu analīzi un atspoguļojumu.

Telemedicīnas servisu piemērs ir detalizēti atspoguļots turpmākajos attēlos (12., 13., 14., 15.attēli), kā arī modeļa kopskats (16.attēls). Modeļu elementu skaidrojums ir pievienots 2.pielikumā.

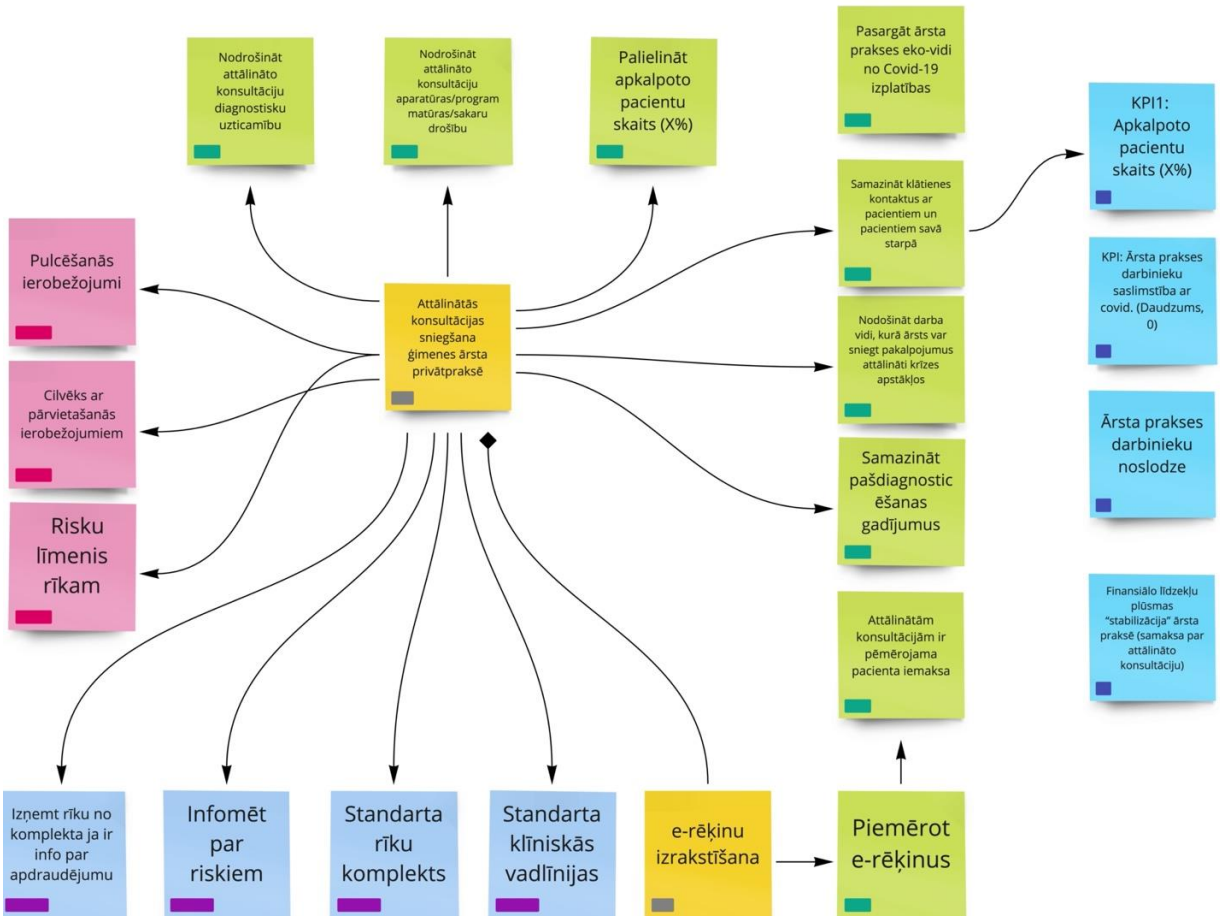
Izstrādātais lietošanas gadījumu piemērs sastāv no šādiem modeļiem:

- Specifiskie mērķi attālinātai konsultāciju sniegšanai ģimenes ārstu privātpraksē (12.attēls), kas sastāv no galvenajiem mērķiem, sasniedzamajiem rezultatīvajiem rādītājiem, kā arī izaicinājumiem un problēmām. Modelis ietver kvalitatīvos un kvantitatīvos mērķus tādus kā servisu/konsultāciju saņēmušo pacientu skaits un pielāgojumi, kas nepieciešami pandēmijas situācijā;

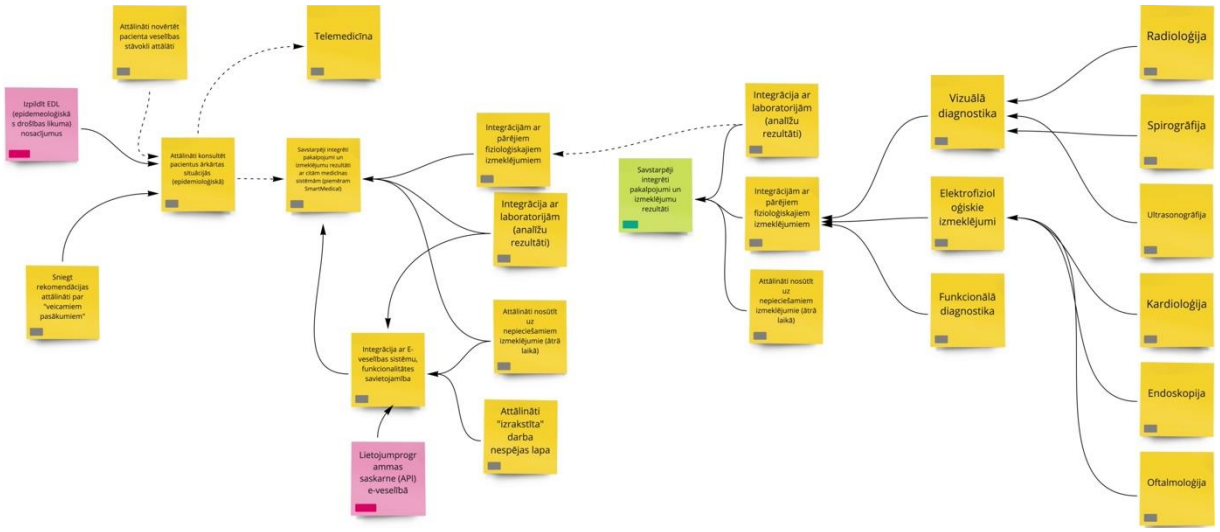
- Spēju/servisu kopums telemedicīnas pakalpojumu integrācijai ģimenes ārstu privātpraksēs (13.attēls), kas ietver spējas un dažādu izmeklējumu rezultātu savstarpējo integrāciju (samazinot izmantojamo lietotņu skaitu), lai palīdzētu ģimenes ārstam iegūt pēc iespējas visaptverošāku pārskatu par pacienta veselības stāvokli, gan arī ietaupītu laiku šāda pārskata ieguvei;

- Pacienta veselības stāvokļa attālināts monitorings (14.attēls), kas ir ļoti svarīgs īpaši pandēmijas situācijā novērtēt un uzraudzīt pacientu veselības stāvokli attālināti, lai savlaicīgi identificētu novirzes no normālajiem rādītājiem pirms kritiska stāvokļa iestāšanās. Modelis ietver spējas, kas iespējamas no tehnoloģiju perspektīvas, bet ir identificēti arī trūkumi integrācijai ar vienoto pacientu datu elektronisko pierakstu un visaptveroša imitāciju modelēšana, lai prognozētu stāvokļa attīstību, kas varētu tikt risināts ar digitālā dvīņa izstrādes palīdzību;

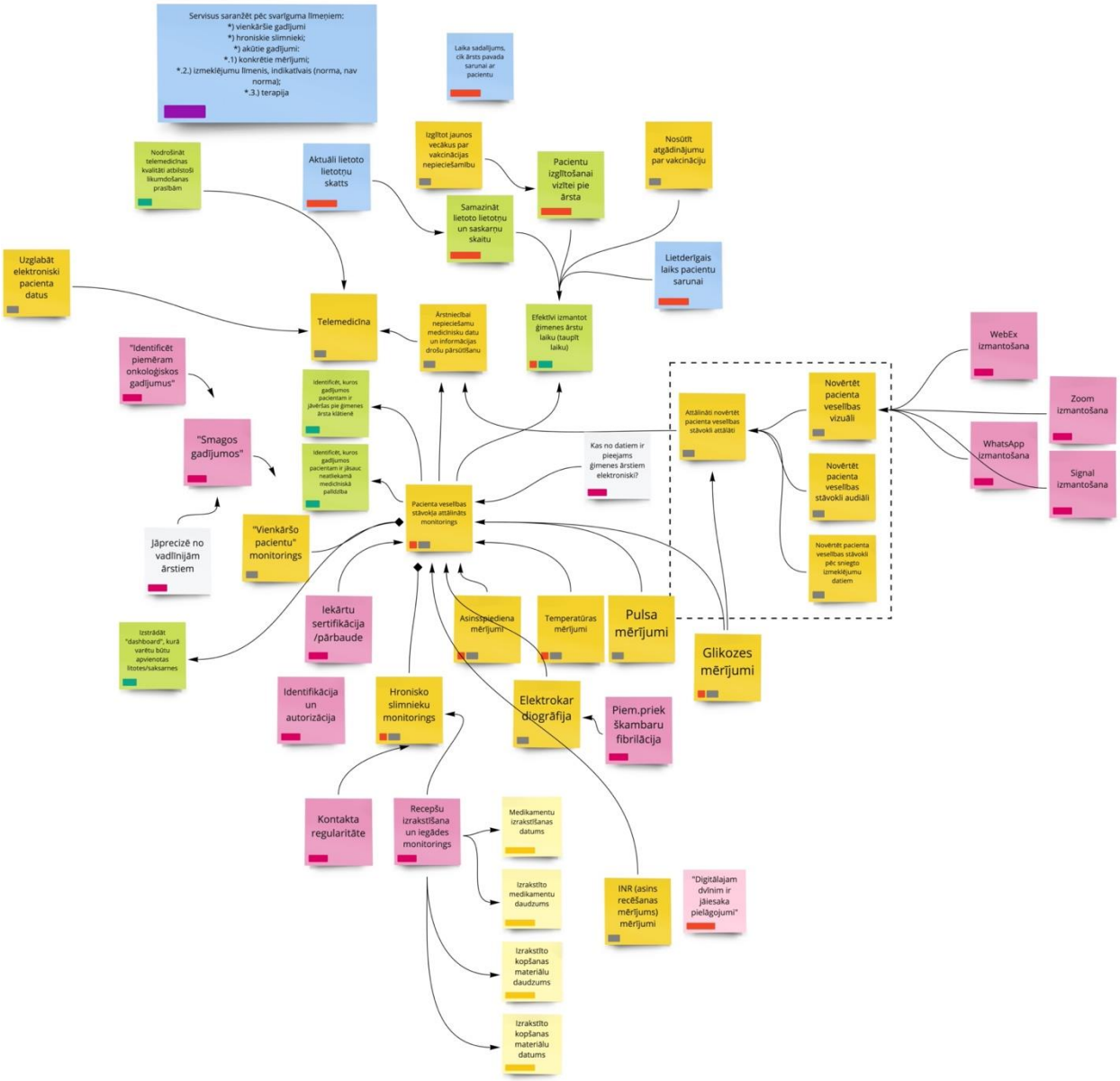
- Drošības aspekti telemedicīnā pacientu konsultēšanā (15.attēls) ietver praktiskus mērķus drošības aspektu īstenošanai, gan arī pacientu un ārstu izglītošanai ne tikai drošības jautājumos, bet arī tajos, kas palīdzētu ietaupīt ārsta un pacienta saskarsmes fizisko laiku un paaugstinātu vizītes efektivitāti un rezultatīvo rādītāju sasniegšanu.



