TIETOTURVAAN LIITTYVÄT LAIT JA MÄÄRÄYKSET

Johanna Hakonen

Sisällysluettelo

1 Johdanto

Asiakasyritys on fiktiivinen fysioterapiakeskus Physio, jonka hoitohenkilökunnan määrä on viisi ja tietohallinnosta vastaa yksi henkilö. IT-ympäristö sisältää Windows-palvelimen ja -työasemia, Microsoft 365:n, Active Directoryn ja lähiverkon. Yrityksellä on Physio-verkkosivut ajanvarausta varten. Yrityksessä käsitellään terveydenhuollon asiakas- ja potilastietoja, mikä vaatii tietosuojaan liittyvien lakien vaatimusten selvittämistä.

STM:n ja THL:n Opas sosiaali- ja terveydenhuollon asiakastietojen käsittelystä (Sandberg, ym., 2025) kertoo, että sitä koskeva sääntely uudistui 1.1.2024, kun laki sosiaali- ja terveydenhuollon asiakastietojen käsittelystä (703/2023) (Finlex, 2025) eli asiakastietolaki tuli voimaan. Muita keskeisiä säädöksiä oppaan mukaan ovat EU:n yleinen tietosuoja-asetus (2016/679, GDPR) (Euroopan Unioni, 2025) eli tietosuoja-asetus ja tietosuojalaki (1050/2018) (Finlex, 1050/2018, 2025). Tietosuojalaki täydentää GDPR:ää Suomen lainsäädännössä. Se säätelee esimerkiksi henkilötietojen käsittelyä työelämässä ja kameravalvonnan käyttöä (OpenAI, 2025). Terveydenhuollon ammattihenkilöitä koskee oppaan mukaan myös terveydenhuollon ammattihenkilöistä annetussa laissa (559/1994) (Finlex, 559/1994, 2025) säädetty salassapitovelvollisuus.

Rikoslain (39/1889) 38. luku ”Tietotekniikkaan liittyvät rikokset” määrittelee tietomurrot, tietojen oikeudettoman käytön ja tietojärjestelmiin kohdistuvat rikokset (OpenAI, 2025). IT-tukihenkilön on hyvä olla tietoinen näistä vastuista. Lisäksi laki sähköisestä tunnistamisesta ja luottamuspalveluista (533/2016) säätelee vahvaa sähköistä tunnistautumista, esimerkiksi jos käytössä on Suomi.fi-tunnistus tai muita tunnistautumispalveluita.

Suoritettiin Eduhousen Tietoturva-asetus GDPR -koulutus (Eduhouse Oy, 2025).

2 Laki sosiaali- ja terveydenhuollon asiakastietojen käsittelystä (703/2023)

Asiakastietolaki säätelee asiakastietojen käsittelyn yleisiä periaatteita, kuten salassapitoa, vaitiolovelvollisuutta ja käyttöoikeuksia, rekisterinpitäjyyttä ja rekistereitä, asiakasasiakirjoihin kirjattavia tietoja sekä tiedonsaantioikeuksia ja asiakastietojen luovutuksia (Sandberg, ym., 2025). Lisäksi asiakastietolaissa säädetään Kansaneläkelaitoksen (Kela) ylläpitämistä valtakunnallisista tietojärjestelmäpalveluista eli Kanta-palveluista ja muista asiakastietojen käsittelyssä käytettävistä tietojärjestelmistä, niiden valvonnasta ja tietoturvallisuudesta.

Asiakastietolain mukaan sosiaali- ja terveydenhuollon palvelunantajan on liityttävä Kanta-palvelujen käyttäjäksi, jos asiakkaiden tietoja käsitellään sähköisessä asiakas- tai potilastietojärjestelmässä (Kanta-palvelut, Kantaan liittyminen ja valmistelut, 2025). Tietojärjestelmän tulee täyttää käyttötarkoituksensa mukaiset olennaiset vaatimukset, jotka jakautuvat kolmeen osa-alueeseen: toiminnallisiin vaatimuksiin, yhteentoimivuuteen sekä tietoturvaan ja tietosuojaan (Valvira, 2025). Näiden täyttämisestä ja ylläpidosta on vastuussa tietojärjestelmäpalvelun tuottaja.

