**Tagasiside KüTS jt seaduste muutmise eelnõu kohta**

Eesti Perearstide Selts ja Eesti Esmatasandi Tervisekeskuste Liit edastavad käesolevaga tagasiside küberturvalisuse seaduse (edaspidi **KüTS**) ja teiste seaduste muutmise seaduse (küberturvalisuse 2. direktiivi ülevõtmine) eelnõu kohta.

## 1. Ebapiisav meetmete proportsionaalsuse ja subjektide ringi analüüs

Nõustume, et infoturve on perearstide töös oluline ning et perearstiabi teenuse osutajate (edaspidi **perearst**) suhtes peavad kehtima infoturbe nõuded. Sellised meetmed peavad aga olema proportsionaalsed ning põhinema valdkonna terviklikul analüüsil. Praegusel kujul eelnõus sisalduv lahendus ei vasta meie hinnangul kummalegi tingimusele ning võib kaasa tuua olukorra, kus osades piirkondades ei ole enam võimalik kodule lähedal perearsti poole pöörduda. Küberturvalisuse 2. direktiivi (edaspidi ka **NIS2**) läbimõtlematu ülevõtmine seab ohtu tervishoiuteenuse osutamise toimepidevuse, seades ühtlasi kahtluse alla ka riigi võime jätkuvalt täita talle põhiseaduse § 28 lg-st 1 tulenevaid kohustusi.

### *1.1. Diskretsiooniruum nõuete kehtestamisel ning sektori tervikliku analüüsi puudumine*

Meie arusaamise kohaselt on KüTS-is sätestatud nõuete kõikide perearstide suhtes kohaldamine olnud siseriiklik valik ning ei NIS ega NIS2 direktiivist ei tulene kohustust kohaldada nõudeid selliste perearstikeskuste suhtes, mis ei ole elutähtsa teenuse osutajad (edaspidi **ETO**) ega keskmise suurusega (või suuremad) ettevõtjad. Eelnõu seletuskirjas on tervishoiu valdkonna osas märgitud, et NIS2 direktiivi soovitakse üle võtta võimalikult kitsalt. Seetõttu ei ole põhjenduste järgi arusaadav, mil põhjusel laiendatakse direktiivi ülevõtmisel siseriikliku valikuna regulatsiooni kohaldamisala isikutele, kes NIS ega NIS2 direktiivi reguleerimisalasse ei lange. Olenemata praegu ametis oleva justiits- ja digiministri Liisa-Ly Pakosta teravast kriitikast sellise õigusloome aadressil, kus direktiivide ülevõtmisel rakendatakse neid oluliselt laiemalt kui direktiiv ise nõuab, on püsib Eestis selline õigusloome halb praktika.

Seletuskirja perearste puudutavas osas on viidatud kehtiva KüTS regulatsiooni säilitamisele ning teatud NIS2 artiklitele, kuid ei nähtu, et seejuures oleks (i) tervishoiusektorit tervikuna analüüsitud, (ii) hinnatud meetmete proportsionaalsust, (iii) arvestatud asjaoluga, et perearstid lisati algselt KüTS-i alles Riigikogu menetluses ilma piisava siseriikliku aruteluta (ja Sotsiaalministeeriumi valdkonnapõhistest ekspertteadmistel rajanevatest seisukohtadest hoolimata), ega (iv) arvestatud muutunud olukorraga (eelkõige perearstidest ETO-de võrgustiku loomine ning baasturbemeetmete kehtestamine). Seega on eelnõu vastuolus HÕNTE § 42 lg 1 punktidega 1-3 ning § 43 lg 1 punktidega 3 ja 5.

