Baasturbe meetmed perearstidele

Sissejuhatus

Juhendi eesmärgiks on anda ülevaade olulisematest infoturbe alastest turvameetmetest.

Turvameetmete rakendamine on vajalik perearsti käsutuses olevate eriliigiliste isikuandmete[1] turvaliseks töötlemiseks ja kaitseks ning nendega seotud konfidentsiaalse info lekkimise vältimiseks. Nende järjekindel rakendamine annab aluse küberturbe baastaseme tekkeks.

Juhendis toodud nõuded peavad kohalduma kõigile seadmetele/süsteemidele, millega töödeldakse eriliigilisi isikuandmeid.

Juhend sisaldab üldiseid meetmeid, mida on soovituslik võtta aluseks oma perearstikeskuse infoturbepoliitika tegemisel, kohandada ja täpsustada neid vastavalt oma asutuse spetsiifikale ning kasutada võrgu-ja infosüsteemi riskianalüüsi sisendiks.

Juhend sisaldab nii organisatsioonilisi, isikulisi, kui ka tehnilisi meetmeid. Tehniliste meetmete rakendamine on mõistlik jätta IT teenusepakkujale, kuna nende rakendamine vajab kohati tehnilisi teadmisi. Samuti saab tehnilisi meetmeid kasutada teenuste sisse ostmisel turvalise ja jätkusuutliku valiku tegemisel. Organisatsioonilised meetmed tuleb tagada perearstikeskuse poolt kõigile töötajatele, kes töötlevad eriliigilisi andmeid, isikulisi meetmeid tuleb rakendada kõigi perearstikeskuse töötajate poolt, kes käitlevad eriliigilisi isikuandmeid.

Infoturbehaldus

- Koostada tuleb asutuse infoturbepoliitika, kus tuuakse välja infoturbealased eesmärgid ja tööprotsessid, mida peavad töötajad täitma ja järgima. Juhendiga peavad tutvuma kõik asutuse töötajad.
- Infoturbe dokumentatsioon peab olema regulaarselt uuendatud ning vähemalt kord aastas üle vaadatud. Infoturbe dokumentatsiooniks on vähemalt:
  - Infoturbepoliitika
  - Infotehnoloogia inventari loetelu
  - Seadme kasutamise eeskiri koos interneti kasutamise eeskirjaga.
  - Tarkvara, seadistuste ja litsentside dokumentatsioon
  - Andmevarunduse dokumentatsioon
- Töötajaid tuleb kaasata ja koolitada infoturbealastel teemadel regulaarselt.
- Tööülesanneteks kasutatavate ja arvutivõrgu toega IT töövahendite kohta koostatud inventari loetelu tuleb täiendada seadmete lisamisel või eemaldamisel ning inventari loetelu kontrolli teostada minimaalselt üks kord aastas.

Kasutajaõiguste haldamine

- Kasutajatunnus ja kasutajaõigused peavad olema personaalsed ja neid hoitakse konfidentsiaalsena. Iga kasutaja teeb tööd ainult tema isikule omistatud kasutajatunnusega.
- Kasutajaõigused peavad olema antud vastavalt tööülesannete vajadustele.

[1] Isikuandmete kaitse üldmääruse artikkel 9 lg 1. sh oma patsientide terviseandmete ja ka perearstikeskuse töötjate isikuandmete

- Kõik mittevajalikud õigused tuleb kasutajatelt eemaldada, kontrolle kasutajate kasutajaõiguste kohta tuleb teostada vähemalt kord aastas, igakordselt töötajate asendamisperioodidel, töösuhte lõppemisel või tööle tulemisel,
- Uued töötajad peavad enne IT seadme või süsteemi kasutamist tutvuma asutuse sisekorra eeskirjade, infoturbepoliitika ja seadmete kasutamise eeskirjadega.
- Töösuhte lõppemisel ning peatumisel peatatakse koheselt töötajaga kõik juurdepääsud infosüsteemidesse ja töötlussüsteemidesse.