12.attēls. Specifiskie mērķi attālinātai konsultāciju sniegšanai ģimenes ārstu privātpraksē

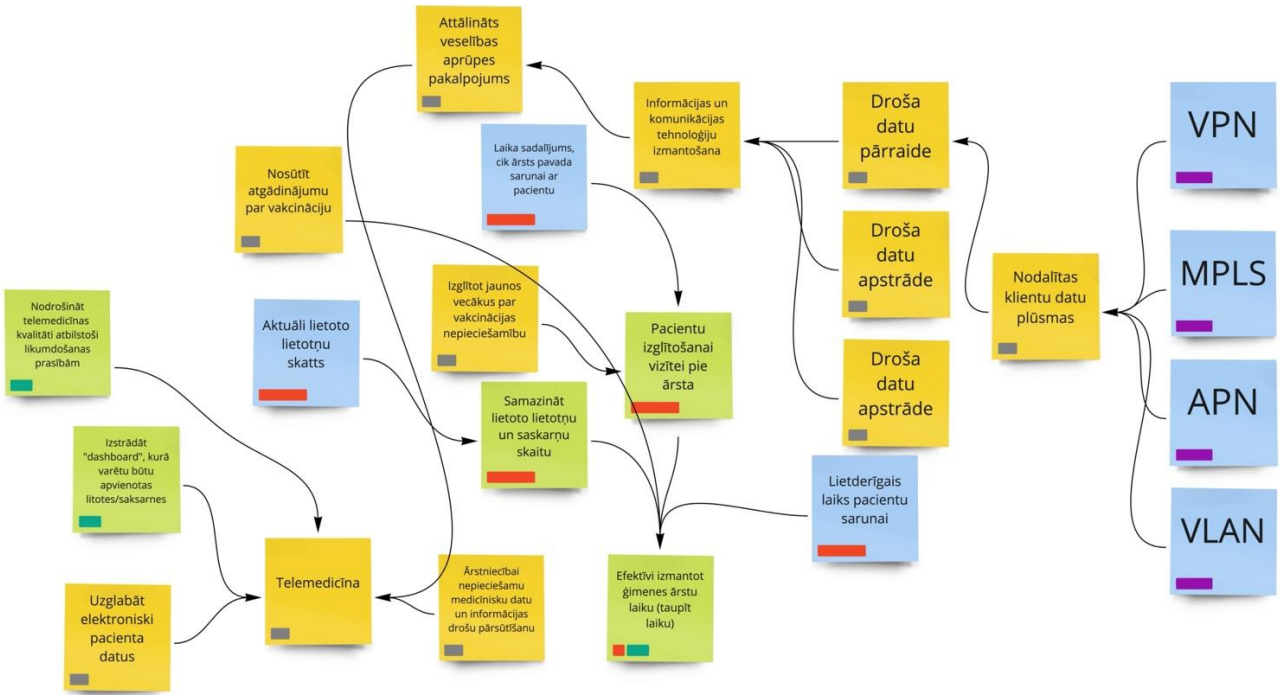


13.attēls. Spēju/servisu kopums telemedicīnas pakalpojumu integrācijai ģimenes ārstu privātpraksēs



14.attēls. Pacienta veselības stāvokļa attālināts monitorings

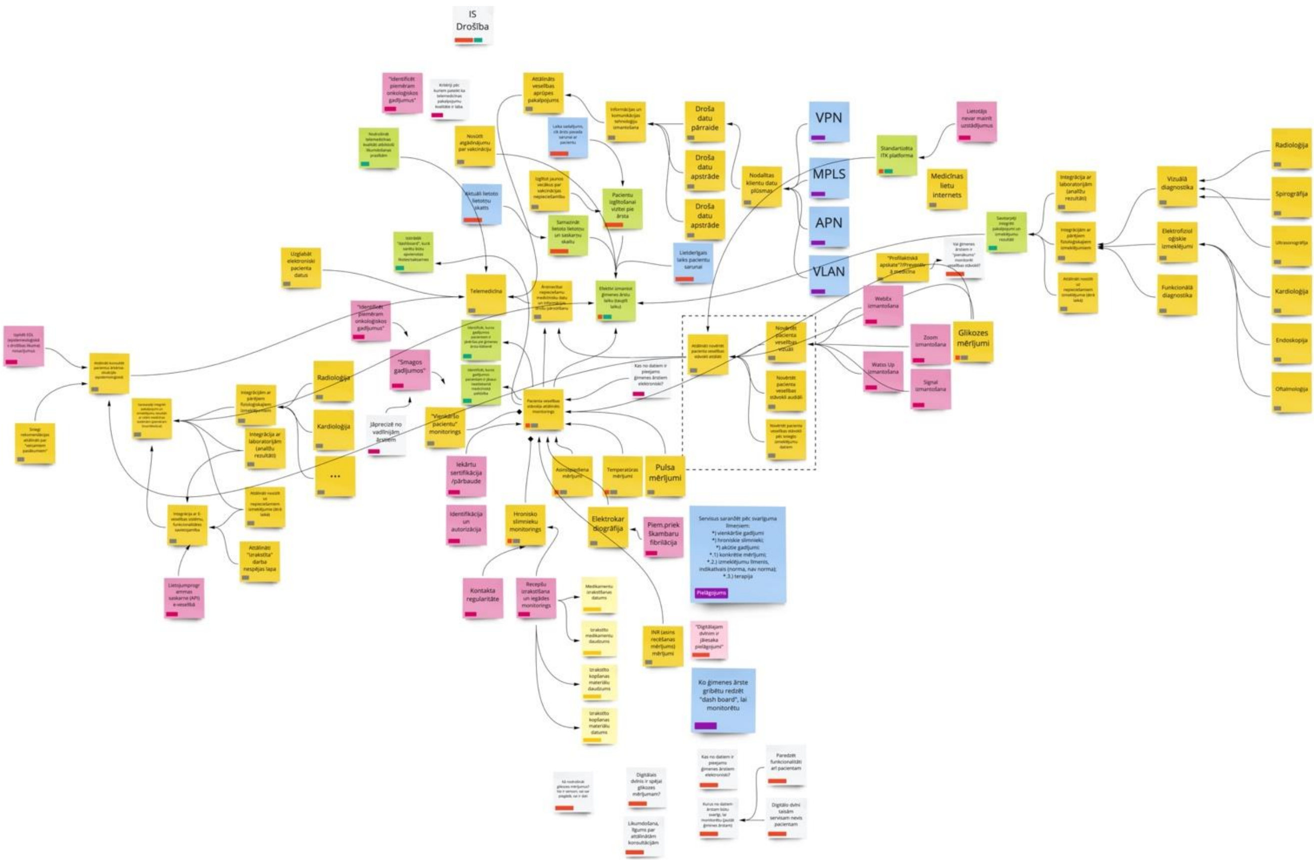
ARTSS projekta ietvaros tika veikta analīze un rezultāti atspoguļoti plašākā kontekstā, kas ir atspoguļots kopējā modelī 16.attēlā. Modelis ietver gan praktiskās ģimenes ārstu vajadzības izmeklējuma datu savstarpējai integrācijai, kas ietaupa laiku praktiski pārskatot pacienta izmeklējuma rezultātus noteiktā laika periodā dažādās lietotnēs, gan arī drošības un pacientu izglītošanas aspektus. Modelis iekļauj arī praktiskas rekomendācijas jau esošo e-Veselības sistēmu pilnveidei un arī to procesu sakārtošanai, kas attiecas uz pacienta datu elektronisku uzskaiti.



15.attēls. Drošības aspekti telemedicīnā pacientu konsultēšanā

Telemedicīnas drošības aspektos visbūtiskāko lomu spēlē pielietotie IKT risinājumi. Datu pārraide telemedicīnā Latvijas Republikā nav regulēta. Izejot no labās prakses IKT jomā, būtu nepieciešams nodalīt klientu datu plūsmas, lai nodrošinātu integritāti, privātumu un konfidencialitāti. Industrijā atzīta pieeja ir datu plūsmu nodalīšana iestādes iekšpusē ar VLAN (Virtual Private LAN vai virtuālais iekšējais datortīkls), savukārt ārējā pieslēgumā lietot izdalītu APN (Access Point Name) mobilajos pieslēgumos vai fiksētajos pieslēgumos citas klientu datu plūsmu nodalīšanas tehnoloģijas – MPLS (MultiProtocol Label Switching) vai VPN (Virtual Private Network).

Ārstu prakšu un pacientu savstarpējā komunikācijā papildus drošam datu pārraides kanālam būtiska loma ir datu drošai uzglabāšanai, IKT rīku lietderībai un efektivitātei, lietotņu un saskarņu skaitam, kā arī to lietošanas ērtībai un efektivitātei. Ideālā gadījumā katram veselības sistēmas lietotājam būtu pieejama viena mobilā lietotne un portāls, kurā ir pārvaldāma visa pacienta medicīnas informācija, kā arī iespējama divvirziena saziņa (sarakste, balss un video) ar ģimenes ārstu un datu integrācija ar e-Veselības sistēmu.



