Meditsiiniõiguslik tagasivaade 2023. aastale ehk kuidas tagada patsientide isikuandmete kaitse?

Merlin Liis-Toomela, Ants Nõmper – Ellex Raidla

SISSEJUHATUS EHK MIKS ME ÜLDSE ANDMEKAITSEST RÄÄGIME?

Viimastel aastatel on tervishoiusektoris märgatavalt sagenenud isikuandmetega seotud rikkumiste arv. 2023. aasta jääb andmekaitse valdkonna inimestele meelde just meditsiinivaldkonna mitme suure juhtumi poolest. See on tekitanud tõsist muret patsientide privaatsuse ja andmeturbe pärast.

Kaasuseid analüüsides järeldub, et meditsiinisektoris esineb puudusi asjakohaste füüsiliste ja organisatsiooniliste turvameetmete rakendamisel, aga edendamist vajab ka privaatsuskultuur laiemalt. Kuigi meditsiinisektorit reguleerivad andmekaitsevaldkonna õigusaktid on püsinud (peaaegu) muutumatuna juba aastaid, annavad toimunud intsidendid põhjuse meenutada peamisi kohustusi patsientide isikuandmete töötlemisel. Arstid ja teised tervishoiutöötajad saavad oma igapäevaseid tööülesandeid täites ligi suurele hulgale tundlikele patsiendiandmetele. Tervishoiusektori usaldusväärsuse tagamiseks on hädavajalik, et kõik tervishoiuteenuse osutamisesse kaasatud isikud mõistaksid isikuandmete töötlemisel kohalduvaid kohustusi, et tagada patsiendiandmete konfidentsiaalsus ning patsientide usaldus.

KAS GDPR TAKISTAB KVALITEETSET TERVISHOIUTEENUSE OSUTAMIST?

Juba 2018. aastal jõustus Euroopa Liidus terviklik andmekaitse ja eraelu puutumatuse raamistik – isikuandmete kaitse üldmäärus –, mida tuntakse ingliskeelse lühendi GDPR järgi. GDPRi peamine eesmärk on anda üksikisikutele kontroll oma isikuandmete üle, kehtestades samal ajal organisatsioonidele, sealhulgas tervishoiuteenuste osutajatele, ranged kohustused seoses andmete töötlemise, säilitamise ja turvalisusega. Nii GDPRi jõustumise ajal kui ka pärast seda on õigusnõustajatel tulnud vastata tervishoiutöötajate murelikele küsimustele selle kohta, kas GDPR takistab kvaliteetse tervishoiuteenuse osutamist. Lühike vastus sellele küsimusele on „ei". Arstide põhiline mure on olnud küsimus, kas patsiendi terviseandmeid võib vahetada teise kolleegiga. Lühike vastus sellele küsimusele on „jah, võib". Küll aga tuleb arvestada, et terviseandmeid võib jagada üksnes konkreetsetel tingimustel.

Tervishoiutöötaja võib isikuandmeid töödelda GDPRi artikli 9 lg 2 punkti h alusel. Viidatud säte annab aluse patsiendi isikuandmete töötlemiseks, kui töötlemine on vajalik meditsiinilise diagnoosi panemiseks, tervishoiuteenuste või ravi võimaldamiseks, tuginedes liikmesriigi õigusele või tervishoiutöötajaga sõlmitud lepingule ja eeldusel, et isikuandmete töötleja suhtes kehtib ametisaladuse hoidmise kohustus ja asjakohased kaitsemeetmed on kehtestatud. Võtmesõnad on siin vajalikkus, eesmärgipärasus ja minimaalsus. Kui arst meditsiinivaldkonna eksperdina ja erialaspetsialistina hindab, et kvaliteetse tervishoiuteenuse osutamiseks, korrektse diagnoosi panemiseks või õige ravi määramiseks on vaja kaasata teine spetsialist, kellele patsiendi terviseandmeid edastada, siis tohib seda teha. Selle jaoks ei ole vaja küsida patsiendi nõusolekut. Ka ei ole vaja patsienti eraldi teavitada, kuigi suurem läbipaistvus on alati tervitatav. Kui see on vajalik diagnoosi panemiseks või ravi osutamiseks, võib raviarsti kaasatud teine spetsialist vaadata ka patsiendi terviseportaali sisestatud andmeid. Nagu aga öeldud, tuleb lähtuda vajalikkusest, eesmärgipärasusest ja minimaalsusest. Neid kriteeriume tuleb iga kord eraldi hinnata.