Seletuskirjas ei ole selgitatud ning meile jääb arusaamatuks:

1. miks peetakse vajalikuks kohaldada nõudeid kõikide perearstide suhtes, kuigi NIS2 nõuaks kohaldamist üksnes kas vähemalt keskmise suurusega ettevõtjate või ETO-deks olevate perearstide suhtes;
2. kas ja millistest kaalutlustest lähtuvalt vastab iga väike perearstikeskus NIS2 direktiivi artikli 2 lg 2 punktides b, c ja e (ehk KüTS § 1 lg $1^4$ punktides 1, 2 ja 4) olevatele kriteeriumidele olukorras, kus üle riigi luuakse ETO-de võrgustik. Samuti, kuidas saadi sellele kriteeriumile vastavate üksuste arvuks 163 (Eestis tegutsevaid perearstikeskuseid on umbes 400, ETO-deks on kavas muuta neist ca 26-60);
3. mille poolest eristuvad perearstid kõigist teistest tervishoiuteenuste pakkujatest, kes samuti töötlevad eriliigilisi isikuandmeid ning on kohustatud edastama andmeid Tervise Infosüsteemi (v.a.

haiglad, kes on ETO-d), ning miks ei kohaldata nende suhtes nõudeid isegi juhul, kui nad on sedavõrd suured, et kvalifitseeruvad vähemalt keskmise suurusega ettevõtjateks ja peaksid seega NIS2 üldreegli kohaselt olema regulatsiooni subjektiks (nt erakliinikud, eriarstiabi osutajad, hambaarstid, laborid jt diagnostikaasutused jne);

4. kas on hinnatud tervishoiu infosüsteeme tootvate ja haldavate ettevõtjate rolli sektoris ja nendega seotud riske, arvestades nende poolt töödeldavate eriliigiliste isikuandmete mahtusid, süsteemide toimimise olulisust ning asjaolu, et väikestel tervishoiuteenuste pakkujatel puuduvad sisulised võimalused nende tegevuse kontrollimiseks.

Ka Sotsiaalministeerium on eelnevate KüTS-iga seotud eelnõude menetlustes viidanud, et tervisoiusektorit tuleks analüüsida tervikuna, mida meie teada ei ole praeguseni tehtud. Süsteemse käsitluse ning riskide hindamise vajadust ilmestavad ka ülaltoodud küsimused. Rahvusvahelise koostöö gruppides avaldatakse teiste Euroopa Liidu liikmesriikide esindajate poolt suurt imestust, et Eestis kohaldatakse kõikide perearstide suhtes niivõrd ulatuslikke nõudeid ning ei ole teada teisi liikmesriike, kus sama tehtaks. Leiame, et infoturbe meetmed peaksid olema kehtestatud selliselt, et suur saab olla üks kahest – kas kohustuste ulatus või subjektide ring – mitte aga mõlemad korraga, nagu praeguses regulatsioonis. Meie arvates oleks mõistlik jätta ulatuslikud nõuded (nagu seda on E-ITS või ISO/IEC 27001 rakendamise kohustus) kohalduma üksnes kitsale subjektide ringile ning kehtestada näiteks määrusandluse teel (või muul moel) baastaseme nõuded sektoris mõnevõrra laiemalt, et vältida „kõik või mitte midagi“ olukorda. Seejuures peaksid nõuded olema riigi poolt tervishoiu jaoks võimaldatavaid ressursse arvestades proportsionaalsed ja realistlikud.

Eeltoodust lähtuvalt teeme ettepaneku analüüsida tervishoiusektori subjektide ringi ja nende suhtes kohaldatavate nõuete ulatust tervikuna.

### *1.2. Nõuete proportsionaalsus ja mõju perearstiabi kättesaadavusele*

Nagu öeldud, peavad ka perearstid infoturbe nõuete olemasolu vajalikuks, kuid need nõuded peaksid olema proportsionaalsed, arvestama valdkonna kui terviku vajadusi, tegevuse eripärasid ning subjektide väiksust. Need peavad toetama, mitte seadma ohtu ravi kättesaadavuse tasakaalustatud arengut käsikäes küberturvalisuse eesmärkide poole pürgimisega.