16.attēls. Kopējais modelis telemedicīnas pakalpojumu nodrošināšanai ģimenes ārstu privātpraksēs

Liela daļa pacientu medicīnas datu joprojām tiek apstrādāta papīra formā “pacienta kartiņās”, kuras katra medicīnas iestāde un ārstu prakse glabā pie sevis, bez iespējas datu apmaiņai. Medicīnas sistēmas lietotājam nonākot situācijā, kad nepieciešama neatliekamā medicīniskajā palīdzība, rodas problēmas palīdzības sniegšanā, jo NMP ārstiem nav pieejama sensitīva informācija par konkrēto pacientu – iepriekšējā slimības vēsture, hematoloģija, alerģijas, u.c.

Veicot drošu un noturīgu telemedicīnas pakalpojumu modelēšanu ģimenes ārstu privātpraksēs, autoru kolektīvs secināja, ka būtiskākā normatīvo aktu problēma ir vāji regulētā normatīvā bāze, kā arī praktiskajos pielietojumos vislielākā uzmanība ir jāpievērš IKT drošības aspektiem. Ilgtermiņā nav pieļaujama situācija, kad ģimenes ārstiem jālieto telemedicīnai nepiemēroti saziņas kanāli un līdzekļi, piemēram, WhatsApp vai neaizsargāts e-pasts, sensitīvu medicīnas datu pārsūtīšanai starp pacientu un ģimenes ārstu.

7 Ieteikumi

Šajā nodaļā apkopotā veidā ir ievietotas visā ziņojumā aplūkotās un ieteikumi. Rekomendācijas ir strukturētas vairākos līmeņos, pievēršot uzmanību ar telemedicīnas ieviešanu saistīto barjeru pārvarēšanai.

Rekomendācijas normatīvo aktu un rīcībpolitikas plānošanas dokumentu pilnveidei

1. Iesakām papildināt nacionālos normatīvos aktus un/vai politikas plānošanas dokumentos ar precīzākām ar telemedicīnu saistītām terminu definīcijām. Normatīvos aktos (piem., Ārstniecības likumā) iesakām ietvert šādus definējumus:

   c) Digitālā veselība, jo šis tiek lietots kā visaptverošs termins, kas atspoguļotu IKT izmantošanu visās ar sabiedrības veselību un veselības aprūpi saistītās jomās.

   d) Telemedicīna – varētu būt alternatīvs termins, ņemot vērā to, ka šis termins tiek plaši lietots sabiedrībā, lai raksturotu un skaidrotu IKT izmantošanu veselības politikā. Tā kā termins "telemedicīna" jau ir ietverts Ārstniecības likumā, tad ieteicams precizēt un atjaunināt definējumu atbilstoši termina lietojumam praksē.

2. Izslēgt no normatīvajiem aktiem (konkrēti likuma "Par prakses ārstiem") normas, kas aizliedz IKT lietošanu ārstēšanā. Respektīvi likuma "Par prakses ārstiem" 6.pants[102] nosaka, ka prakses ārsts ārstēšanu nedrīkst veikt ar masu saziņas un komunikācijas līdzekļu starpniecību vai sarakstes veidā. Tādējādi, normatīvo aktu starpā (t.i., Ārstniecības likums un likums "Par prakses ārstiem") ir savstarpēja pretruna, kas būtu jānovērš, lai veicinātu telemedicīnas attīstību.

3. Latvijā normatīvajos aktos nav izvirzītas specifiskas prasības telemedicīnas pakalpojumiem, kamēr normatīvie akti paredz regulējumu un definē prasības veselības aprūpes pakalpojumiem, kas tiek sniegti neizmantojot telemedicīnu. Tādējādi, iesakām pilnveidot normatīvo bāzi, pievēršot uzmanību tādiem aspektiem kā piekļuve pacientu datiem, datu koplietošana, pacienta piekrišana, drošība, privātums, datu savietojamība.

Rekomendācijas tehnoloģisko aspektu pilnveidei telemedicīnā

4. Ieteicams veikt digitālo tehnoloģiju izmantošanas izvērtējumu vismaz vienu reizi divos gados, ņemot vērā tehnoloģiju attīstību.
5. Definēt telemedicīnas pakalpojumu IKT drošuma prasības.

[102] Saeima (pieņemts 24.04.1997). *Par prakses ārstiem*. Izgūts no https://likumi.lv/ta/id/43338-par-prakses-arstiem, skatīts 31.10.2020.

6. Palielināt valsts atbalstu un izvērtēt iespējas veikt ESF investīcijas atbalstu IKT nozarei tieši telemedicīnas attīstībai;

7. Noteikt prioritārās veselības aprūpes jomas digitālo tehnoloģiju plašākai izmantošanai, lai veicinātu veselības aprūpes pieejamību. Pasaules pieredze liecina, ka telemedicīnas konsultācijas strauji attīstītaās ambulatorajā veselības aprūpē.

8. Izveidot mobilo lietotni, kur personai ir pieejami visi savi e-Veselības dati. Katram Latvijas medicīnas sistēmas individuālajam lietotājam nodrošināt iespēju savā viedierīcē lietot eVeselības vai tai pieslēgtu citu mobilo lietotni ar ārstu aizpildītiem visiem pacienta datiem, iespēju droši pievienot pacienta citu viedierīču datus (glikozes mērītāji, u.c.), kā arī droši dalīties ar informāciju un spēt pārvaldīt pieejas tiesības saviem medicīnas datiem (piem., nosūtīt rentgenu fizioterapeitam nepametot drošu vidi, visu veicot sistēmas iekšpusē).

9. Veidot valstī vienotu Medicīnas saziņas lietotni (MSL) un portālu vai E-veselības sistēmas sadaļu, kurā pacienti varētu tiešsaistē sazināties ar ārstiem un droši pārsūtīt audio, vizuālo un video informāciju. Paredzēt iespēju MSL saņemto un nosūtīto informāciju ievietot E-veselības sistēmā.

10. Pēc MSL ieviešanas, aizliegt ārstiem un pacientiem lietot citus saziņas rīkus medicīnas informācijas pārsūtīšanai, kuras nav domātas medicīnas informācijas pārsūtīšanai un kuru informācijas glabāšana garantēti neatrodas Eiropas Savienībā.

11. Papildināt E-veselības sistēmu un/vai izveidot jaunu informatīvo portālu par IKT aktualitātēm, problēmām un incidentiem telemedicīnā. Alternatīva varētu būt ar telemedicīnas drošības incidentiem saistīto informāciju ievietot CERT.LV mājaslapā.

12. E-veselības sistēmas nākotnes attīstības plānos paredzēt:

    a) lietojumprogrammas programmēšanas saskarnes visa veida nosūtījumiem un to atbildēm;

    b) iespēju droši saņemt un uzglabāt informāciju no sertificētām valkājamām medicīnas iekārtām (pulss, sirds ritms, skābekļa saturs, asinsspiediens, glikozes līmenis, u.c.), t.sk. hronisku slimību uzraudzībā.

13. Ārstniecības iestādēm un telemedicīnas pakalpojumu sniedzējiem izvērtēt kritisko datu rezerves kopiju veidošanas un glabāšanas opcijas ārpus organizācijas un datu pārraides tīklu segmentāciju.

14. Nākotnē veselības aprūpē izmantot Zoom programmatūras veselības aprūpei paredzēto moduli, jo Zoom izstrādātājs ir jau pielāgojis savu platformu medicīnas pakalpojumu sniedzējiem. Savukārt, WebEx nodrošina pārāk šaurus datu centrus bez iespējām apstrādāt sapulču datus. Ziņojumapmaiņai ne lietotne WhatsApp, ne Signal nav piemērotas telemedicīnas vajadzībām, to izmantošana potenciāli pārkāpj Vispārīgās

datu aizsardzības regulas nosacījumus. Kā alternatīvu var izpētīt Tiger Connect (https://tigerconnect.com/about/) vai izveidot vietējo ziņojumapmaiņas lietotni, kas varētu iekļaut pašreizējo ziņojumapmaiņas lietotņu labākos aspektus un kuras ieviešanā tiktu ņemti vērā Latvijas Republikas un Vispārīgās datu aizsardzības regulas aizsardzības pasākumi.

15. Ņemot vērā ģimenes ārstu darba specifiku, it īpaši Covid-19 krīzes laikā, lai paaugstinātu ģimenes ārsta laiku tiešam pacienta kontaktam vizītes laikā un nodrošinātu drošu vidi kā arī lai pasargātu pacienta datus, nepieciešams izveidot vienotu IT ekosistēmu ārstu praksēm, kura ietvertu centralizētu datortehnikas apkalpošanu, programmatūras atjauninājumu pārvaldību komplektā ar valsts nodrošinātu pārvaldītu medicīnas datu mākoņpakalpojumu ģimenes ārstiem. Datortehnikas apkalpošanai un programmatūras atjauninājumu pārvaldībai par saprātīgām izmaksām ir nepieciešams izstrādāt vienotu datortehnikas un programmatūras bāzes standartu. Katrs ģimenes ārsts saņemtu valsts apmaksātu datoru, kura specifikācijas un funkcionalitāte paredzētu:

    a) augstas kvalitātes datoru, kuru iespējams lietot vismaz 4 gadus ģimenes ārstu praksē;

    b) vismaz *Full HD* spēja ekrāna kvalitātei, lai nodrošinātu iespējamu strādāt ar rentgena, ultrasonogrāfijas u.c. attēliem; vismaz Full HD spēja ekrāna kvalitātei, lai nodrošinātu iespēju strādāt ar rentgena, ultrasonogrāfijas, datortomogrāfijas un citiem vizualizētajiem izmeklējumu attēliem

    c) spēja lietot gan jaunāka tipa WiFi standartus un 4G/5G mobilo internetu;

    d) kvalitatīva video kamera un mikrofons, lai spētu lietot videokonferences programmas;

    e) centralizēta programmatūra datortehnikas un programmatūras atjauninājumu pārvaldībai.

    f) Operētājsistēmai rekomendējam atbilstību šādām spējām un funkcijām:

        - maksimāli ierobežotai Telemetrijas funkcijai, lai pasargātu pacientu datu noplūdi uz programmatūras ražotāja vidi, analīzei ko neparedz Latvijas likumdošana;
        - programmatūras atjaunojumi nedrīkst izjaukt darba vidi ārsta praksē. Atjaunojumi jātestē, lai pārliecinātos par to saderību ar ģimenes ārstu vidi. IT dienests šādus testus varētu veikt centralizēti un, pēc sekmīgiem testiem, nosūtīt atjaunojumu uz ģimenes ārstu datoriem.
        - Tuvākais analogs ir Microsoft Windows 10 Enterprise 2019 LTSC.