Loodetavasti ei vaja selgitamist, et kõiksugu uudishimupäringud patsientide kohta on arusaadavalt keelatud. Vajalikkuse ja minimaalsuse põhimõttega on vastuolus ka pelgalt põnevuse ja klatšihimu rahuldamiseks kolleegidele haiguslugude jagamine koos nimedega. Tuttavate arstidega vesteldes on jäänud mulje, et eelkirjeldatu on murekoht eelkõige meditsiinitöötajatele endile, kes on sattunud patsiendi rolli. Mitmed arstid on väljendanud oma muret, et patsiendina ei ole meditsiinitöötaja privaatsus tihtipeale kaitstud ning kohe saavad meditsiinitöötaja terviseprobleemist (või ka rõõmusündmusest, näiteks raseduse korral) teadlikuks kolleegid, kellel ei tohiks sellist infot olla. Tuleb meeles hoida, et võlaõigusseaduse (VÕS) § 768 lõige 1 sätestab juba VÕSi jõustumisest aastal 2002, et tervishoiuteenuse osutaja ja tervishoiuteenuse osutamisel osalevad isikud peavad hoidma saladuses neile tervishoiuteenuse osutamisel või tööülesannete täitmisel teatavaks saanud andmeid patsiendi isiku ja tema tervise seisundi kohta, samuti

hoolitsema selle eest, et tervishoiuteenuse osutamise dokumentides sisalduvad andmed ei saaks teatavaks kõrvalistele isikutele. Konfidentsiaalsuskohustusest võib kõrvale kalduda üksnes siis, kui andmete avaldamine võib oluliselt kahjustada patsienti (nt seada ohtu tema elu) või kui seaduses või kokkuleppel patsiendiga ei ole ette nähtud teisiti.

KÜBERTURVALISUSE OLULISUS

Vaieldamatult kõige suurem andmekaitsevaldkonna rikkumisjuhtum, mis on Eestis pärast GDPRi jõustumist toimunud, on Asper Biogene'i andmeleke, mille tulemusena lekkisid ligikaudu kümne tuhande patsiendi geenitestide vastused. Käesoleva artikli kirjutamise ajal on Asper Biogene'i juhtumi uurimine Andmekaitse Inspektsioonil alles pooleli, kuid avalikkusele antud informatsiooni pinnalt tundub, et rikkumist oleks saanud ära hoida või vähemalt selle toimumise tõenäosust vähendada, kui oleks rakendatud asjakohaseid turvameetmeid.

Asper Biogene'i juhtum on küll väga ilmekas, aga kõigest üks näide küberintsidendist, mis võib tabada kõiki tervishoiuteenuse osutajaid. Küberohtudest ja võimalike häkkimiste eest ei ole kaitstud ükski meditsiinisektori ettevõtja. Juba enne GDPRi jõustumist, 2017. aastal, toimus Leedus andmeleke, mille tulemusena said häkkerid ligipääsu ilukliiniku serverisse. Serveris olid kliiniku patsientide enne-ja-pärast-fotod, kusjuures patsientide hulgas oli mitmeid kohalikke kuulsusi. 2020. aastal said kurikaelad ligipääsu Soome Vastaamo kliiniku patsientide haiguslugudele. Need on kõigest mõned näited meie lähiriikide juhtumitest.

Mida pahalased rünnakutega taotlevad? Tüüpiliselt nõuavad arvutikelmid süsteemide taastamise või avamise eest lunaraha, tavaliselt mõnes krüptovääringus, näiteks *bitcoin*'ides. Kui nõuet ei täideta, siis süsteeme ei avata, lekitatakse kättesaadud andmed avalikkusele või tumeveebi.

