

# Kuidas kaitsta isikuandmeid tervishoiuasutuses?

Oluline ei ole, kas tervishoiuteenuse osutajaks on perearst, suur haigla, hambaravikabinet või erakliinik, igaüks neist peab tagama oma patsientide isikuandmete konfidentsiaalsuse. Seejuures tuleb arvestada, et meditsiinisektoris töödeldakse terviseandmeid, mis on eriliigilised isikuandmed ja mille konfidentsiaalset töötlemist nõuab nii seadusandja kui ka kliendid.



## 1. Kontrolli mis lepingud ja mis tingimustel need koostööpartnerite ja töötajatega sõlmitud on

Tuleb analüüsida ja kaardistada kõigi teenuseosutajatega ja koostööpartneritega sõlmitud lepingud. Raviteenust osutav ettevõtja peab tagama, et tal oleks võimalik nõuda isikuandmete turvalist töötlemist koostööpartnerilt ning et oleks üheselt selge, mis on konfidentsiaalne informatsioon ja kuidas sellega ümber võib käia. Tervishoiuteenuse osutajal peab olema kindlus, et andmete väärkasutamisel saab ta nõude esitada lepingu osapoolle vastu. Kui vastutussätteid lepingus reguleeritud ei ole, siis ainus võimalus teistelt osapoolelt midagi nõuda on läbi kahju hüvitamise nõude, mis eeldab reeglina kohtumenetluses nõude esitajale suurt tõendamiskoormist. Leping koostööpartneriga peab andma tervishoiuteenusele kindluse, et koostööpartner teab mida teeb ja kui on toimunud koostööpartnerist tulenevalt või teadmisel intsident, siis kuna ja kuidas peab tervishoiuteenuse osutajat teavitama.

Ka töotajaid ei tohi unarusse jätta. Esiteks peab töötajatele selge olema, kuidas isikuandmeid töödelda tuleb ja milline info on konfidentsiaalne. Teiseks peavad koostööpartneritega suhtlevad töötajad teadma, mida koostööpartneritelt nõuda ja mida lepinguid sõlmides tähele panna.

## 2. Tee selgeks mis andmeid ja kus hoitakse?

Iga organisatsioon peab teadma, mis andmeid neil oma teenuse osutamise raames vaja on ja mis alusel võib andmeid koguda? Põhjendatud ei ole kõikide andmete kogumine, kui neid praktikas vaja ei ole. Seejuures tuleb arvestada, et andmete kogumiseks peab olema õiguslik alus: (i) kas andmete töötlemise kohustus tuleb seadusest, lepingust või andmesubjekti antud nõusolekust? Kui on ära kaardistatud, mis andmeid vaja on, siis tuleb ära kaardistada, kus neid andmeid hoitaks ja kas andmete hoidmise viisid on turvalised? Läbi tuleb mõelda millal ja kuidas toimub andmete hävitamine?

## 3. Koostage isikuandmete töötlemist käsitlevad töökorraldusereeglid töötajatele ja privaatsuseeskirjad patsientidele

Kõik isikuandmete töötlemise reeglid peavad vastama tegelikkusele. See tähendab, et andmete töötlemise reeglid ei või erineda tegelikust olukorrast (protseduuri kohaselt on kõik väga turvaline ja tipp-topp ja tegelikult puudub ülevaade, kes millal mis andmete ligi pääseb ja kuidas neid töötleb). Ka n-õ majavälistel isikutel peab olema võimalus tutvuda reeglitega, mille alusel tervishoiuteenuse osutaja isikuandmeid töötleb. Seejärel on oluline välja töötada privaatsuseeskirjad (privaatsuspoliitika) oma klientidele.

#### **4. Kontrolli üle patsientidelt võetavad nõusolekud ja sõlmitavad lepingud**

Tervishoiuteenuse osutamise lepingud peavad samuti sisaldama isikuandmete sätteid. Eelnimetatud dokumentide juures on oluline teada, et ei piisa lausetest „kõik andmed on konfidentsiaalsed“ või „annate nõusoleku kõigi oma isikuandmete töötlemiseks.“ Kontrolli, kas patsientidele lubatud isikuandmete töötlemise tingimused vastavad tegelikkusele ja kuidas on korraldatud andmete muutmine, ülekandmine ja õiguse olla unustatud rakendamine.

#### **5. Andmed siiski lekivad või on pantvangis! Mis siis tuleb teha?**

Intsidendide toimumist ei saa 100% ette näha ja vältida. Samas saab kindlasti aegsasti välja töötada praktilised sammud, mida teha ja keda tuleb teavitada nii organisatsiooni sees kui ka organisatsiooniväliselt, kui andmetega on juhtunud midagi, mida ei oleks tohtinud. Käsuliin teabe liikumisest ja edasistest korraldustest peab olema selge, sest nii väikesele perearsti praksisele kui ka suurele haiglale võib tekkida suur kahju, kui intsidenti käsitletakse valesti.

#### **6. Kontrolli, kas on vaja määrata andmekaitseametnik?**

GDPR sätestab tingimused, mil organisatsioon peab määrama andmekaitseametniku. Kuna tervishoiuteenuse osutaja põhitegevus hõlmab terviseandmete töötlemist, on tal ilmselt ka andmekaitseametniku määramise kohustus. Isegi, kui tervishoiuteenuse osutaja ei pea määrama andmekaitseametnikku, siis peaksid nad endale leidma nõustaja, kes suudaks neid igapäevaselt ja operatiivselt nõustada isikuandmete teemadel.

#### **7. Koolita ja treeni oma töötajaid**

Enamik probleeme isikuandmete töötlemisega tulenevad sellest, et töötajaid ei ole koolitatud seoses isikuandmete töötlemise põhimõtetega. Organisatsioon võib olla isegi välja töötanud põhjalikud materjalid, aga pahathti ei ole töötajaid nendega tutvunud. Vältida tuleb situatsioone, kus teadmatuses või hoolimatusest tekivad intsidendid. Mängi töötajatega läbi erinevad situatsioonid, et töötajad teaksid millist infot nad telefonis avaldada võivad, millist infot nad teise patsiendi kuulates rääkida võivad, kuidas isikut tuvastada, mida võib avaldada lähedastele.

#### **8. Määra kindlaks ja korralda korrapäraseid vastavuskontrolle, et tuvastada ja parandada probleeme**

Andmekaitsega tuleb tegeleda pidevalt. Oluline on, et regulaarselt vaadatakse üle kõik protseduurireeglid ja koolitatakse töötajaid. Vajadusel vii läbi mõjuhinnangud kontrollimaks, millised ohud võivad esineda või tekkida.



#### **LIISI JÜRGEN**

VANDEADVOKAAT, PARTNER

(+372) 66 76 440

LIISI.JURGEN@NJORDLAW.EE