16. Veidojot vienotu iekārtas un programmatūras platformu tiktu samazināts nesankcionētas piekļuves risks veselības aprūpes IKT infrastruktūrai un datiem, uzlabota vispārējā ārsta prakses efektivitāte, pacientu apkalpošanas kvalitāte, kā arī panākta veselības aprūpes sistēmas stiprināšana no informācijas drošības aspekta. Tas

savukārt samazina valsts un ģimenes ārsta prakses neplānotus izdevumus, kuri ir saistīti ar nevienmērīgu IT nodrošinājuma platformu.

Rekomendācijas organizatorisko faktoru pārvarēšanai

17. Uzlikt par pienākumu visām analīžu, radioloģijas un citu izmeklējumu veicējiem ievietot rezultātus E-veselības sistēmā, tā veidojot E-veselību kā vienotu datu uzkrāšanas platformu Latvijā.

18. Apsvērt iespēju izmantot publiskās privātās partnerības sadarbību, lai mudinātu privāto sektoru iesaistīties telemedicīnas attīstībā.

19. Ģimenes ārstiem, dodot laiku līdz 2022. gada 1. jūnijam, aizpildīt E-veselības sistēmā paredzētos pacienta kartes laukus – alerģijas, brīdinājumi, medikamenti, medicīniskās ierīces un vakcinācijas dati.

Rekomendācijas cilvēcisko faktoru pārvarēšanai

20. Veidot komunikācijas un izglītojošas kampaņas par telemedicīnas ieguvumiem un pakalpojuma drošības nosacījumiem;

21. Motivēt iedzīvotājus lietot telemedicīnas pakalpojumus, kur nozīmīgākais uzdevums ir uzlabot iedzīvotāju digitālās prasmes, palielinot sabiedrības uzticēšanos un atbalstu digitālās veselības risinājumu izmantošanai. Piem., Igaunijā telemedicīnas attīstība ir tiešā veidā saistīta ar iedzīvotāju digitālo pratību.

22. Veicināt digitālo tehnoloģiju pieejamību lauku reģionos un mazāk aizsargātām sociālām grupām un lietošanu arī krīzes situācijās, tā stiprinot sabiedrības veselības spēju atjaunoties (angl. *resilience*),

23. Stiprināt cilvēkresursus veselības aprūpes jomā, veidojot medicīnas personālam nepieciešamos telemedicīnas standartus;

24. Integrēt praktiskas telemedicīnas zināšanas medicīnas studiju procesā dažādos izglītības līmeņos.

25. Izglītot medicīnas personālu, IT personāla un atbalsta personālu veselības aprūpē:

    a) piedāvājot kursus un seminārus par telemedicīnas ierīču,tehnoloģiju un metožu drošu izmantošanu.

b) organizēt vairāku posmu valsts atbalstītas ārstu prakšu IKT prasmju apmācības un regulāras zināšanu pārbaudes.
c) par pikšķerēšanu un sociālās inženierijas uzbrukuma metodēm, kā arī kibernoziegumiem
d) par digitālās kriminālistikas gatavības nozīmi ļaunatūras seku mazināšanā;

1.pielikums. Ārvalstu prakse apkopojums

Piezīme: Ārvalstu prakses apkopojums atspoguļo tikai galvenās tendences attiecīgajā valstī, un tas nav pamats rīcībpolitikas pārcelšanai vai tās elementu pārcelšanai uz Latviju.

Zviedrija

Rīcībpolitikas mērķis

Zviedrijas e-Veselības vīzija līdz 2025.gadam nosaka: "*2025. gadā Zviedrija būs labākā pasaulē, izmantojot digitalizācijas un e-Veselības piedāvātās iespējas, lai cilvēkiem būtu vieglāk sasniegt vienlīdzību veselības aprūpē un labklājībā, kā arī attīstīt un stiprināt savus resursus, lai palielinātu neatkarību un līdzdalību sabiedrības dzīvē.*"[103]

Regulējums

Pirmā e-Veselības stratēģija Zviedrijā tika pieņemta 2006. gadā (t.i., Nacionālā IT stratēģija veselībai un sociālajai aprūpei, kas tika aktualizēta 2010. gadā, apstiprinot Nacionālo eVeselības stratēģiju)[104]. 2016. gadā tika izstrādāta e-Veselības vīzija 2025 (turpmāk tekstā – e-Veselība) un rīcības plāns, kas noteica , ka rīcībpolitikas un regulējuma uzdevums e-Veselībā (t.i., telemedicīnā) ir panākt līdzsvaru starp personas privātumu, pakalpojumu kvalitāti, drošību un efektivitāti. Pie tam, tiesību aktiem un citiem noteikumiem ir jāgarantē dažādas indivīda tiesības un intereses. Vienlaikus e-Veselības vīzijas plāns uzsver nepieciešamību investēt telemedicīnas infrastruktūrā un to attīstīt, lai nodrošinātu privātumu un drošību.

Galvenais akcents e-Veselības 2025. gada vīzijā ir likts uz mērķi izveidot tādu regulējumu, kas no vienas puses spēs pasargāt indivīda drošību, bet no otras puses, ārstiem ļaus sniegt nepieciešamos veselības pakalpojumus. Šī iemesla dēļ vīzijā ir izvirzīti divi galvenie uzdevumi, kas saistīti ar telemedicīnas regulējumu:

1) izveidot atbilstošus noteikumus, kas gan garantē personas privātumu un drošību, kā arī veicina veselības aprūpes sistēmas digitālo pārveidi;
2) attīstīt digitālās prasmes visos veselības aprūpes līmeņos;

[103] *Vision for eHealth 2025 – common starting points for digitisation of social services and health care*. (2016.). Izgūts no: https://www.government.se/4a3e02/contentassets/b0fd09051c6c4af59c8e33a3e71fff24/vision-for-ehealth-2025.pdf , 3.lpp. , skatīts 30.11.2020.
[104] *Vision for eHealth 2025 – common starting points for digitisation of social services and health care.* (2016.). Izgūts no: https://www.government.se/4a3e02/contentassets/b0fd09051c6c4af59c8e33a3e71fff24/vision-for-ehealth-2025.pdf , 7.lpp. , skatīts 30.11.2020.

3) nodrošināt IT atbalstu telemedicīnas pakalpojumu attīstībai ievērojot kvalitātes vadības nosacījumus.[105]

Piedāvātie pakalpojumi

Šobrīd Zviedrija piedāvā dažādus telemedicīnas pakalpojumus - ir iespējams attālināti pierakstīties vizītei un konsultācijām, saņemt pakalpojumus un izmeklējumu rezultātus. Zviedrijas digitālās veselības uzņēmums KRY ir šobrīd viens no lielākajiem telemedicīnas pakalpojumu sniedzējiem ne tikai Zviedrijā, bet arī Eiropā[106]. 2015.gadā KRY tika izveidota digitālās veselības aplikācija, kas ļauj saņemt ārstniecības personas konsultācijas izmantojot viedtālruni vai planšeti[107].

Nīderlande

Rīcībpolitikas mērķis

Nīderlandes valdība vēlas, lai e-Veselība kļūtu plašāk pieejama un mudina veselības aprūpes nozari to attīstīt tālāk, izvirzot šādus mērķus:[108]

1) Piekļuve medicīniskajai dokumentācijai

Līdz 2019. gadam vismaz 80% pacientu ar hroniskām slimībām vajadzētu spēt piekļūt saviem medicīniskajiem dokumentiem un datiem elektroniski. Pārējiem pacientiem šim rādītājam jāsasniedz vismaz 40%.

2) Veselības uzraudzība

Līdz 2019. gadam 75% pacientiem ar hroniskām slimībām un vecāka gadagājuma cilvēkiem jābūt nodrošinātai iespējai uzraudzīt atsevišķus savus veselības rādītājus (piem., asinsspiediens, glikozes līmenis, holesterīna līmenis) un apmainīties ar datiem ar veselības aprūpes pakalpojumu sniedzēju.

3) Tiešsaistes kontakts ar aprūpes pakalpojumu sniedzēju

Tiem iedzīvotājiem, kas saņem aprūpi mājās (gan veselības, gan sociālo) tiek nodrošināta iespēja sazināties ar savu aprūpes pakalpojumu sniedzēju 24 stundas diennaktī, izmantojot videozvanu.

Lai sasniegtu šos mērķus, Nīderlandē tiek veikti sekojoši pasākumi:

a) Atbalsts jaunām idejām, izmantojot tiešsaistes platformu

Veselības aprūpes jomas inovatori un jaunuzņēmumi, kas vēlas izveidot jaunu digitālo lietojumprogrammu, var doties uz mājaslapu *zorgvoorinnoveren.nl*, kur viņi saņems atbalstu,

[105] *Strategy 2020-2022*. Izgūts no: https://ehalsa2025.se/bilagor/strategy-2020-2022/, 10.lpp., skatīts 30.11.2020.

1 [106] Charlotte Tucker. Stockholm-based KRY secures €140 million to expand its health app for online doctor appointments. January 7, 2020 https://www.eu-startups.com/2020/01/stockholm-based-kry-secures-e140-million-to-expand-its-health-app-for-online-doctor-appointments/ skatīts 30.11.2020.

[107] KRY. *How to use Kry*. Izgūts no: https://www.kry.se/en/, skatīts 30.11.2020.