Küberturvalisuse meetmete rakendamise legitiimseks eesmärgiks saab pidada küberintsidentide, vähendamist ja nende häiriva mõju vähendamist. Põhiseaduse § 11 kohaselt peavad sellist eesmärki taotlevad meetmed olema sobivad, vajalikud ja mõõdukad. Proportsionaalsuse põhimõtte rakendamisel on elementaarne, et mida suuremat ohtu või häiringut on vaadeldavast nähtusest võimalik tajuda, seda intensiivsemad meetmed on selle ärahoidmiseks sobilikud. Seisukoht ei saa olla erinev ka küberturvalisuse taotlemisel – mida suurem on andmeid töötlevast isikust lähtuv risk, seda intensiivsem on lubatav sekkumise määr. Paratamatult tähendab see vajadust hinnata riskiallikaid ning nende gruppe ja kohandada meetmeid lähtuvalt riskide realiseerumise tõenäosusest.

Meie hinnangul aitaks lihtsamate, kitsamate ning tegevuse spetsiifikat arvestavate nõuete kehtestamine kaasa perearstide infoturbe taseme tõstmise eesmärgi saavutamisele, kuivõrd perearstid tuleksid arusaadavamate ja hoomatavamate nõuete rakendamisega paremini toime – seda iseäranis olukorras, kus enamik perearste peab nõuete rakendamisega ise hakkama saama, kuna neil ei ole võimalik teenust väljastpoolt tellida. Sobivamate nõuete väljatöötamisse saab kaasata Riigi Infosüsteemi Ameti, kellega koostöös on varasemalt välja töötatud baasturbemeetmeid perearstidele, mis on Tervisekassa lepingute kaudu kohustuslikud kõigile perearstidele. Proportsionaalsemate nõuete kehtestamine ei avalda perearstide toimepidevusele ega infoturbe tasemele olulist negatiivset mõju, pigem on mõju hoopis positiivne.

Lisaks ei ole meie hinnangul üksiku perearsti teenuse katkestusel olulist mõju perearstiabi toimepidevusele. Arvestades, et üle Eesti luuakse ETO-de võrgustik, ei ole üksiku perearstikeskuse teenuse ajutise katkestuse mõju suur. Lisaks säilib enamasti ka intsidentide korral esmase abi osutamise võimekus. Võimalike intsidentide mõju hindamisel tuleks arvestada ka seda, et perearstidel on kohustus edastada andmed Tervise Infosüsteemi, mis tähendab, et patsiendi terviseandmete ajaloo säilimine ei põhine üksnes perearsti infosüsteemil.

Ebaproportsionaalsed nõuded seevastu on toonud kaasa olukorra, kus perearstide halduskoormus on hüppeliselt suurenenud ning lisandunud on kohustused, mille katmiseks ei ole ressursse ette nähtud. Perearstide tegevus põhineb peaaegu täielikult riiklikul rahastusel ning kehtestatud on ulatuslikud tegevuspiirangud, mis ei võimalda perearstidel muul moel oma sissetulekut suurendada. Samas ei ole aga kahe aasta jooksul leitud nõuete täitmiseks rahastust - kulumudelis on küberturvalisuse jaoks ette nähtud ainult 49 eurot kuus ühe nimistu kohta. Ka tuleviku osas on perearstidele antud selge sõnum, et perearstide küberturvalisuse rahastuse suurendamine ei ole lähiajal võimalik, mis loob olukorra, kus KüTS-ist tulenevate ulatuslike nõuete rakendamine tuleb kliinilise raviressursi ning inimestele abiandmise võimekuse arvelt. Kehtiv standard on mõeldud eelkõige oluliselt suuremate ettevõtete jaoks ning selle rakendamiseks puudub perearstidel ühelt poolt kompetents ja teiselt poolt ressurss teenuse väljastpoolt tellimiseks. Ebaproportsionaalselt suur halduskoormus ning puudulik rahastus ohustavad perearstiabi kättesaadavust. Eestis valitseb juba praegu perearstide puudus ning tulemuseks võib olla, et paljudes piirkondades ei ole lõpuks võimalik kodule lähedal perearsti juurde pääseda, kuna perearstid loobuvad tööst.