Süsteemide tarkvara ajakohasus

- Installeeritud tarkvara kasutusel olevad versioonid peavad olema dokumenteeritud koos seadistustega.
- Kõik tarkvara litsentsid ja sertifikaadid, mis on kasutusel, peavad olema dokumenteeritud.
- Kasutada tuleb ainult legaalset ja asutuse poolt aktsepteeritud tarkvara.
- Viirustõrje tarkvara tuleb kasutada pidevalt kõikidel serveritel, laua- ja sülearvutitel, nutitelefonidel, tahvelarvutitel.
- Kasutatav operatsioonisüsteem ja viirusetõrje tarkvara peab olema ajakohane ja omama kõiki turvauuendusi ning olema tootja poolt toetatud. Tooteid, millele ametlikke turvauuendusi ei väljastata, tuleb kasutusest eemaldada või vastavalt riskianalüüsile rakendada täiendavaid turvameetmeid (nt võrgust isoleerida).

Seadmete kasutamine

- Eriliigiliste isikuandmete töötlemisel peab arvuti olema paigutatud nii, et kuvaril toimuv ei ole kolmandatele isikutele nähtav. Tööjaama kuvari paigutamisel akna või ukse lähedusse selliselt, et kuvaril toimuv on kõrvaltvaatajale nähtav, on vajalik kasutada seadmel turvaekraani või kilet.
- Seadmed tuleb paigutada selliselt, et volitamata isikutel ei oleks neile juurdepääsu.
- Tööjaama juurest lahkudes peab kasutaja arvuti sulgema või lühema pausi korral lukustama tööjaama (näiteks Windows logo klahv + L).
- Kui arvutivõrku kasutatakse isikliku kiipkaardiga, tuleb tööjaama juurest lahkudes kiipkaart (sh. ID kaart) kaasa võtta.
- Pisteliselt tuleb kontrollida kasutajate seadmetest väljalogimist. Vajadusel tuleb kasutajatele koostada lühike infoleht või meeldetuletus, miks on vaja seadmest välja logida töökohalt lahkumise korral.
- Konfidentsiaalse informatsiooni printimisel või paljundamisel tuleb väljaprinditud/paljundatud materjal koheselt pärast printimist printerist eemaldada.
- Kaugtöö tegemisel tuleb kasutada tööjaama, mis vastab käesoleva juhendi turbenõuetele.
- Mobiilseid seadmeid peab hoidma turvalises kohas. Seadet ei tohi jätta järelevalveta, nt vältida tuleb sõidukisse jätmist.
- Lauaarvutitel ja sülearvutitel tahvlitel, nutitelefonidel jt mobiilsetel seadmetel tuleb rakendada automaatset ekraanilukustust, seadme (kõvaketta) krüpteeringut. Lisaks tuleb mobiilseid seadmeid kaitsta turvaliste ja nõuetele vastavate paroolide ja PIN koodide abil.

Digitaalsed andmekandjad

- Digitaalseks andmekandjaks loetakse seadmeid, mille peale saab salvestada digitaalset infot (kõvakettad, USB pulgad, mälukaardid, CD/DVD plaadid, telefonide ja fotoaparaatide mälukaardid, meditsiiniseadmetes sisalduv mälu jne).
- Tööseadmete külge tohib ühendada ainult digitaalseid andmekandjaid mille päritolu ja turvalisus on usaldusväärne (näiteks usaldusväärsest kauplusest ostetud, avamata originaalpakendis hangitud mälupulk).
- Kiipkaardi kasutamisel tuleb see peale kiipkaardi funktsionaalsust vajavate tööprotsesside lõpetamist kaardilugejast eemaldada.
- Krüpteerimata konfidentsiaalset informatsiooni sisaldavat andmekandjat tuleb hoida ja transportida isikliku järelevalve all.
- Digitaalse andmekandja kasutamise lõpetamisel tuleb selle sisu turvaliselt kustutada või andmekandja hävitada.
- Konfidentsiaalse informatsiooni kopeerimisel eemaldatavale andmekandjale või konfidentsiaalse informatsiooniga eemaldatava andmekandja ühendamisel tööjaamaga tuleb võimaluse korral juhtmevaba ühenduse asemel eelistada juhtmega ühendust.