[108] *Government encouraging use of eHealth.* Izgūts no: https://www.government.nl/topics/ehealth/government-encouraging-use-of-ehealth, skatīts 30.11.2020.

lai palīdzētu ātri un efektīvi attīstīt ideju līdz strādājošai lietojumprogrammai. Vietnē tiek piedāvāti arī padomi un norādījumi par finansējuma iegūšanu idejas attīstībai.

b) Digitālo datu koplietošanas atvieglošana

Valdība apspriežas ar veselības administratoriem par standartiem, kuriem butu jāveicina digitālo datu koplietošana. Viņi runā arī ar IT sistēmu piegadātājiem.

c) Dalīšanās ar e-Veselības zinātību ("know-how")

Nīderlandes valdība lielu uzmanību pievērš sadarbībai un domu apmaiņai starp inovāciju autoriem un citām iesaistītajām pusēm. Tā piemēram, Nīderlandē ir izveidots jaunuzņēmumu tīkls, kas ietver, veselības aprūpes pakalpojumu sniedzējus, pacientus un juristus. Tīkls ļauj viņiem dalīties zināšanās un palīdzēt jaunuzņēmumiem attīstīt inovācijas kvalitatīvi jaunā pakāpē.

d) Sabiedrības izpratnes palielināšana

Veselības aprūpes rīcībpolitikas ietvaros regulāri tiek veikti pasākumi, lai uzlabotu veselības aprūpes speciālistu un pacientu informētību par e-Veselību.

e) Personiskā digitālā veselības aprūpes vide

2016. gadā Nīderlandes veselības aprūpes nodrošināšanā iesaistītās puses (politikas veidotāji, pakalpojumu sniedzēji, IT uzņēmumi) vienojās par standartiem un pamatprasībām attiecībā uz personas digitālo veselības aprūpi. Tas rada iespēju piegādātājiem izstrādāt drošus, uzticamus, lietotājiem draudzīgus produktus, kā arī ļauj ikvienam droši apkopot un dalīties ar savu veselības informāciju tiešsaistē.

Regulējums:

Nīderlandes veselības aprūpes sistēma tika decentralizēta 2015. gadā. Kopš tā laika 380 pašvaldības ir atbildīgas par veselības aprūpes politikas ieviešanu. Tajā pat laikā, tiek ievērots, ka maksimālu efektivitāti ir iespējams panākt iesaistot visas ieinteresētās puses. Pacienti un pacientu organizācijas tieši tiek iesaistītas politikas veidošanas procesā. Arī apdrošinātājiem kā veselības aprūpes finansētājiem ir nozīmīga loma dažādu aprūpes politiku veidošanā.[109]

Nīderlandes valdība lielu uzmanību pievērš digitalizācijas uzlabošanai veselības jomā. Veselības, labklājības un sporta ministrija ir paziņojusi par juridiska ietvara izveidošanu kopš 2019.gada vidus, kas paredz obligātu medicīnisko datu apmaiņu starp visiem aprūpes sniedzējiem,. Šī obligātā pasākuma iemesls bija medicīnas datu apmaiņas lēnā attīstība un uzlabošanās. Tika konstatēts, ka dažādi aprūpes pakalpojumu sniedzēji izmanto dažādu terminoloģiju vieniem un tiem pašiem jēdzieniem, kas padarīja datu apmaiņu neiespējamu. Regulējuma mērķis ir terminoloģijas un procesu harmonizēšana[110]

Nīderlandes Standartizācijas institūts ir noteicis kritērijus veselības aprūpes sniedzējiem un iestādēm, kas izmanto telemedicīnu. Pārņemot Eiropas Medicīnas ierīču direktīvu

[109] Embassy of the Kingdom of the Netherlands in Berne, Switzerland (2019). *The Digital Health market in the Netherlands and Switzerland* . Izgūts no: https://www.rvo.nl/sites/default/files/2019/03/the-digital-health-market-in-the-netherlands-and-switzerland.pdf, 13.lpp., skatīts 30.11.2020.
[110] Turpat.

93/42/EEG, ir izdots Medicīnisko ierīču likums (“Wet op de medische hulpmiddelen”)un ar to saistītais dekrēts par medicīnas ierīcēm (“Besluit medisch hulpmiddelen” Atbilstoši šim regulējumam, arī programnodrošinājums tiek uzskatīts par medicīnisku ierīci. Veselības aprūpes iestādes, kas darbā izmanto telemedicīnu, ir atbildīgas par to, lai nodrošinātu drošu telemedicīnas lietošanu atbilstoši normatīvajam ietvaram. [111]

Ārstniecības līgumu likums (“Wet op de geneeskundige behandelingsovereenkomst”) ir tiesību akts, kas regulē attiecības starp veselības aprūpes sniedzēju un saņēmēju līdzās regulējumam par personas datu apstrāde veselības aprūpes jomā (“Wet op thulingulingw thulenenenening”). Abi tiesību akti nodrošina Vispārīgās datu aizsardzības regulas prasību izpildi, jo īpaši pievēršoties personas datu aizsardzībai veselības aprūpes nozarē.[112]

Nīderlandes valdība uzrauga digitālo norišu gaitu veselības aprūpes nozarē, kā arī monitorē, vai un kā tiek sasniegti sākotnēji noteiktie mērķi. Katru gadu tiek veikts apsekojums par to, cik iedzīvotāju izmanto e-Veselības pakalpojumus un kā mainās telemedicīnas konsultāciju proporcijas pret klātienes konsultācijām.[113] Būtiski, ka katrs pacients Nīderlandē var izmantot telemedicīnas pakalpojumus citās ES valstīs, un katrs pacients no citas ES valsts var izmantot telemedicīnas pakalpojumus Nīderlandē [114].

Piedāvātie pakalpojumi

Ir izveidota Nīderlandes personiskā digitālā veselības aprūpes vide. Tā ir vieta, kur katrs var glabāt visu medicīnisko informāciju: no aprūpes pakalpojumu sniedzējiem, no saviem medicīniskajiem pierakstiem un lietotnēm, kas monitorē veselību un, piemēram, vingrinājumus, kas jāveic. Tā ir tiešsaistes vide, kurai var piekļūt tikai lietotājs. Lietotāja paša ziņā ir tas, ar ko koplietot šo informāciju.[115]

Nīderlandē tiek īstenota programma pensionāriem “ilgāk mājās.” Šī programma vērsta uz lielo un augošo vecāka gadagājuma cilvēku grupu, kuri mājās dzīvo patstāvīgi. Idejas pirmssākumi ir meklējami vecāku gadagājuma cilvēku vēlmē turpināt dzīvot patstāvīgi, tik ilgi cik vien iespējams, ar atbalstu, gādību un mājās, kas atbilst viņu personīgajām vajadzībām. [116]

Nīderlandē pieejama e-diagnostika, e-konsultācijas, e-aprūpe, piemēram, monitorings, e-profilakses pasākumi cilvēkiem ar augstu saslimšanas risku.[117]

---

[111] Osborne Clarke. (2020). 2. Laws (or other mandatory rules – like professional code of conduct) covering telemedicine . Izgūts no https://www.osborneclarke.com/wp-content/uploads/2020/05/H_2004141116LSH_Telemedicine-Questionnaire_v03.pdf, 13.lpp., skatīts 29.11.2020.

[112] Turpat.

[113] *Government encouraging use of eHealth.* Izgūts no https://www.government.nl/topics/ehealth/government-encouraging-use-of-ehealth, skatīts 29.11.2020.

[114] Osborne Clarke. (2020). *2. Laws (or other mandatory rules – like professional code of conduct) covering telemedicine* . Izgūts no https://www.osborneclarke.com/wp-content/uploads/2020/05/H_2004141116LSH_Telemedicine-Questionnaire_v03.pdf, 49.lpp., skatīts 29.11.2020.

[115] *What is a personal digital healthcare environment?* https://www.government.nl/topics/ehealth/question-and-answer/what-is-a-personal-digital-healthcare-environment

[116]*Living independently for longer*. Izgūts no: https://www.government.nl/topics/care-and-support-at-home/living-independently-for-longer skatīts 29.11.2020.

[117] *Reimbursement of telemedicine and digital care in the Netherlands* Izgūts no: https://mtrconsult.com/news/reimbursement-telemedicine-and-digital-care-netherlands, skatīts 29.11.2020.

Polija

Rīcībpolitikas mērķis:

Attiecībā uz telemedicīnu, Polijā nav definēts atsevišķs rīcībpolitikas mērķis.

Regulējums

Polijā nav normatīvo aktu, kas tieši reglamentētu attālināto veselības aprūpes pakalpojumu sniegšanu. Nav arī nekādu izteiktu aizliegumu. Neraugoties uz trūkumiem tiesiskajā regulējumā un konservatīvo pieeju medicīnas jomas profesiju profesionālās darbības reglamentācijai, dažas pētniecības iestādes un universitātes ir uzsākušas projektus, kuru pamatā ir telemedicīnas risinājumi, piemēram, tādi projekti ietver telekonsultācijas un telerehabilitāciju[118]

Piedāvātie pakalpojumi

Polijā telemedicīnas izplatīšanas iniciatīvas galvenokārt ir vērstas uz sistēmu izstrādi un ieviešanu EKG signālu sūtīšanai pa tālruni (tostarp ar mobilajiem telefoniem), rentgena fotoattēlu, USG un CT attēlu efektīvai nosūtīšanai caur iekštīklu vai internetu konsultāciju nolūkos, kā arī efektīvu datu bāzu un nepieciešamo sistēmu organizēšanu un piekļuves kontroli šīm informācijas bankām.

Ir pieejamas jaunas telemedicīnas tehnoloģijas, kas ir valsts un privātā sektora sadarbības rezultāts. Piemēram, kardiotelerehabilitācija (*Kos-infarction* (*KOS; pol. Kompleksowa Opieka po Zawale Mięśnia, visaptveroša aprūpe pēc sirdslēkmes*)) neierobežota pēcinfarkta aprūpes nodrošināšana, kas ietver vienu gadu ilgu ārstēšanas atbalstu pacientiem pēc sirds saslimšanas.[119] Tomēr, lielākā daļa pakalpojumu vēl ir tikai izstrādes stadijā, tādēļ šobrīd Polijā pacientiem ir pieejama e-recepte un e-nosūtījums un lēnām tiek ieviestas telekonsultācijas.[120]

2018. gadā tika ieviestas e-receptes. Šis projekts bija pirmais valstī, un neskatoties uz kļūdām un problēmām, ir uzskatāms par ievērojamu Polijas telemedicīnas sasniegumu. Elektroniski tiek izsniegtas arī darba nespējas lapas. No 2018. gada 1. decembra darba nespējas lapas ir obligāti jāizsniedz elektroniskā veidā. Šīs funkcionalitātes galvenais mērķis ir atvieglot

[118]Cross-border telemedicine: A distant vision or the immediate future? Izgūts no http://bpcc.org.pl/contact-magazine/issues/8/categories/31/articles/259, skatīts 30.11.2020

[119] Turpat. 42.lpp.