Meie hinnang ei ole paljasõnaline. Nagu ülal juba kord viitasime, märkis Sotsiaalministeerium küberturvalisuse seaduse eelnõud kooskõlastamata jättes oma 02.11.2017 kirjas nr 1.2-3/3754-3, et eelnõu toob kaasa täiendava kulu tervishoiuteenuste osutajatele, kelle valikukriteeriumid on jäetud selgitamata ja mis avaldab täiendavat survet Tervisekassa (2017.a Eesti Haigekassa) tervishoiuteenuste loetelule ning sellega seoses negatiivset mõju ravikindlustuse eelarvele. Kritiseeriti ka kergemeelset hinnangut, et küberturvalisuse meetmete rakendamisega kaasnev kulu on vähene ning et eelnõu ei näe ette täiendavaid rahalisi vahendeid tervishoiuteenuste osutamisele. Sotsiaalministeeriumi hoiatused osutusid õigeks, need probleemid ei ole tänaseks muutunud ega leidnud lahendust. Halduskoormuse ja -kulu suurendamine ilma sellega toimetulekuks vajalike rahastusallikateta on seega kujunenud süsteemseks probleemiks, mis saab valimatu küberturvalisuse nõuete karmistamisega muutuda vaid halvemaks.

Julgeme väita, et mõeldavate küberriskide realiseerumisest tingitud üksikute perearstide töö ajutised katkestused või häiringud on laiapindsele tervishoiuteenuste kättesaadavusele väiksem oht kui perearstide vabatahtlik või sunnitud loobumine tööst suurenenud halduskoormuse tõttu, sest viimasel juhul ei ole enam võimalik tagada ka esmase abi kättesaadavust. Eeltoodust tulenevalt teeme ettepaneku, et perearstid, kes pole ETO-d ega vähemalt keskmise suurusega ettevõtjad, tuleks KüTS kohaldamisalast välja jätta või kehtestada nende suhtes näiteks määrusandluse teel või muul moel proportsionaalsed nõuded. Arvestades, et perearstid on kohustatud järgima ka baasturbe meetmeid, ei tähendaks perearstide eelnõust väljajätmine nende jäämist ilma infoturbe nõueteta, ent võimaldaks sihitult, paindlikult ja proportsionaalselt rakendada küberturbe nõudeid vastavalt riskiastmele.

**2. Auditikohutuse lävendi muutmine ja kohustuse täitmise tähtaeg**

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 (auditi maksumus jääb eeldatavasti suurusjärku 10 000 – 30 000 eurot, audiitorite vähesuse tingimustes võivad aga hinnad olla veelgi suurenenud). 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. Lisaks, arvestades auditikohustuslaste hulka,

ei ole Eestis tegutsevate audiitorite hulk kaugeltki piisav auditikohustuse tähtaegseks täitmiseks. Praegusel kujul kehtestatud auditeerimiskohustus on nõue, mille täitmine ei ole suure osa kohuslaste jaoks realistlik ega võimalik.

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

Teeme käesolevaga ettepaneku muuta E-ITS auditeerimise kohuslase lävendit selliselt, et see vastaks NIS2 direktiivi üldreeglile, st auditeerimiskohustust kohaldatakse üksnes ettevõtjate suhtes, kes on vähemalt keskmise suurusega ettevõtjad. Juhul, kui eeltoodud ettepanek ei ole vastuvõetav, palume kaaluda alternatiivina 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). Märgime seejuures, et finantsauditite kaasnev rahaline ja halduskoormus on oluliselt madalam spetsiifilisest E-ITS auditiga kaasnevast kulust.