2.1 Velvollisuudet

Asiakastietolain mukaan Physion velvollisuutena terveydenhuollon palvelunantajana potilastietojärjestelmän suhteen ovat muun muassa seuraavat (lista suora kopio) (Valvira, 2025):

- käyttää olennaiset vaatimukset täyttävää tietojärjestelmää, joka vastaa käyttötarkoitukseltaan palvelunantajan ja apteekin toimintaa ja jonka tiedot löytyvät Astori-rekisteristä.
- liittyä Kanta-palvelujen käyttäjäksi säännöksissä kerrottujen määräaikojen mukaisesti, jos palvelunantajalla on käytössään asiakas- ja potilastietojen käsittelyyn tarkoitettu tietojärjestelmä
- vastata Kanta-palveluihin tallennettavien tietojen oikeellisuudesta
- ottaa käyttöön säännösten edellyttämät uudet toiminnot määräaikojen mukaisesti
- pitää rekisteriä asiakas- ja potilastietojärjestelmien käyttäjistä ja näiden käyttöoikeuksista sekä määritellä sosiaali- ja terveydenhuollon ammattihenkilöiden oikeus käyttää asiakas- ja potilastietoja
- kerätä lokitiedot rekisterikohtaisesti kaikesta asiakas- ja potilastietojen sekä lääkemääräysten käytöstä ja luovutuksesta seurantaa ja valvontaa varten
- laatia tietoturvaan ja tietosuojaan sekä tietojärjestelmien käyttöön liittyvä tietoturvasuunnitelma ja ylläpitää sitä
- ilmoittaa tietojärjestelmäpalvelun tuottajalle merkittävistä poikkeamista tietojärjestelmän olennaisten vaatimusten täyttymisessä. Ilmoitus on tehtävä myös Valviralle, jos poikkeama aiheuttaa merkittävän riskin asiakas- tai potilasturvallisuudelle tai tietoturvalle. Poikkeamailmoituksen Valviralle voi tehdä Merkittävä poikkeama -sivulla.
- ilmoittaa tietosuojavaltuutetulle, jos tietojärjestelmän olennaisten vaatimusten täyttymisessä on tietosuojapoikkeama
- tunnistaa luotettavasti asiakastietojen käsittelijä sekä tietotekniset laitteet ja valtakunnalliset tietojärjestelmäpalvelut

- tarkistaa asiakastietoja käsittelevien henkilöiden ja tietoteknisten laitteiden tunnistamisessa käytettävien tunnistusvälineiden voimassaolo tunnistus- ja luottamuspalvelulaissa säädetyn mukaisesti.

2.2 Tietoturvasuunnitelma

Physiolla on oltava käytössään ajantasainen ja dokumentoitu tietoturvasuunnitelma, jotta Kanta-palvelun käytön voi aloittaa (Kanta-palvelut, Tietoturvasuunnitelma, 2025). Tietoturvasuunnitelmaan sisällytettävät selvitykset ja vaatimukset löytyvät THL:n määräyksestä 3/2024 (THL, THL:n määräys 3/2024 tietoturvasuunnitelmaan sisällytettävistä selvityksistä ja vaatimuksista (pdf), 2025). Kyseessä ovat selvitykset siitä, miten asiakastietojen käsittelyyn ja tietojärjestelmiin liittyvät vaatimukset varmistetaan. Mallipohja löytyy THL:n Tietoturvasuunnitelma-sivulta (THL, Tietoturvasuunnitelma, 2025). Tietoturvasuunnitelmassa on kuvattava seuraavat kohdat (luvun 6 mukaiset alakohdat 6.1–6.12):

- yleiset tietoturvakäytännöt
- menettelyt virhe- ja ongelmatilanteissa sekä jatkuvuudenhallinta
- henkilökunnan koulutus sekä osaamisen ylläpito ja kehittäminen
- tietojärjestelmien käyttöohjeet ja ohjeiden mukainen käyttö
- tietojärjestelmien perustiedot, kuvaukset ja olennaisten vaatimusten täyttyminen
- tietojärjestelmien asennus, ylläpito ja päivitys
- Käyttövaltuuksien hallinnan ja tunnistautumisen käytännöt
- asiakas- ja potilastietojärjestelmien pääsynhallinnan ja käytön seurannan käytännöt
- fyysinen turvallisuus osana tietojärjestelmien käyttöympäristön turvallisuutta
- Työasemien, mobiililaitteiden ja käyttöympäristön tukipalveluiden hallinta
- alusta- ja verkkopalvelujen tietoturvallinen käyttö tietosuojan ja varautumisen kannalta
- Kanta-palvelujen liittymisen ja käytön tietoturvakäytännöt