WIFI

- WIFI seadet (Access Point) ei tohi kasutada tehase seadetes. Seadme kasutuselevõtul tuleb veenduda, et kasutatakse turvalist krüptograafia protokolli (WPA/ WPA2 koos TKIP või CCMPga või turvalisem).
- Traadita kohtvõrku (WIFI), mida kasutatakse asutuse töö tegemiseks tohivad kasutada ainult asutuse töötajad.
- Kui tahetakse pakkuda WIFI võimalust külastajatele, tuleb luua asutuse võrgust eraldatud WIFI mida ei tohi kasutada asutuse töö tegemiseks.

E-post, interneti kasutamine

- E-posti rakendus peab olema konfigureeritud järgides turvanõudeid ja suuniseid. Sobiva autentimismeetodi valimisel tuleb lähtuda kõrgemat turvalisust pakkuvast lahendusest, nt kasutada kaheastmelist autentimist.
- Eriliigilisi isikuandmeid tohib teistele volitatud osapooltele jagada ainult krüpteeritult (nt ID-kaardiga).
- Minimaalselt tuleb kasutada andmeside krüpteerimiseks TLS´i võimalikult uut versiooni ja E-posti kaitsmiseks SPF´i, DKIM´i, DMARC´i.
- E-posti teenusepakkuja peab andmeid hoidma EL piires.
- E-postiteenusepakkuja ei tohi aktiivselt e-kirjade sisu töödelda muude teenuste pakkumiseks - nt reklaami kuvamiseks.
- Perearstikeskuse veebilehed peavad kasutama HTTPS-i ja DNS peab olema kaitstud DNSSEC-iga.
- E- posti lahendusel peab olema viirustõrjeprogrammiga meiliskanner, mis kontrollib sisenevate ja väljuvate meilide ning eelkõige nende manuseid rämpsposti, arvutiviiruste ja muud laadi pahavara suhtes.

- Asutuse e-posti aadressi on keelatud kasutada välistele teenustele või uudiskirjadele registreerimiseks, kui see ei ole seotud tööga. E-posti aadressi on lubatud kasutada ainult tööalaselt.
- Kahtlase sisu, adressaadiga või manusega kirjad, tuleb kustutada või edasta infoturbe eest vastutavale isikule, kes vajadusel edastab selle aadressile cert@cert.ee edasiseks uurimiseks.
- Kasutajal on keelatud avada kahtlusi tekitava pealkirjaga või kahtlustäratavalt elektronposti aadressilt saabuvat elektronkirja ning avada elektronkirjade manuses olevaid faile.
- Interneti kasutamise kohta peab olema loodud reeglistik, kus kirjeldatakse millised on lubatud ja lubamatud tegevused interneti kasutamisel. Samuti tuleb kirjeldada millise sisuga veebiaadressidel viibimine ei ole lubatud.
- Asutuses ei ole lubatud kasutada sotsiaalmeediat konfidentsiaalse tööalase informatsiooni ja teabe, s.h. eriliigiliste isikuandmete vahetamiseks teiste töötajate või asutustega.
- Keelatud on tööalase elektronposti aadressi kasutamine tarbijamängude mängimiseks, isiklike kommertsteadete tellimiseks, foorumite kasutamiseks ning muudeks tööga mitteseotud tegevusteks.

Varukoopiate tegemine ja varukoopiatest taastamine

- Asutus peab hindama IT-süsteemide ja rakenduste varundamise vajaduse sagedust ja tagama, et on koostatud andmevarunduse dokumentatsioon, mis sisaldab:
- andmevarunduse regulaarsus;
- andmevarunduse tegemise kuupäeva;
- andmevarunduse jaoks valitud parameetrid;
- andmete varundamise koht.
- Andmete varundamiseks vajalikud protseduurid peavad olema dokumenteeritud sh. regulaarse varundusega, erakorralise varunduse seotud protseduurid, varukoopiatest taastamist kui ka varundussüsteemi enese taastamist.
- Varundatud andmete taastamist kõikides süsteemides tuleb testida vähemalt üks kord aastas või pärast varundamise protseduuride muutmist.

Füüsiline turvalisus

- Ruumide uksed ja aknad hoitakse suletuna tööpäeva välisel ajal ning töökohalt pikemaks ajaks lahkudes takistamaks volitamata isikute juurdepääsu andmetele
- Üldkasutatavates maja osades, kus liiguvad võõrad, peavad uksed olema lukustatud kui ruumis ei viibi volitatud isikuid.