[120] The first News. *Poland's healthcare system is going through a revolution*. Izgūts no https://www.thefirstnews.com/article/polands-healthcare-system-is-going-through-a-revolution-7928, skatīts 29.11.2020.

slimību lapu apstrādi, samazināt kļūdas, optimizēt laiku no ārstu un pacientu puses un novērst neskaidrības.[121]

Kopumā, jāmin četri projekti, kas saistīti ar telemedicīnu Polijā pēdējos piecos gados:[122]

1.projekts - Medicīnisko resursu apkopošanas, analīzes un piekļuves elektroniskā platforma. Paredz IT sistēmu ieviešanu, lai racionalizētu procesus, kuri saistīti ar veselības aprūpes pakalpojumu sniegšanas plānošanu un uzraudzību, piekļuvi informācijai par sniegtajiem pakalpojumiem un informācijas publicēšanu veselības aizsardzības jomā.

2.projekts – platforma, kas sniedz iespēju e-pārvaldes pakalpojumus uzņēmējiem integrēt veselības aprūpes jomā. Šī projekta rezultātā ir izstrādāts investīciju pieteikumu novērtēšanas instruments, kas ļauj saņemt atzinumu par ieguldījumu lietderību.

3. projekts - kvalitātes vadības uzlabošana veselības aprūpē. Šis projekts paredzēts veselības aprūpes pārvaldības kvalitātes uzlabošanai, popularizējot zināšanas par IT tehnoloģiju izmantošanu ārstniecības personām un medicīnas iestādēs strādājošajiem.

4.projekts – domēna informācijas un sakaru sistēmu izveidošana. Projekts ietver pamatdarbības procesu pilnveidošanu, kas saistīti ar piekļuvi statistikas datiem, nelabvēlīgas ārstniecības gadījumu ietekmi, zāļu apriti, veselības stāvokli un medicīniskā personāla resursiem[123].

IGAUNIJA

Rīcībpolitikas mērķis

Igaunijas eVeselības Stratēģiskās attīstības plānā līdz 2020.gadam ir definēts stratēģiskais mērķs: **"labāka informācija- vairāk veselības"** [124]. Šī mērķa sasniegšanai ir nepieciešams attīstīt pamata kompetences un pakalpojumu inovācijas, ko atbalsta tehnoloģijas šādos pamatvirzienos:

Veselības datu jomā: "*no cilvēkiem savāktie dati par veselību vienmēr ir kvalitatīvi*". Pamatojoties uz datiem, ir iespējams iegūt visaptverošu pārskatu par visu, kas saistīts ar cilvēka veselību: laika skalā sākot ar informāciju par ģenētiku, rādītājiem, kas raksturo veselības stāvokli, veselības uzvedības īpatnībām līdz vides informācijai (t.i., informāciju no mums, par mums un par mūsu vidi). Datu izmantošana vienmēr ir pārredzama un kontrolēta, un dati tiek aktīvi izmantoti visos veselības aprūpes posmos, ieskaitot pētniecību.[125]

---

[121] Bukowski,H. Pogorzelczyk, K. *Polish Healthcare Sector.* Izgūts no https://www.innowo.org/userfiles/publikacje/Polish%20Healthcare%20Sector.pdf, 40.lpp., skatīts 29.11.2020.
[122] Bukowski,H. Pogorzelczyk, K. *Polish Healthcare Sector.* Izgūts no: https://www.innowo.org/userfiles/publikacje/Polish%20Healthcare%20Sector.pdf 38.-39.lpp., skatīts 29.11.2020
[123] Pro Plus. *Telemedicine.* Izgūts no http://www.pro-plus.pl/en/telemedicine, skatīts 29.11.2020.
[124] *Estonian eHealth Strategic Development Plan 2020.* Izgūts no https://www.sm.ee/sites/default/files/content-editors/sisekomm/e-tervise_strateegia_2020_15_en1.pdf 6.-7. lpp., skatīts 29.11.2020.
[125] Turpat. 6.lpp.

Veselības aprūpes pakalpojumu jomā : "*veselības aprūpes pakalpojumi vienmēr ir orientēti uz cilvēkiem un atbilstoši*". Mērķis paredz, ka veselības aprūpes pakalpojumi ir izmantojami neatkarīgi no patērētāju atrašanās vietas un viņu spējām izmantot ICT. Dažādu līmeņu pakalpojumi un pakalpojumu sniedzēji ir savstarpēji cieši saistīti: katrs cilvēka veselības jautājums tiek risināts vispusīgi; speciālistu starpā pārvietojas tikai dati (nevis persona). Veselības pakalpojumu efektivitāte ir personalizēta un labāk izmērāma. Tiek nodrošināta pastāvīga atgriezeniskā saite starp personu un speciālistu katrā procesa stadijā, kā arī slimības gaitā kopumā.[126].

Veselības aprūpes sistēmas jomā mērķis ir ievērojami palielināt iespējas slimību profilaksei, lai cilvēki pie ārsta vēršas tikai sarežģītu jautājumu gadījumā. Izejas informācija veselības rīcībpolitikas attīstībai ir pārskatāmāka un pieejamāka, kas noved pie labāk pamatotiem un ātrākiem lēmumiem, nodrošinot optimālu resursu izlietojumu visos līmeņos. E-Veselības risinājumi ir kļuvuši par lielu palīdzību speciālistam: dati un atbalsts uz pierādījumiem balstītiem lēmumiem nekavējoties pieejami speciālistiem visur. Lai to sasniegtu, datu ievadīšana sistēmās ir vienkārša. Turklāt, sistēmā nepārtraukti tiek veikti pastāvīgi jauninājumi visos līmeņos: jaunu risinājumu testēšana un ieviešana, lai uzlabotu pakalpojumu efektivitāti un sistēmas efektivitāti.

Piedāvātie pakalpojumi

Katram cilvēkam Igaunijā, kurš apmeklējis ārstu, ir tiešsaistes e-Veselības lapa, kur var sekot līdzi visai informācijai (slimības gaitai, ārstēšanas taktikai). Elektroniskajā ID-kartē identificētā informācija par veselību tiek glabāta pilnīgi droši un tajā pašā laikā pieejama pilnvarotām personām. Veselības aprūpes sistēma izmanto *KSI Blockchain* tehnoloģiju, lai nodrošinātu datu integritāti un mazinātu iekšējos datu apdraudējumus.[127]

E-Veselības sistēmā tiek uzglabāti dati no dažādiem pakalpojumu sniedzējiem, kuri, iespējams, izmanto dažādas sistēmas, bet e-Veselības portālā tos augšuplādē standartizētā formātā. Šis rīks ārstiem ļauj viegli piekļūt pacienta ierakstiem neatkarīgi, kura ārstniecības iestāde vai medicīnas pakalpojumu sniedzējs ir sagatavojis datus (piem., attēlus, analīžu rezultātus) Piemēram, ārkārtas situācijā ārsts var izmantot pacienta identifikācijas kodu, lai nolasītu svarīgu informāciju, piemēram, par asins tipu, alerģijām, nesenu ārstēšanu, zālēm vai grūtniecību. Sistēma arī apkopo datus par valsts statistiku, lai atbildīgā ministrija varētu novērtēt veselības tendences, izsekot epidēmijām un nodrošināt, ka tās veselības resursi tiek tērēti efektīvi.[128]

Pacientiem ir pieejami viņu pašu, nepilngadīgo bērnu un trešo personu dati, kuras tam ir devušas atļauju. Piesakoties e-pacientu portālā (https://www.digilugu.ee/login?locale=en) ar elektronisku ID-karti, pacients var pārskatīt ārstu apmeklējumus un pašreizējās receptes, kā arī pārbaudīt, kuriem ārstiem ir bijusi piekļuve viņa datiem.[129] Šobrīd Igaunijā iespējams saņemt tādus telemedicīnas pakalpojumus kā e-Veselības ieraksti, e-ambulance, kā arī e-receptes.[130]

[126] Turpat, 6-7.lpp.
[127] E-estonia. *Healthcare*. Izgūts no: https://e-estonia.com/solutions/healthcare/e-health-record/, skatīts 02.12.2020.
[128] E-estonia. *Solutions.* Izgūts no:https://e-estonia.com/solutions/healthcare/, skatīts 02.12.2020.
[129] Turpat.
[130] Turpat.

Secinājumi

1. E-Veselības (telemedicīnas) risinājumu ieviešana ir katras Eiropas savienības dalībvalsts kompetence un līdz ar to, attīstības līmenis šajā jomā ir ļoti dažāds. Tajā pat laikā redzama tendence, ka šo risinājumu pielietojums pieaug.
2. Normatīvā regulējuma jomā situācija dalībvalstīs ir atšķirīga, taču visas iesaistītās puses pievērš uzmanību Eiropas savienības regulas Nr. 2016/679 „Par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula)" prasībām.
3. Datu apmaiņas risinājumu izmantošana un pacientu datu uzkrāšana ir viens no attīstības virzieniem visu apskatīto valstu rīcībpolitikās. Tāpat politikas plānošanas līmenī uzmanība tiek pievērsta datu drošības, pieejamības un izmantošanas kontroles aspektiem.
4. Kopīga tendence ir tehnisko risinājumu attīstīšana, kas saistīta ar veselības aprūpes pakalpojumu administrēšanu un ar to saistītajiem pakalpojumiem. Tādi risinājumi kā e-receptes un elektroniskas darba nespējas lapas tiek ieviesti visās pētījumā apskatītajās valstīs.