Milliseid küberturvalisusega seotud kohustusi kehtiv õigus meditsiiniandmete hoiustamisele seab? GDPR on selles osas üsna lakooniline. Isikuandmete turvalisuse kohta on GDPRis ainult üks artikkel. GDPRi artikkel 32 sätestab kokkuvõtlikult, et rakendada tuleb piisavaid turvameetmeid, arvestades sealjuures teaduse ja tehnoloogia viimast arengut, asjakohaste meetmete rakendamise kulusid, isikuandmete töötlemise laadi ja võimalikke ohte füüsiliste isikute õigustele.

Andmekaitse Inspektsioon on juhendis „Isikuandmed sotsiaalhoolekande- ja tervishoiusektoris" nimetanud mitmeid elementaarseid turvameetmeid. Infotehniliselt peaks olema kindlasti tagatud tarkvara uuendamine, viirusetõrje, tulemüürid, turvaline andmete edastamine, VPN-ühendus avaliku võrgu kasutamise korral, logidega kasutajasüsteem ja andmete hoidmine ainult asutuse infosüsteemis. Terviseandmete edastamisel tuleb kasutada vastavalt võimalusele krüpteerimist ja pseudonüümimist. Teiste andmetöötlejate kaasamisel tuleb alati hinnata, kas andmetöötleja vajab andmeid isikustatud kujul või piisab pseudonüümist. Nimede või isikukoodide asendamine pseudonüümidega aitaks paljudel juhtudel päästa andmelekkest. Näiteks, kui laborit tabab rünnak, aga labori infosüsteemis on ainult patsientide pseudonüümid ning pseudonüümi võti on turvaliselt laborianalüüsi tellija (haigla või muu tervishoiuasutuse) serveris, siis labori andmelekke tulemusena jääksid patsientide isikustatud terviseandmed kaitstuks. Samal ajal kätkeb aga pseudonüümimine teistsuguseid riske. Kui pseudonüümimine korraldada lohakalt, võib pseudonüümimise tulemusena suureneda risk, et erinevate patsientide analüüside tulemused lähevad omavahel segamini. Seega pole ka pseudonüümimine alati ideaalne ning riskivaba lahendus.

Küberturvalisuse kõrge taseme hoidmine ei ole vajalik aga ainult andmekaitselistel eesmärkidel. Pahavararünnakud võivad häirida meditsiiniteenuste toimimist laiemalt, seades ohtu patsientide turvalisuse ja tervishoiuasutuse töökorralduse. Kui arvutisüsteemid on lukus, broneerimissüsteemi ja e-postikontosid avada ei saa, on tõenäoliselt kogu organisatsiooni töökorraldus kaoses ning takistatud on ka ravi osutamine. 2020. aastast on teada ka juhtum Saksamaalt Düsseldorfi haiglast, kus küberrünnak nõudis inimelu, sest lukustunud süsteemid ei võimaldanud õigeaegse abi andmist.

ORGANISATSIOONILISED JA FÜÜSILISED TURVAMEETMED

Küberturvalisuse kõrval ei ole vähem tähtsad organisatsioonilised ja füüsilised turvameetmed. Laia meediakajastust on saanud kohtuasi, kus väidetavalt ühe haigla renoveerimistööde käigus jäeti patsientide paberkandjal olevad haiguslood ja epikriisid sisuliselt kõigile mööndujatele kättesaadavaks. Mida sellest loost õppida? Esiteks tuleb küsida, kas paberil terviseandmete säilitamine on alati vajalik. Paber toob alati kaasa turvariski, sest võib sattuda valedesse kätesse või võib ununeda selle korrektne arhiveerimine ning hävitamine. Ka on digilahenduste eelistamine loodusele sõbralikum lahendus.

Siinjuures tuleb rõhutada, et ka digilahendused ei ole turvariskidest vabad ning patsientide andmete töötlemiseks tuleb valida sobiv ja turvaline kanal. 2023. aasta andmekaitsejuhtumite hulgas oli ka kaasus, mille asjaolude kohaselt jagasid meditsiinitöötajad patsientide fotosid ja terviseandmeid Facebooki grupivestluses, kuhu oli väidetavalt lisatud ka mitmeid meditsiinisektoris mittetöötavaid isikuid. Facebook ning muud erasuhtluseks mõeldud kanalid ei ole sobivad patsientide kohta info vahetamiseks. Lubamatu on terviseandmete jaga-

mine tervishoiuteenuse osutamisse mittekaasatud isikutele, kellele ei laiene eelkirjeldatud konfidentsiaalsuskohustus VÕSi alusel.

