



TIETOTURVASUUNNITELMA

Asiakastietolain (703/2023) ja EU:n tietosuoja-asetuksen (EU 2016/679) mukainen kuvaus asiakas- ja potilastietojen suojaamisesta

Toimipaikka: Fysio Ohmeroluoma Oy
Tuusantie 3
03100 Nummela

Y-tunnus: 2770575-6

Versio: 1.0
Päivitetty: 25.01.2026
Hyväksytty: 30.01.2026

Jakelu: Julkinen / Asiakkaat



SISÄLLYSLUETTELO

1	Tietoturvan ja tietosuojan periaatteet	3
2	Vastuut.....	3
3	Käytössä olevat tietojärjestelmät.....	3
4	Käyttöoikeuksien hallinta.....	3
5	Lokiseuranta.....	4
6	Fyysinen ja tekninen turvallisuus.....	4
7	Riskienhallinta	4
8	Poikkeamat ja tietoturvaloukkaukset.....	4
9	Toiminnan jatkuvuus	5
10	Henkilöstön koulutus ja salassapito.....	5
11	Asiakirjan saatavuus.....	5
12	Asiakirjan voimassaolo.....	5
13	Hyväksyntä	5



1 TIETOTURVAN JA TIETOSUOJAN PERIAATTEET

Fysio Ohmeroluoma Oy käsittelee potilas- ja asiakastietoja luottamuksellisesti, huolellisesti ja voimassa olevan lainsäädännön mukaisesti.

Toiminnassa noudatetaan erityisesti:

- Asiakastietolaki (703/2023)
- EU:n yleinen tietosuoja-asetus (EU 2016/679)
- Tietosuoja laki (1050/2018)
- Laki potilaan asemasta ja oikeuksista (785/1992)
- THL:n määräys 3/2024

2 VASTUUT

Tietoturvasta vastaa yrityksen johto. Tietosuojavastaava valvoo tietosuojan toteutumista, käyttöoikeuksia, lokiseurantaa ja mahdollisten poikkeamien käsittelyä. Tietoturvasuunnitelma katselmoidaan vuosittain tai merkittävän muutoksen yhteydessä.

3 KÄYTÖSSÄ OLEVAT TIETOJÄRJESTELMÄT

Potilastietojen käsittelyssä käytetään terveydenhuollon vaatimukset täyttävää, Kanta-yhteensopivaa potilastietojärjestelmää. Lisäksi käytössä on turvalliset sähköiset asiointi- ja viestintäpalvelut.

Kaikilla palveluntarjoajilla on voimassa olevat tietojenkäsittelysopimukset (DPA) EU:n tietosuoja-asetuksen mukaisesti. Potilastietojen käsittelyssä noudatetaan Kanta-palvelujen vaatimuksia ja vahvaa tunnistautumista.

4 KÄYTTÖOIKEUKSIEN HALLINTA

- Jokaisella käyttäjällä on henkilökohtainen käyttäjätunnus
- Yhteiskäyttötunnuksia ei käytetä
- Käyttöoikeudet myönnetään työtehtävän mukaisesti
- Käyttöoikeudet poistetaan välittömästi työsuhteen päättyessä
- Vahvaa tunnistautumista käytetään, mikäli mahdollista

5 LOKISEURANTA

Potilastietojärjestelmässä syntyy lokitietoja, joista ilmenee tietojen katselu ja käsittely.

- Lokitietoja seurataan säännöllisesti
- Potilaalla on oikeus pyytää omat lokitietonsa

6 FYYSINEN JA TEKNINEN TURVALLISUUS

- Toimitilat pidetään lukittuina
- Näyttöpäätteet lukittuvat automaattisesti
- Laitteet on suojattu ajantasaisilla tietoturvaratkaisuilla
- Ohjelmistopäivitykset tehdään säännöllisesti
- Tietoliikenne on suojattu
- Paperiaineisto säilytetään lukitussa tilassa ja hävitetään tietoturvallisesti

7 RISKIENHALLINTA

Tietoturvariskejä arvioidaan säännöllisesti osana omaa valvontaa.

Merkittävimpiä tunnistettuja riskejä ovat:

- tietomurrot
- haittaohjelmat
- inhimilliset virheet
- laiterikot
- verkkokatkokset

Näitä ehkäistään muun muassa käyttöoikeuksien hallinnalla, teknisillä suojausratkaisuilla, koulutuksella ja varautumissuunnittelulla.

8 POIKKEAMAT JA TIETOTURVALOUKKAUKSET

Mahdolliset tietoturvaloukkaukset:

- havaitaan ja eristetään viipymättä
- arvioidaan riskin perusteella
- dokumentoidaan
- ilmoitetaan viranomaiselle 72 tunnin kuluessa, mikäli lainsäädäntö sitä edellyttää
- ilmoitetaan rekisteröidyille, jos riski on korkea



9 TOIMINNAN JATKUVUUS

Toiminta voidaan palauttaa häiriötilanteen jälkeen ilman kohtuutonta viivettä.

- Käytössä on varalaitteet
- Pilvipalveluilla on omat jatkuvuussuunnitelmat
- Palautettavuutta testataan säännöllisesti

Toipumisaikatavoite (RTO) on enintään 24 tuntia.

10 HENKILÖSTÖN KOULUTUS JA SALASSAPITO

- Henkilöstö perehdytetään tietosuojaan ja tietoturvaan
- Tietoturvakoulutusta järjestetään vuosittain
- Kaikki työntekijät ja alihankkijat ovat sitoutuneet salassapitoon

11 ASIAKIRJAN SAATAVUUS

Tämä julkinen tietoturvasuunnitelma on saatavilla yrityksen verkkosivuilla.

Yksityiskohtainen sisäinen tietoturvasuunnitelma, versionhallinta ja omavalvonnan seuranta-aineisto säilytetään yrityksen hallitussa ympäristössä ja esitetään valvovalle viranomaiselle pyydettyäessä.

12 ASIAKIRJAN VOIMASSAOLO

Tämä tietoturvasuunnitelma on voimassa toistaiseksi ja tarkistetaan vähintään kerran vuodessa tai merkittävän toiminnallisen tai järjestelmämuutoksen yhteydessä.

13 HYVÄKSYNTÄ

Yrityksen johto sitoutuu varmistamaan suunnitelman toteutumisen, seurannan ja säännöllisen päivittämisen voimassa olevan lainsäädännön mukaisesti.

Tämä tietoturvasuunnitelma on hyväksytty Fysio Ohmeroluoma Oy:n johdon toimesta ja otettu käyttöön 30.01.2026.

Allekirjoitus:

Hannele Ohmeroluoma
Toiminnanjohtaja