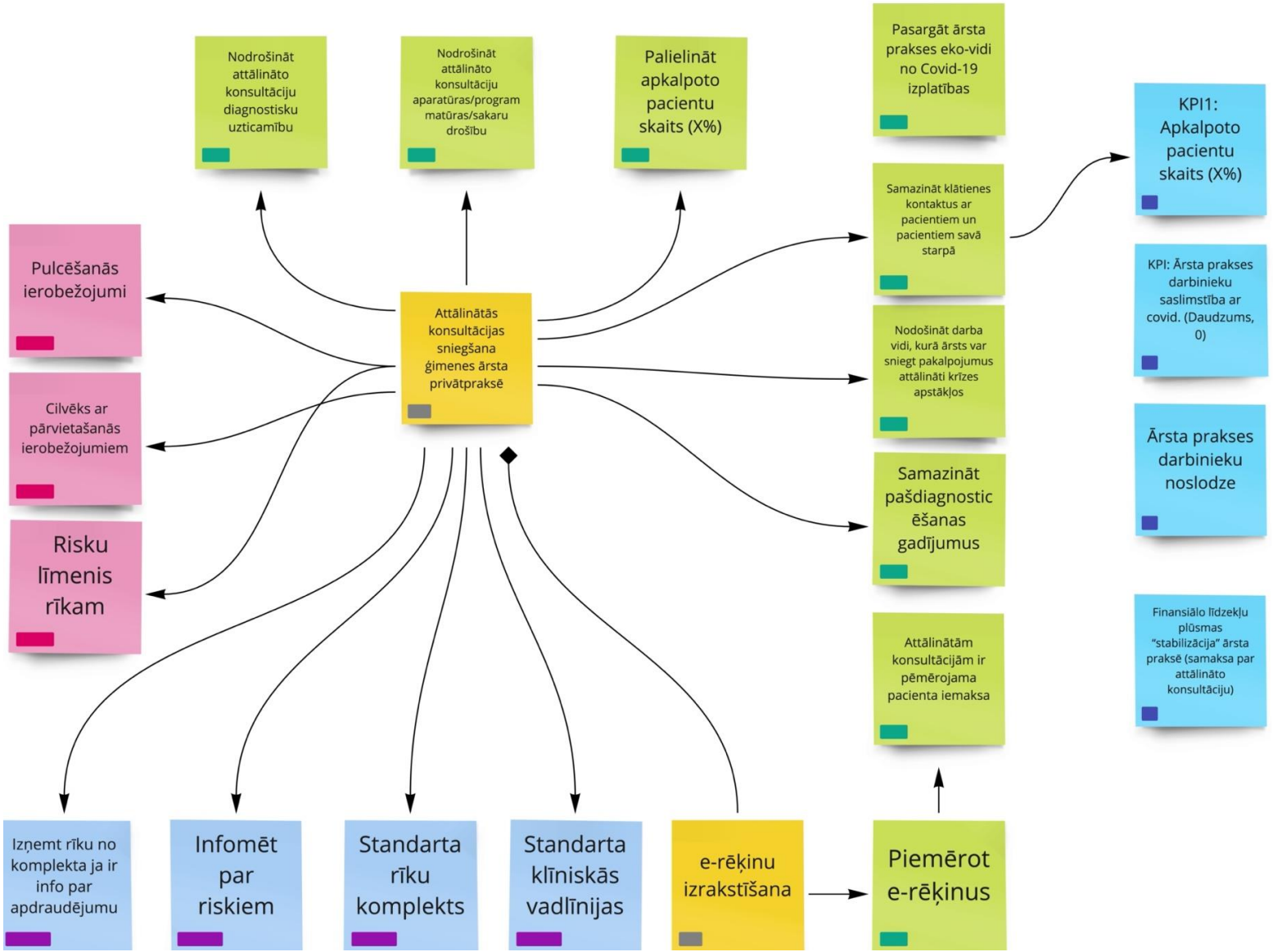
2.pielikums. Modeļu izvērsums un elementu skaidrojumi atbisltoši ARTSS metodei

ARTSS metodes pamatjēdzieni ir aprakstīti 1. tabulā. Metodes komponenti izmanto šos kopējos jēdzienus, un nepieciešamības gadījumā metodes komponentiem tiek pievienoti papildus jēdzieni. Detalizēts ARTSS metodes apraksts ir ievietos projekta mājas lapā pēc adreses: https://artss.rtu.lv/lv/ARTSSmetode

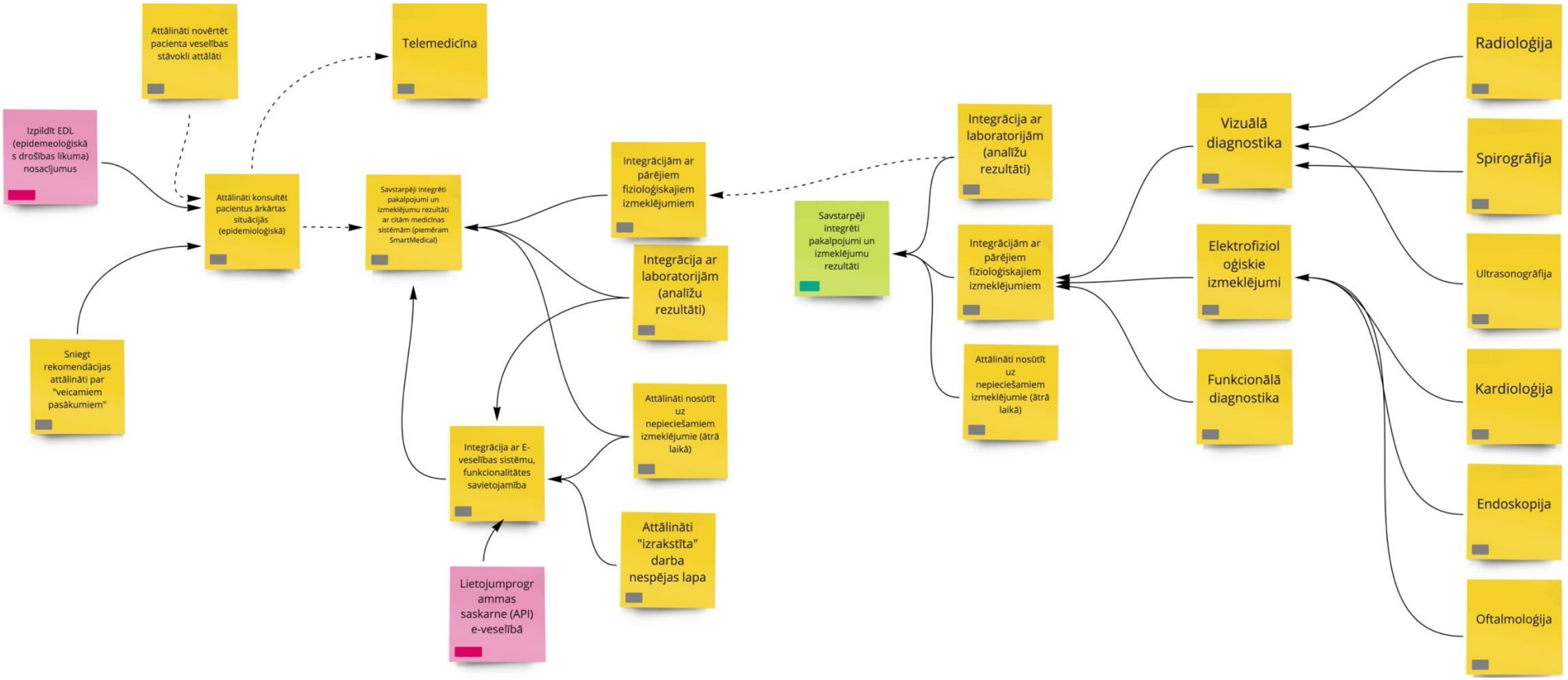
1. tabula. ARTSS metodes pamatjēdzienu apraksts

Koncepts	Apraksts
Pielāgojums *Adjustment*	Algoritmiska rekomendācija spējas pielāgošanai atbilstoši konteksta situācijai
Spēja *Capability*	Varēšana un kapacitāte sasniegt organizācijas mērķus mainīgos kontekstuālos apstākļos
Konteksta elements *Context Element*	Uz datiem balstīta informācija, kas raksturo situāciju, kurā sistēma darbojas.
Digitālais dvīnis *Digital twin*	Kontrolei un analīzei izmantojams reālā servisa nodrošināšanas tīkla attēlojums virtuālajā vidē
Ekosistēma *Ecosystem*	Visu drošu un noturīgu servisu nodrošināšanu ietekmējošo iesaistīto pušu kopums
Mērķis *Goal*	Mērķis ir dažādu lietu un apstākļu vēlamais stāvoklis, kuru nepieciešams sasniegt.
KPI	Skaitlisks rādītājs, mērķa sasniegšanas mērs
Mācīšanās modulis	Nodrošina apmācību par servisa drošu izmantošanu
Mērāmu datu vienība *Measurable property*	Spējas nodrošināšanas un servisa darbības vides mērījumi
Tīkls	Servisa nodrošinātāju kopumus
Šablons	Strukturētas, atkāroti izmantojamas zināšanas par drošu un noturīgu servisu izstrādi un darbināšanu
Drošības aspekts	Mērķa specializācija, kas attēlo drošības mērķus
Serviss	Komponents, kas, nodrošina noteiktu funkcionalitāti atbildot uz partnera pieprasījumu

