Ettepanek KüTS muudatuseks

27.06.2024

Sissejuhatus

Eestis toimiv tervishoid on valdavalt digitaalne ja küberturvalisus on tervishoius esmatähtis. Kuid kehtiva küberturvalisuse seaduse järgi on vastavate nõuete üle kontrolli mehhanismide rakendamine perearstikeskustes seotud ebaproportsionaalselt suure finants- ja haldus koormusega. Leiame, et küberturvalisuse tagamiseks toimivad ka muud lahendused, mis võimaldavad raviraha otstarbekamalt kasutada. Eesti Perearstide Seltsil on RIA-ga kujunenud välja hea koostöö. Sellest koostööst on perearstideni jõudnud mitmed RIA poolt profiilselt esmatasandi tervishoiuasutustele pakutud koolitused, hindamised, konsultatsioonid ja juhendid. Samuti on käivitunud järelevalvemenetlused, mis on piisavalt karmid ja suunavad perearste Eesti Infoturbestandardi (E-ITS) nõudeid järgima. Lisaks on küberturvalisusega seotud nõuete jälgimine integreeritud perearstikeskuste kvaliteedisüsteemi ning neid on plaanis täiendada. Koostöös Tervisekassa, RITi, RIA, Eesti Perearstide Seltsi ja Esmatsandi Tervisekeskuste Liiduga on väljatöötamisel perearstide arvutitöökoha teenus mis tagab turvalise tehnilise lahenduse nõuded perearsti töökohtadele ja võimaldab neid kasutada ka erasektorist teenuse tellimiseks.

Tänane 10 töötaja kriteerium E-ITS auditi tellimiseks on ebaproportsionaalne nii finantskoormuse kui halduskoormuse osas ning selline kohustus ei ole jõukohane ei rahastusmudeli jätkusuutlikkuse ega perearsti teenuse pakkumise seisukohalt. 10 töötajat võib olla juba ka väga väikeses perearstikeskuses, kus osutatakse teenust 2-3 nimistule. Selliseid keskuseid on Eestis hinnanguliselt üle 200, st enamik Eesti perearstikeskustest.

Hetkel katab Tervisekassa rahastus küberturvalisuse arendamiseks (sh E-ITS rakendamiseks) mõeldud kulutusi summas 49,22 eurot kuus ühe perearsti nimistu kohta, mis ei ole piisav infoturbe auditi tellimiseks.

Ka küberturvalisuse seaduse, avaliku teabe seaduse ja Eesti Rahvusringhäälingu seaduse muutmise seaduse eelnõu seletuskirjas on märgitud, et auditeerimiskulud võivad majanduslikult koormavamad olla väikestele ettevõtetele ja majandusliku mõju tasakaalustamiseks võiks olla erand mikroettevõtetele, sealhulgas suurele osale tegutsevatele perearstidele. Praeguste reeglite alusel kohaldub auditi nõue siiski suurele hulgale perearstidest. (Viide: Küberturvalisuse seaduse, avaliku teabe seaduse ja Eesti Rahvusringhäälingu seaduse muutmise seaduse eelnõu esimese lugemise seletuskirja lk 35 kohaselt on auditi läbiviimise erand mõeldud laienema suurele osale tegutsevatele perearstidele (“*Seega on majandusliku mõju tasakaalustamiseks auditikohustust kehtestava rakendusakti kavandis ettenähtud ka erand mikroettevõtjatele (nt suurele osa tegutsevatele perearstidele))* Seega ei ole praegune auditikohustuse regulatsioon meie hinnangul kooskõlas seadusandja tahtega.

Auditeerimise kulude katmiseks ei kohaldu ka EASi poolt loodud toetusmeede.

Peame samas oluliseks seletuskirjas väljatoodut, et erand on kavandatud konkreetselt auditite läbiviimise suhtes, mitte E-ITS-i järgimise kohustuse suhtes.

Eesti infosüsteemide audiitorite ühingu kodulehel leiab 11 audiitor-asutust. 12.06.24 saatis üks perearstikeskus hinnapäringud neist neljale ning ei ole seni neist üheltki tagasisidet saanud. 3 aastat tagasi küsitud pakkumiste järgi on E-ITS auditi hind ühe keskmise suurusega tervisekeskuse jaoks suurusjärgus 10000-30000 eurot. Kuna teenusepakkujaid on vähe, aga nõudlus seaduse alusel hakkab olema neile suur, siis see olukord avaldab tõenäoliselt mõju ka hinna kujunemisel. Seega on oht, et ravirahad hakkavad liikuma ärilist kasu teenivate audiitor-ettevõtete kätte.