Olenemata sellest, kas terviseandmeid hoitakse paberil või digitaalselt, tuleb läbi mõelda, kuidas tagada andmete turvalisus. Selleks tuleb rakendada asjakohaseid organisatsioonilisi ja füüsilisi turvameetmeid, millest ühed olulisemad on asjakohaste pääsukontrollide ja juurdepääsupiirangute seadmine, arvestades vajalikkuse ja minimaalsuse põhimõtteid. Kahjuks pole harv juhus, kus tervishoiuasutuses pääsevad suurele hulgale patsientide terviseandmetele ligi töötajad, kes sellist infot enda tööülesannete täitmiseks ei vaja. Näiteks, administratsioonitöötajal võib broneeringu kinnitamiseks olla vaja näha, millal käis patsient viimati visiidil ning milline saatekiri on patsiendile väljastatud. Küll aga ei pea broneeringu kinnitamiseks nägema infot selle kohta, millise tervisemurega patsient arsti juurde täpselt pöördub ning millised on patsiendile tehtud uuringute tulemused. Selliste rikkumiste eest on Euroopa praktikas määratud haiglatele ka trahve. Näiteks trahvis 2020. aastal kohalik järelevalveasutus üht Portugali haiglat 400 000 euro suuruse trahviga, sest haigla infosüsteemid võimaldasid patsiendi tervisekaartidele ligipääsu töötajatele, kes sellist infot oma tööülesannete täitmiseks ei vajanud. Samas suurusjärgus, summas 460 000 eurot, trahviti sarnase rikkumise eest 2019. aastal ka Hollandis Haagis asuvat haiglat.

PIISAV VÄLJAÕPE JA TEADLIKKUSE SUURENDAMINE

Praktikas näeme, et andmekaitseliste rikkumiste oluliseks põhjuseks on jätkuvalt inimlikud eksimused. Inimlikust eksimusest tuleb ette juhtumeid, mille tulemusena patsiendi terviseandmed edastatakse nimekaimule, trükitakse vigane e-postiaadress, avatakse õngitsuskiri, mis halvab meditsiiniasutuse arvutisüsteemi töö, või unustatakse töökohalt lahkudes arvutiekraan lukustada. Kuigi inimlikke eksimusi ei ole võimalik kunagi lõpuni välistada, on neid siiski võimalik oluliselt vähendada teadlikkuse suurendamise ja kollektiivi asjakohase koolitamise kaudu. Teadlikkuse suurendamine on vajalik nii andmeturbe parimate tavade kui ka laiemalt privaatsusõiguste valdkonnas. Ohtude ja riskide teadvustamine teeb võimalikuks ka nende vältimise. Lisaks õiguslike nõuete teadvustamisele aitab pädev koolitamine mõista patsientide andmete käitlemise eetilisi küsimusi ning edendada organisatsiooni privaatsuskultuuri.

KOKKUVÕTTEKS

Isikuandmete kaitse ja privaatsuse tagamine meditsiinivaldkonnas on äärmiselt oluline patsientide põhiõiguste tagamiseks. Patsientide terviseteabe hoidjatena lasub Eesti arstidel kohustus seada esikohale andmete privaatsus ja järgida kõrgeimaid konfidentsiaalsusstandardeid. Seejuures on oluline, et ka patsiendid ise tajuksid, et nende terviseteave on kaitstud ning hoolikalt hoitud. Tasemel privaatsuskultuur aitab suurendada usaldusväärsust tervishoiuteenuse osutajate suhtes. Usaldus tervishoiusektori vastu hõlbustab patsiendi ja arsti vahelist avatud suhtlust. Avatud suhtlus aitab kaasa tervishoiuteenuse kvaliteedi tõstmisele ning lihtsustab arstide tööd. Seega järeldub, et tugevast privaatsuskultuurist on arstkonnal ainult võita.