Digiloo turvalisusest

Valdo Praust – E-tervise Sihtasutus

Eesti meditsiiniandmete digiteerimise ehk digiloo projekt on Eesti ühiskonna viimaste aastate üks turvakriitilisemaid infosüsteeme, kuna selle raames koondatakse ühtsesse süsteemi kõikide Eesti residentide delikaatsed terviseandmed. See nõuab suurt eritähelepanu turbe erinevatele aspektidele, mis peaksid võimaliku suuremahulise turvaintsidendi tõenäosuse viima nullilähedaseks.

Me oleme e-tervise arendamisel selle projekti turbe osas lähtunud viiest alljärgnevast põhimõttest:

1. Kasutajate turvaline autentimine. Kõik projektiga seotud isikud – nii meditsiinitöötajad kui ka patsiendid – peavad end autentima turvalise autentimisvahendiga, nt ID-kaardiga, mobiil-ID-kaardiga või muu säärase seadmega. Ebaturvalist ning viirustele ja troojalastele väga haavatavat paroolipõhist autentimist me ei luba. See peaks välistama olukorra, kus kellelgi õnnestub mingeid sobinguid teha nn autentimisründega, et varastatud identiteediga süsteemi siseneda.

2. Süsteemi maksimaalne jälgitavus ja läbipaistvus. Me oleme planeerinud e-tervise süsteemi sellisena, et igast tegevusest – andmete lisamisest, muutmisest, vaatamisest jms – jääb maha kindel jälg. Kesksüsteemis kasutatav tehnoloogia võimaldab saavutada olukorra, et seda jälge ei saa hiljem muuta ega parandada. Seega säilib nii andmete lisamiste/muutmiste kui ka vaatamiste ajalugu pea igavesti. Iga kodanik saab näiteks patsiendiportaali vahendusel vaadata, kes on tema kohta andmeid lisanud ja neid andmeid vaadanud.

Selline andmete läbipaistvus võimaldab näiteks ära hoida paljusid väärkasutusi (nt andmete volitamata vaatamisi), kuna on teada, et igast vaatamisest jääb maha jälg. Andmete vaatamisõiguste väärkasutamised (nt kui arst vaatab lubamatult temaga mitteseotud patsientide haiguslugusid) tulevad süsteemi turvamonitoorimise käigus tavaliselt välja ning nendele järgneb karistus. Seetõttu on digilugu praegu kasutatavatest paberil haiguskaartidest palju turvalisem, sest nende korral igast vaatamisest jälge maha ei jää ning patsiendil pole seega üldse teavet ega kindlust, kes tema andmeid on vaadanud ja mis põhjusel.

3. Kesksüsteemis olevate andmete kodeerimine. Üks suuremaid ohte e-tervise infosüsteemile on võimalik andmete suuremahuline lekkimine, mille käigus lekiksid paljude Eesti residentide delikaatsed isikuandmed. Seepärast oleme digiloo serveri poolel kasutanud mitmeid keerukaid turbe erilahendusi, mis peaksid selle riski välistama. Üks sääraseid lahendusi on kodeerimine: andmebaasis hoitavate ning salvestatud meditsiiniandmete korral on reaalsed isikuandmed asendatud süsteemisisese kokkuleppelise koodiga, mis ei võimalda nende andmete juhusliku avalikuks tuleku korral kindlaks määrata konkreetset isikut, kelle kohta need andmed käivad.

4. Andmebaasis olevate andmete krüpteerimine. Täiendavaks turvameetmeks,

mis takistab andmete lekkimist, eriti just suuremahulist lekkimist kesksüsteemist, on andmebaasis olevate andmete krüpteerimine. Kõik kettale salvestatud andmed on e-tervise kesksüsteemis krüpteeritud, nii et ketaste varguse, ebaseadusliku kopeerimise vm turvaründe korral meditsiiniandmete leket ei toimu.

5. Seiremoodul. Kesksüsteemis toimuv pidev jälgimine võimaldab esiteks võimalikult efektiivselt leida väärkasutamisi, nt kui meditsiinitöötaja vaatab selliste patsientide andmeid, kellaga ta seotud ei ole. Samas aitab korralik seiremoodul koos sellele järgnevate efektiivsete tegevustega ära hoida keerukamaid ründeid, s.t avastada need juba eos, nii et neile saab efektiivselt reageerida.

Ülaltoodu koosmõjus ei võimalda küll saavutada digiloo absoluutset turvet – see on ühes praktilises süsteemis ülepea võimatu –, kuid peaks võimaldama saavutada piisaval tasemel turbe ehk siis viima võimalike tõsiste turvaintsidentide toimumistõenäosuse äärmiselt väikeseks. Näiteks on praegu masskasutatavatest paberil tervisekaartidest digilugu palju turvalisem.