Teine mure on seotud perearstikeskuste IKT partnerite küberturvalisuse tagamisega. Sellised teenuspakkujad käitlevad ning säilitavad suures koguses patsientide terviseandmeid ning nende infosüsteeme kasutatakse riiklikult olulise tervishoiuteenuse osutamiseks. Tervishoiu IKT ettevõtte infosüsteemis toimuva infoturbeintsidendi tõenäoline mõju on meie hinnangul suurem kui üksikus perearstikeskuses toimuval intsidendil. Seejuures aga kontrollivad selliste teenusepakkujate tegevust üksnes nende klientideks olevad tervishoiuasutused, sealhulgas väikesed perearstikeskused, kellel puudub sisuline kompetents ja võimekus teenusepakkujate tegevuse piisavaks kontrollimiseks. Seetõttu peame oluliseks, et kirjeldatud teenusepakkujate tegevuse suhtes kohalduksid KüTS-ist tulenevad nõuded ning et nende tegevuse üle oleks võimalik teostada riiklikku järelevalvet.

Lisaks soovitame kaaluda, kas KüTS-ist tulenevate nõuete rakendamine oleks vajalik ja põhjendatud ka laborite, erameditsiini ettevõtete ja muude sarnaste ettevõtete osas, kes töötlevad suures mahus terviseandmeid, ning kelle teenuseid perearstikeskused palju kasutavad.

Tahame olla kindlad, et ettevõtted, kelle teenuseid perearstid kasutavad, vastaksid küberturvalisuse nõuetele ning oleksid usaldusväärsed partnerid tervishoius. Lähtuvalt eeldoodid murekohtadest teeme alljärgnevad ettepanekud KüTSi muutmiseks.

Ettepanekud

1. **E-ITS auditeerimiskohustuse lävendi muutmine**

Muuta küberturvalisuse seaduses (KüTS) kehtestatud nõuet perearstide E-ITS auditeerimise kohuslase lävendit selliselt, et see vastaks NIS2 direktiivi üldreeglile, st auditeerimiskohustust kohaldatakse direktiivi lisades I või II nimetatud üksuste suhtes, mis kvalifitseeruvad soovituse 2003/361/EÜ lisa artikli 2 kohaselt keskmise suurusega ettevõtjateks või ületavad kõnealuse artikli lõikes 1 sätestatud keskmise suurusega ettevõtja piirmäärasid, ning mis osutavad teenuseid või tegutsevad ELis. Vastavalt sellele on keskmise suurusega ettevõte, kus töötab miinimum 50 inimest ja kelle aasta bilansimaht või aastakäive ületab 10 miljonit eurot. Selliseid esmatasandi tervishoiuasutusi on Eestis üksikud ja koostöös Tervisekassaga on mõistlik nendele rakenduva auditi kohustuse kulud katta.

Juhul, kui eeltoodud ettepanek ei ole vastuvõetav, palume kaaluda alternatiivina perearstide E-ITS auditeerimise kohuslase lävendi viimist samale tasemele, mis on kehtestatud majandusaasta aruande auditeerimiskohustuseks audiitortegevuse seaduse §91 lõikes 1 (kaks kriteeriumi vastavalt: tulu/müügitulu 4M€, varad 2M€, 50 töötajat).

2. **KüTS-i kohadamine tervishoiu IKT ettevõtjate ja teiste partnerite suhtes**

KÜTS peaks kohalduma ka tervishoiu infosüsteeme tootvatele ja haldavate ettevõtete suhtes, kelle tegevust on mõistlik reguleerida tsentraalselt. Sellisteks ettevõteteks on näiteks:

- Tervishoiuteenuse osutamiseks kasutatavad infosüsteemid - s.h. perearstide, haiglate, erakliinikute ning laborite infosüsteemid jm.
- Digiregistratuurid tarkvarade juures (näiteks perearstide veebiregistratuur)
- Tervishoiuteenuse osutamisel kasutatavad suhtlusplatvormid, mille kaudu edastatakse konfidentsiaalset infot.
- Eeltoodud süsteemide majutusteenuse pakkujad

Lugupidamisega

Eesti Tervisekassa
Eesti Perearstide Selts
Eesti Esmatasandi Tervisekeskuste Liit