

## **Eesti Perearstide Seltsi tagasiside sihipärase turvaauditi korraldamise määrusele**

06.10.2026

Eesti Perearstide Selts tänab võimaluse eest anda tagasisidet määrusele sihipärase turvaauditi korraldamise täpsemad tingimused ja kord.

Üldise märkusena palume, et tagasisidestamisele eelneks edaspidi alati ka eelnõu tutvustus ja arutelu. Üksnes kirjalike materjalide pealt tagasisidestamisel on tõenäoline, et eelnõu mõju ja puutumus ei ole kõigi osapoolte jaoks piisavalt arusaadav, samuti jõutakse mõistlike lahendusteni tavaliselt diskussiooni käigus.

Teise läbiva põhimõttena toome välja, et perearstiabis, kus tegevus põhineb peaaegu täielikult riiklikul rahastusel, peab kõigi kohustuste lisandumine toimuma koostöös vastava valdkonna ministeeriumi (SoM) ning rahastajaga (Tervisekassa) - et oleks võimalik kokku leppida, millise taseme rahastamist saab riik võimaldada. Nii nõuded kui järelevalveprotsessid tuleb kokku leppida osapoolte koostöös, hõlmates ka rahastuse teemad. Heaks näiteks on siinkohal arvutitöökooha teenuse projekt, kus Tervisekassa, RIA ja perearstide esindajad on välja töötamas töökohateenust, mille osas on eesmärgiks proportsionaalne lahendus, arvestades nii kohalduvaid nõudeid kui rahastuse võimalusi. Samast põhimõttest lähtuvalt tuleb nii valdkonna ministeerium kui Tervisekassa kaasata aruteludesse ka turvaauditi rakendamise ja hüvitamise tingimuste osas - antud teemal ei ole vähemalt meile teadaolevalt toimunud arutelusid ega sõlmitud kokkuleppeid lahenduste leidmiseks.

Eesti Perearstide Selts on korduvalt rõhutanud, et infoturve patsiendi isikuandmete kaitse on perearstide vaates väga oluline, kuid seejuures peavad nõuded - sh menetluslikud tingimused - olema proportsionaalsed ja mõistlikud, et esmatasandi arstiabi toimimist toetada, mitte seda ohustada. Samuti kordame ettepanekut viia läbi tervishoiusektori terviklik analüüs.

Ettepanekud eelnõu sõnastuste osas:

1. **Auditi määramise tingimuste täpsustamine.** Auditi korraldamise täpsemate tingimuste raames tuleb sätestada ka see, milliste asjaolude ja eeltingimuste esinemisel võib Riigi Infosüsteemi Amet sihipäraselt turvaauditit nõuda. Arvestades, et ettevõtja jaoks on tegemist väga koormava meetmega, tuleb eelnõu tekstis muuhulgas selgelt sätestada, et auditit ei rakendata olukordades, kus järelevalve eesmärk on võimalik saavutada vähem koormavate meetmetega, näiteks dokumentide küsimise, enesehindamise või piiratud ulatusega kontrolliga – iseäranis olukorras, kui tegemist on üksusega, millel tavapäraselt ei ole auditikohustust. Samuti tuleb sätestada, et järelevalve teostajal peab olema kohustus põhjendada, milline konkreetne asjaolu või riskiteave auditi tingis, kas see on oluline asjaolu või risk, ja miks ei ole järelevalve eesmärki võimalik saavutada vähem koormava meetmega. Järelevalve väga avar diskretsiooniruum muudab menetluse teenuseosutajate jaoks prognoosimatuks ja tekib risk, et järelevalve vaates võib turvaauditi nõudmine muutuda väga mugavalt rakendatavaks meetmeks, mis annab asjaolude järelevalve poolt detailsema kontrollimise asemel võimaluse nõuda auditeerimist.

Lisaks palume selguse huvides seletuskirjas täpsustada, et olulisele üksusele saab sihipärase turvaauditi määrata üksnes juhul, kui on alust arvata, et konkreetne üksus ei järgi KÜTS-is, eelkõige selle §-des 7 ja 8, sätestatud nõudeid (KÜTS § 14 lg 6 p 3), kuivõrd tegemist on meetmega, mida ei saa rakendada väljaspool riiklikku (või haldus-) järelevalvemenetlust, ning üksnes sektori üldisest riski- või ohuproгноosist olulisele üksusele auditi määramiseks ei piisa.