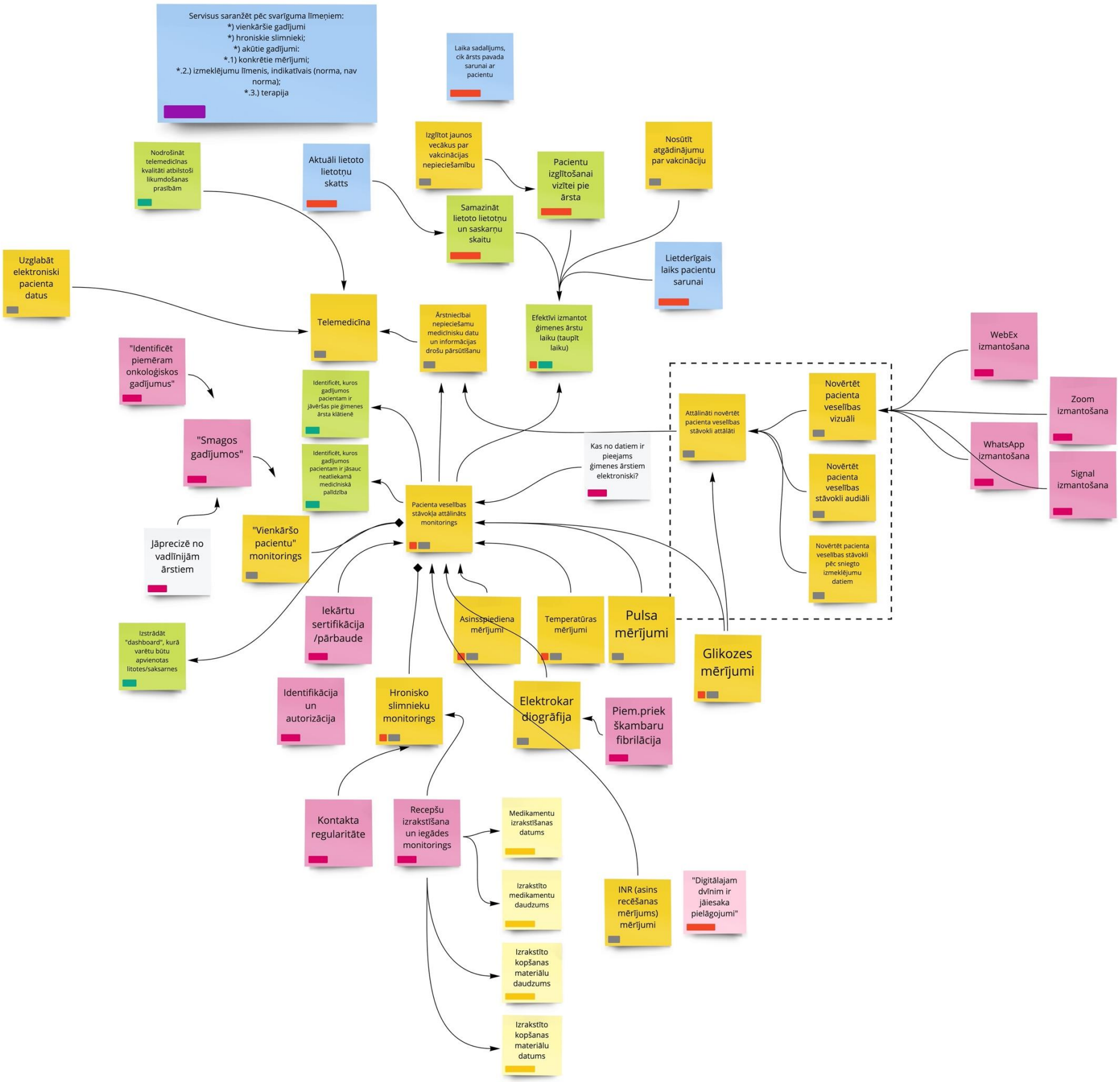
Spēju apzināšanas notācija



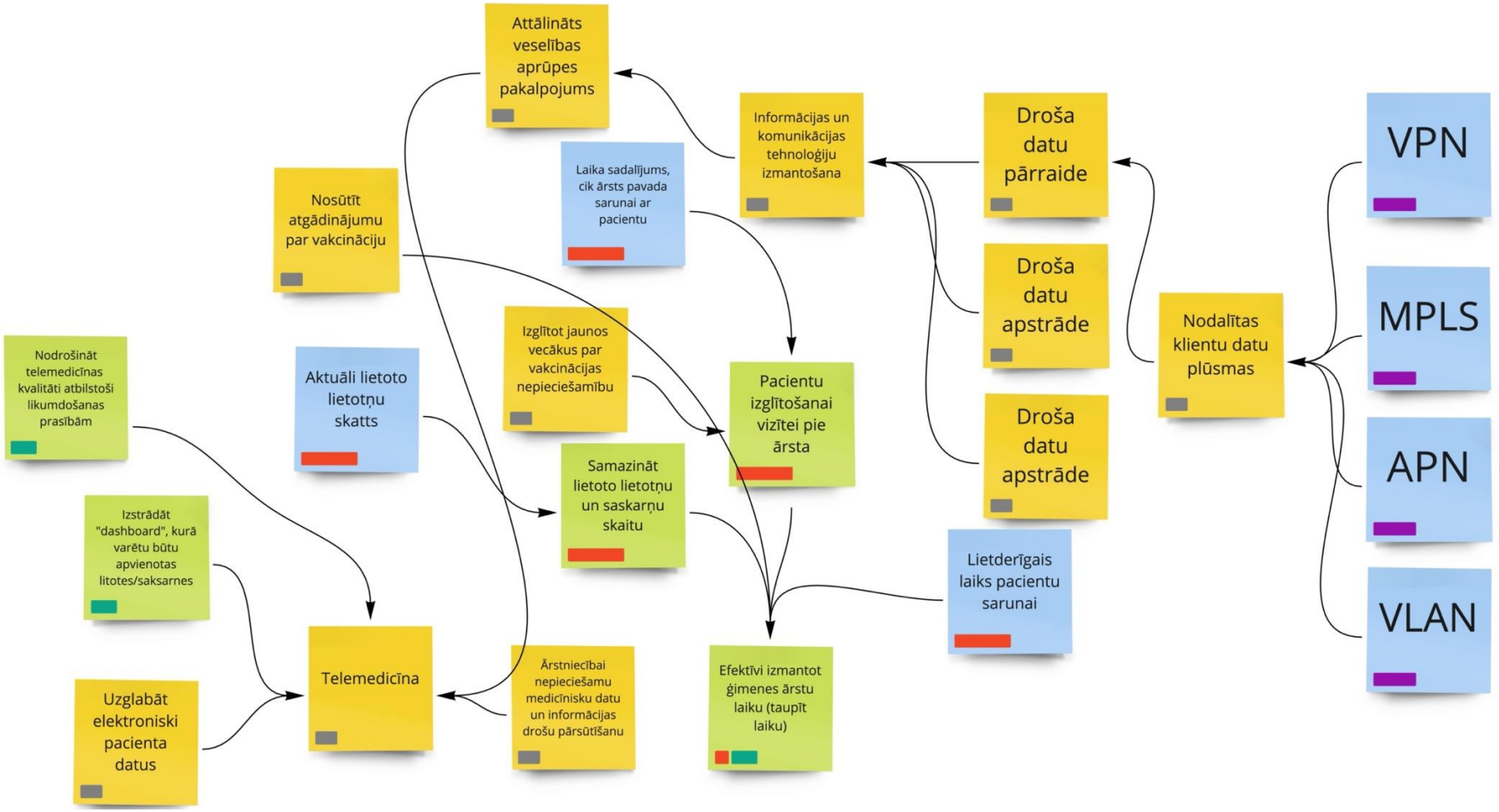
12.attēls. Specifiskie mērķi attālinātai konsultāciju sniegšanai ģimenes ārstu privātpraksē



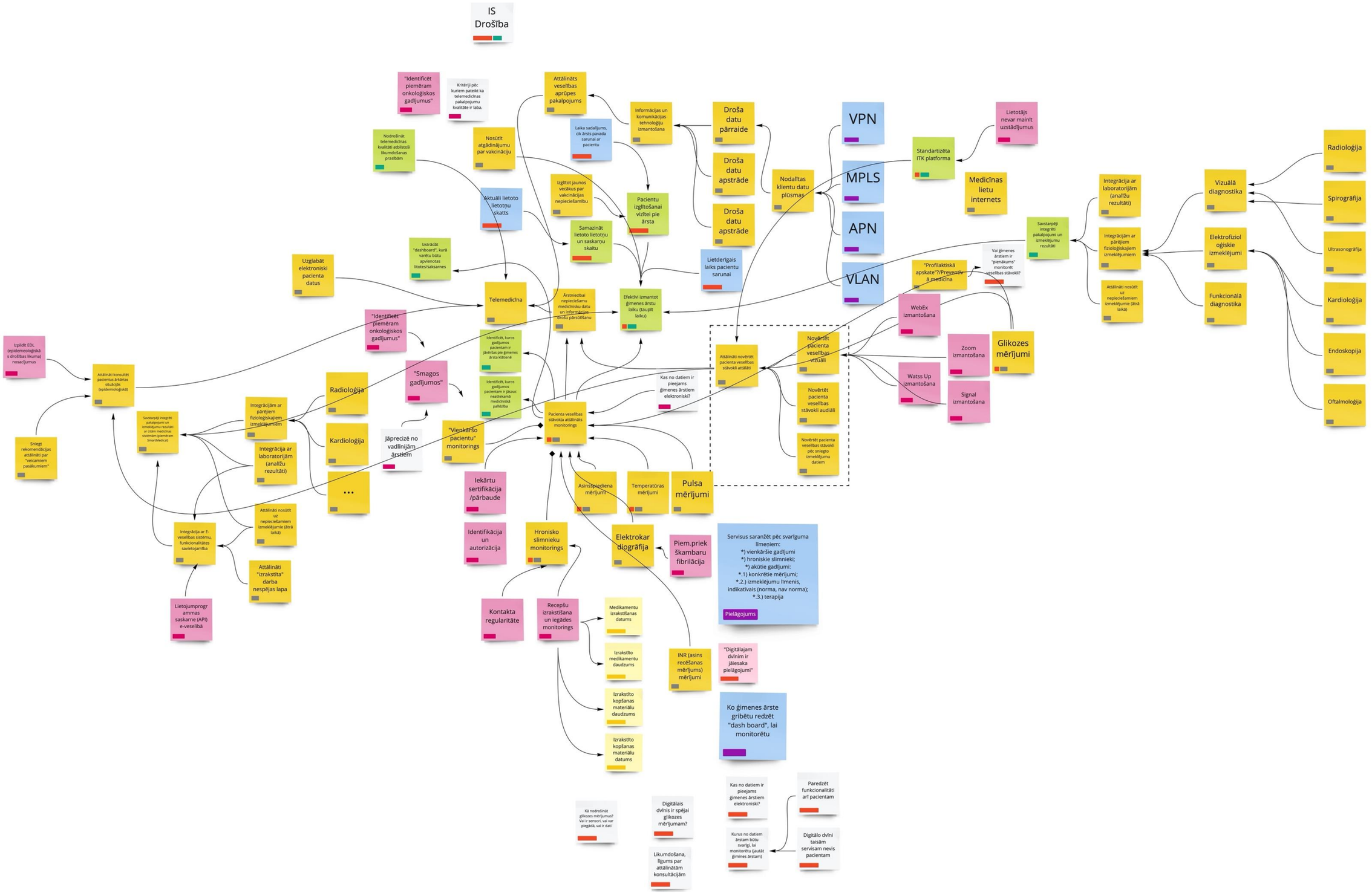
13.attēls. Spēju/servisu kopums telemedicīnas pakalpojumu integrācijai ģimenes ārstu privātpraksēs



14.attēls. Pacienta veselības stāvokļa attālināts monitorings



15.attēls. Drošības aspekti telemedicīnā pacientu konsultēšan



16.attēls. Kopējais modelis telemedicīnas pakalpojumu nodrošināšanai ģimenes ārstu privātpraksē