Patsientide isikuandmed on tervishoiuteenuse osutajate poolt kaitstud

Andmekaitse Inspektsioon kontrollis lõppeval aastal järelevalve korras 24 juhuslikult valitud tervishoiuteenuse osutajat (edaspidi TTO), sh nii töötervishoiu- kui ka perearste. Kõik kontrollitavad asutused kuuluvad nn mikroettevõtete hulka ehk töötajate arv on kuni 10.

Järelevalve viidi läbi kahes etapis: esmalt tuli TTO-l vastata 22 küsimusest koosnevale küsimustikule ning seejärel toimusid intervjuud kohapeal.

Kontrollreidide eesmärgiks oli teha kindlaks, kas TTO-d järgivad oma tegevuses isikuandmete kaitse seaduse (edaspidi IKS) põhimõtteid.

Järelevalve käigus hindasime mitut aspekti: kas andmeid kogutakse ausalt ja seaduslikult, kas andmete kogumine on eesmärgipärane, kas järgitakse minimaalsuse printsiipi ehk kogutakse rangelt ainult neid andmeid, mida on vaja patsiendile konkreetse tervishoiuteenuse osutamiseks.

Samuti täpsustasime, kuidas delikaatseid isikuandmeid töödeldakse (elektrooniliselt või paberkandjal), st kuidas neid säilitatakse ja hävitatakse ning kellele ja kuidas on võimaldatud juurdepääs isikuandmetele ning kuidas toimub andmete edastamine e-tervise infosüsteemi.

Järelevalve tulemusel jõudsime järgmiste järeldusteni:

1. Isikuandmete töötlemine TTO-des vastab IKS-i § 6 põhimõtetele, st andmete töötlemine on eesmärgikohane, seaduslik ning järgitakse minimaalsuse printsiipi.
2. Kaugtööd TTO-d ei kasuta, samas volitatud töötlejale (tarkvara väljatöötaja) on võimaldatud tarkvara kaughooldus.
3. Kõik TTO-d väljastavad andmed ainult kirjaliku või digitaalse taotluse esitamisel ning kõik toimingud registreeritakse vastavas päevikus.
4. Kõik TTO-d on liidestatud e-tervise infosüsteemiga (Digilugu). Andmeid edastatakse jooksvalt, st kui andmed on valmis edastamiseks. Kõik TTO-d kasutavad digiloo andmeid ehk andmete liikumine on kahesuunaline (TTO-st Digilukku ja vastupidi) ning TTO-d kasutavad Tervise infosüsteemi andmeid oma töös (infosüsteemis)
5. Paberdokumentide töötlemine vastab isikuandmete töötlemise nõuetele, sh nii hoiustamine kui hävitamine.
6. Andmete kasutamine ehk juurdepääs infosüsteemi andmetele on aktsepteeritud ainult konkreetse TTO töötajatele.
7. Andmete varundamine toimub automaatselt igapäevaselt.
8. Andmeid edastatakse x-tee kaudu ja krüpteeritult.

AKI selgitused ja soovitused TTO-le:

1. Selgitasime **vastutava ja volitatud isikuandmete töötleja** rolle, vastutust ja kohustusi. Selgitasime, kuidas kuidas eristada **vastutava töötleja alluvuses** töötavat isikut volitatud töötlejast. Alluvuses töötav isik on kohustatud isikuandmeid töötlema seaduses lubatud eesmärkidel ja tingimustel ning vastutava töötleja antud juhiste ja korralduste kohaselt.

2. Arutasime **suuliste lepete probleemi**, sest neid on raske tõendada ning AKI soovitab teatud suulised lepped vormistada kirjalikult, näiteks korraldused, mis reguleerivad TTO-de põhimõttelisi küsimusi nagu infosüsteemi kasutamine, juurdepääs andmetele (kasutamine) ning samuti andmete väljastamise kord jne.

3. Juhtisime TTO-de tähelepanu asjaolule, et infoturve on pidev protsess, mis nõuab pidevat parendamist ja tõhustamist (kaasajastamist) ning järjepidevat tööd. Tegelik olukord infoturbe osas ei pruugi vastata kehtivates dokumentides esitatud nõuetele. **Kehtiva ja kaasajastatud infoturbereeglistiku** puudumisel või juhul, kui töötajad ei ole nendega tutvunud, ei pruugi töötajad olla vajalikul määral teadlikud infotehnoloogiaga seotud riskidest ning oma osast turvaintsidentide ärahoidmisel.

4. **Konfidentsiaalsuse nõudena** peab olema väljatoodud nõue, et isik on kohustatud hoidma saladuses talle tööülesannete täitmisel teatavaks saanud isikuandmeid ka pärast töötlemisega seotud tööülesannete täitmist või töö- või teenistussuhte lõppemist.

Otsus: Kontrollitud TTO-des rakendatavad turvameetmed ei põhjusta isikuandmete kadu või isikuandmete omavolilist kasutamist, seega on tagatud isikuandmete kaitse seaduse § 25 lõike 2 turvanõuete täitmine. Olukord TTO-des andmete töötlemise küsimustes **on rahuldav.**

E-tervise probleem (andmete kvaliteet) algab algandmete tekkimisest TTO-de juures, mis osaliselt edastatakse e-tervisesse.

Ettepanek:
TTO-de, eriti perearstide IT rakendusvahendid on killustunud, kasutusel on mitmed erinevad tarkvaralised lahendused (programmid ehk infosüsteemid), mille IT halduse nõuded on väga erinevad. Iga perearst salvestab patsientide andmed lokaalselt nn „oma serverisse“ ning E-tervisesse edastatakse lühike koond ehk epikriis.

AKI näeb vajadust ühtse veebipõhise infosüsteemi järele, mille nõuetekohase arenduse, halduse ja kontrolli tagab SoM. Ainult nii saab tagada patsientide andmete ühese turvalise töötluse ja majutuse, sh varundamise.

Teisalt tagab ühtne lahendus ka maksimaalselt turvalised autentimislahendused (ID kaart, m-ID) ilma andmete terviklust kahjustavate eranditeta. Ainult nii on tagatud IKS § 25 maksimaalne täitmine käideldavuse, tervikluse ja konfidentsiaalsuse osas.

17. november 2016

Boris Põldre

andeturbeekspert
Andmekaitse Inspektsioon