2. **Subjektide ringi kitsendamine.** Teeme ettepaneku sätestada sihipärase turvaauditi täpsemate tingimuste raames, et sihipärase turvaauditi läbiviimist saab rakendada ainult ettevõtjate suhtes, kellel on e-ITS või ISO 27001 rakendamise kohustus.
3. **Väikese teenuseosutaja auditikulu hüvitamine.** Juhul, kui jääb võimalikuks nõuda sihipärase turvaauditi läbiviimist ka ettevõtjatelt, kellel ei ole e-ITS või ISO 27001 rakendamise kohustust, tuleb kindlasti muuta tingimust, mille kohaselt peab alla 50 töötajaga ja sätestatud finantspiirmääradele vastav teenuseosutaja tõendama, et ta ei ole võimeline auditikulu kandma. Selliselt sõnastatud tõendamiskohustus on ebaproportsionaalselt koormav ja liiga jäik, puudub võimalus tugineda kulude ebaproportsionaalsusele või ebamõistlikkusele. Väikese teenuseosutaja auditikulu tuleks jagada riigi ja teenuseosutaja vahel, arvestades teenuseosutaja suurus, auditi maksumust ning auditi määramise aluseks olnud rikkumise kinnitamist ja olulisust, samuti asjaolu, kas üksusel tavapäraselt e-ITS auditi läbimise/ISO sertifitseerimise kohustus või mitte. Kehtestada tuleb ka väikese teenuseosutaja omaosaluse ülemmäär. Kui audit ei kinnita selle määramise aluseks olnud olulist rikkumist, peaks auditi põhjendatud kulu kandma riik. Arvesse tuleb võtta ka tegevusvaldkonna eripärasid - näiteks perearstikeskuste tegevus põhineb peaaegu täielikult riiklikul rahastusel, mille raames auditikulu ette nähtud ei ole. Seetõttu tuleb auditi maksumuse ja hüvitamise mudelid läbi arutada ka valdkonna rahastajatega.
4. **Esmaseid turvameetmeid rakendava teenuseosutaja auditi ulatus.** Seletuskirjas tuleb selgelt välja tuua, et üksnes esmaseid turvameetmeid rakendavalt teenuseosutajalt ei eeldata E-ITSi või ISO 27001 auditiga võrreldava mahu ja põhjalikkusega sihipärasest turvaauditit. Auditi käsitusala ja kontrollimeetodid peavad lähtuma auditi määramise aluseks olevast konkreetsest riskist ning olema vastavuses teenuseosutajale tegelikult kohalduvate nõuetega. Lisaks palume täpsustada, et muude sõltumatute isikute poolt auditeerimine peaks olema võimalik ka näiteks juhtudel, kus auditeeritakse esmaste meetmete rakendajat. Samuti tuleb tagada, et sellise piiratud ulatusega auditit oleks võimalik tellida mõistliku hinna ja tähtajaga ja/või luua mehhanism juhtude puhuks, kus teenuseosutaja tõendab, et vaatamata tehtud jõupingutustele ei ole õnnestunud RIA poolt aktsepteeritava turuhinnaga auditit tellida. E-ITS kogemus näitas, et väiksel teenusepakkujal oli raske saada pakumisi isegi e-ITS täismahus auditi jaoks, kuivõrd teenusepakkujad eelistasid suuremaid töid; samuti on e-ITS konsultatsioonide hankimisel olnud praktikas murekohaks, et suur osa teenuspakkujatest soovib müüa terviklikku paketti, mitte tegeleda üksikute spetsiifiliste küsimustega. Selle valguses oleme sügavalt mures, kas ja mis tingimustel on praktikas võimalik sellist auditit tellida.
5. **Hüvitatava auditikulu sisu.** Seletuskirjas tuleks täpsustada, et hüvitatava auditikulu hulka võivad kuuluda kõik auditi läbimiseks vajalikud ja põhjendatud kulud, sealhulgas vajaduse korral kolmandalt isikult tehniliste tõendite hankimise kulud (§ 4 lg 3). Näiteks võib perearstikeskuse auditi jaoks vajalik tehniline teave olla IT-partneri või arstitarkvara pakkuja valduses. Auditiga võivad seetõttu kaasneda täiendavad kulud näiteks varunduse kirjelduste või tehniliste seadistuste tõendite koostamise ja väljastamise eest.
6. **Auditi maksumuse eelnev hindamine.** Audiitori sobivuse kinnitamisel peaks RIA teenuseosutaja taotlusel hindama ka kavandatava auditi maksumuse põhjendatust. Kui RIA on hinnapakumise eelnevalt heaks kiitnud, ei tohiks hüvitatavat summat hiljem turuhinnale viidates vähendada, välja arvatud juhul, kui auditi ulatus või maksumus erineb kooskõlastatust. See ei tähenda lõpliku hüvitise eelnevat määramist, kui hüvitise ulatus sõltub auditi tulemusest.

7. **Mõjuanalüüsi täiendamine.** Eelnõu mõjuanalüüsi tuleb täiendada. Praegu keskendutakse peamiselt auditikulu hüvitamise taotlemisega kaasnevale halduskoormusele, kuid ei hinnata piisavalt teenuseosutajale tekkivat majanduslikku mõju juhul, kui auditikulu ei hüvitata või hüvitatakse vaid osaliselt. Mõju hindamisel tuleb arvestada auditi võimalikku maksumust, selle proportsionaalsust teenuseosutaja majandusliku võimekusega ning mõju põhitegevusele ja küberturvalisuse puuduste kõrvaldamisele. Näiteks võib riigi määratud auditi oluline ettenägematu kulu piirata väikese perearstikeskuse võimalusi panustada tervishoiuteenuse osutamisse või auditis tuvastatud puuduste kõrvaldamisse. Auditi harv kasutamine ei tähenda, et selle mõju üksikule teenuseosutajale oleks väike. Kui auditi määramise eeltingimusi ei sätestata, tuleb mõjuanalüüsis hinnata ka eeltingimuste puudumise mõju.

Lugupidamisega

Eesti Perearstide Seltsi juhatuse nimel

Elle-Mall Sadrak