Juhul, kui auditikohustusega seotud siseriiklikeks aruteludeks kulub aega ning lävendi muutmise otsust ei tehta lähiajal, või kui lävendit otsustatakse mitte muuta, siis palume pikendada auditeerimiskohustuse täitmise tähtaega. Perearstide jaoks saabub tähtaeg käesoleva aasta lõpus.

### 3. Nõuded tervishoiu infosüsteeme tootvatele ja haldavatele ettevõtete

Viimaste aastate praktika kinnitab, et tervishoiu infosüsteeme tootvate ja haldavate ettevõtete intsidentide mõju on oluliselt suurem kui üksiku perearstikeskuse intsidendi mõju, seda nii perearstiabi toimepidevuse kui andmete tervikluse, kättesaadavuse kui konfidentsiaalsuse aspektist – peaaegu kogu Eesti perearstiabisüsteemi toimivus sõltub paari üksiku teenusepakkuja süsteemide tööst. Kohati kasutavad samade arendajate teenuseid ka haiglad vm tervishoiuasutused, mistõttu võib nendega seotud intsidentide mõju tervishoiusektorile olla iseäranis laialdane. Enamikus perearstikeskustes ei hoita enam andmeid kohapeal, vaid need on majutatud infosüsteemide tootjate/haldajate serveristesse. Kirjeldatud teenuspakkujad käitlevad ning säilitavad suures koguses patsientide terviseandmeid ning kuid nende tegevust kontrollivad üksnes klientideks olevad tervishoiuasutused, sealhulgas väikesed perearstikeskused, kellel puudub sisuline kompetents ja võimekus teenusepakkujate tegevuse piisavaks kontrollimiseks. Terviseinfosüsteemide arendajatele koostalitluse ning turvanõuete kehtestamist käsitletakse ka e-Tervise strateegias.

Seetõttu peame oluliseks, et perearstide põhitegevuse seisukohast kõige olulisemate tervishoiu infosüsteemide tootjad ja haldajad oleksid iseseisvad KüTS subjektid ning et nende tegevust reguleeritaks tsentraalselt. Vähem kriitiliste teenuste (nt perearstide tarbeks loodud suhtlusplatvormide) puhul tuleks taaskord analüüsida valdkonna nõudeid ja vajadusi tervikuna. Kaaluda võiks selliste nõuete kehtestamist, mis on võrreldavad süsteemi kasutava tervishoiuteenuse osutaja enda suhtes kehtivate nõuetega.

Kui seejuures piirab tervishoiu infosüsteemide tootjate või haldajate suhtes nõuete kehtestamist oht, et teenused võivad nõuete tulemusel turult kaduda, siis see on selge märk sektorisse kavandatavate nõuete ebaproportsionaalsusest. Perearste ega teisi ettevõtjaid ei tohiks panna olukorda, kus nad peaksid lepingute kaudu nõudma teenusepakkujatelt selliste nõuete täitmist, mille osas on tekkinud kahtlus, kas teenus oleks nõuete õigusaktide tasandil kehtestamise korral kättesaadav.

Teeme ettepaneku, et tervishoiu infosüsteeme tootvate ja haldavate ettevõtete suhtes kehtivad infoturbenõuded tuleks kehtestada tsentraalselt, tuginedes valdkonna terviklikule hindamisele. Sellisteks ettevõteteks on näiteks:

- tervishoiuteenuse osutamiseks kasutatavad infosüsteemid - s.h. perearstide, haiglate, erakliinikute ning laborite infosüsteemid, Tervise Infosüsteemiga liidestatud andmebaasid jm;
- digiregistratuurid tarkvarade juures (näiteks perearstide veebiregistratuur);
- tervishoiuteenuse osutamisel kasutatavad suhtlusplatvormid, mille kaudu edastatakse konfidentsiaalset infot;
- eeltoodud süsteemide majutusteenuse pakkujad.

Lugupidamisega

Eesti Perearstide Selts

Eesti Esmatasandi Tervisekeskuste Liit