3 Yleinen tietosuoja-asetus

Tietosuoja-asetus (GDPR, General Data Protection Regulation) koskee henkilötietojen keräämistä, säilytystä ja hallinnointia (Euroopan Unioni, 2025). Se edellyttää rekisterinpitäjältä selkeää tietosuojaselostetta ja potilastietojen asianmukaista suojaamista (OpenAI, 2025). Potilailla on oikeus tarkastaa tietonsa ja pyytää niiden korjaamista tai poistamista, ellei lakisääteinen säilytysvelvollisuus estä sitä. Tiedonkäsittelyssä tulee ottaa huomioon tietojen minimointi, täsmällisyys, säilytyksen rajoittaminen sekä tiedon eheys ja luottamuksellisuus (Eduhouse Oy, 2025).

Physionin tulee tehdä julkinen tietosuojaseloste, jossa kerrotaan mitä tietoa kerätään ja miksi, kauan tietoja säilytetään sekä kuvaus rekisteröidyn oikeuksista (perustelut, käsittelytoimet) (Eduhouse Oy, 2025). Lisäksi sillä on ilmoitusvelvollisuus tietosuojapoikkeamista 72 h kuluessa havainnosta. Tietosuojan toteuttaminen on kaikkien vastuulla. Tietosuojavastaavaa ei tarvitse nimetä Physionin mittakaavassa, vaikka käsitellään henkilötunnus- ja terveystietoja (Euroopan Unioni, 2025).

Lähdeluettelo

Eduhouse Oy. (18. Maaliskuu 2025). *Tietosuoja-asetus GDPR - Eduhouse*. Noudettu osoitteesta https://app.eduhouse.fi/palvelu/koulutukset/38187984-38187984?element=38189777

Euroopan Unioni. (18. Maaliskuu 2025). *Yleinen tietosuoja-asetus (GDPR) - Your Europe*. Noudettu osoitteesta https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_fi.htm

Finlex. (19. Maaliskuu 2025). *703/2023*. Noudettu osoitteesta https://www.finlex.fi/fi/lainsaadanto/saadoskokoelma/2023/703

Kanta-palvelut. (19. Maaliskuu 2025). *Kantaan liittyminen ja valmistelut*. Noudettu osoitteesta https://www.kanta.fi/ammattilaiset/kantaan-liittyminen-ja-valmistelut

Kanta-palvelut. (19. Maaliskuu 2025). *Tietoturvasuunnitelma*. Noudettu osoitteesta https://www.kanta.fi/ammattilaiset/tietoturvasuunnitelma

OpenAI. (17. Maaliskuu 2025). *ChatGPT*. Noudettu osoitteesta chatgpt.com

Sandberg, A.;Geitlin, H.;Helenius, I.;Kauvo, T.;Lehmuskoski, A.;Palm, N.;. . . Älander, A. (19. Maaliskuu 2025). *Opas sosiaali- ja terveydenhuollon asiakastietojen käsittelystä*. Noudettu osoitteesta https://yhteistyotilat.fi/wiki08/display/JULOPTA/1+Johdanto

THL. (19. Maaliskuu 2025). *THL:n määräys 3/2024 tietoturvasuunnitelmaan sisällytettävistä selvityksistä ja vaatimuksista (pdf)*. Noudettu osoitteesta https://thl.fi/documents/155392151/190361269/THL_Maarays_3_2024_Tietoturvasuunnitelmaan_sisallytettavista_sevityksista_ja_vaatimuksista.pdf

THL. (19. Maaliskuu 2025). *Tietoturvasuunnitelma*. Noudettu osoitteesta https://thl.fi/aiheet/tiedonhallinta-sosiaali-ja-terveysalalla/tiedonhallinnan-ohjaus/tietoturvasuunnitelma

Valvira. (19. Maaliskuu 2025). *Sosiaali- ja terveydenhuollon tietojärjestelmät*. Noudettu osoitteesta https://valvira.fi/sosiaali-ja-terveydenhuollon-tietojarjestelmat