



Valvira

Sosiaali- ja terveysalan
lupa- ja valvontavirasto

Poikkeamista ilmoittaminen

Antti Härkönen, yli-insinööri

11.4.2024

Esityksen sisältö

- Poikkeama asiakastietolaissa
- Merkittävän poikkeaman määritelmä
- Ilmoituksen tekeminen
- Ilmoituksen sisältö
- Vaaratilanneilmoitus ja NIS-häiriöilmoitus
- Kyberturvallisuusdirektiivi NIS2
- Esimerkit poikkeamailmoituksista
- Poikkeamailmoituksen käsittely

Poikkeamista ilmoittaminen (90 §)

- Jos palvelunantaja tai apteekki havaitsee, että tietojärjestelmän olennaisten vaatimusten täyttymisessä on merkittäviä poikkeamia, sen on ilmoitettava asiasta **tietojärjestelmäpalvelun tuottajalle**.
- Jos tietojärjestelmän tai hyvinvointisovelluksen poikkeama voi aiheuttaa **merkittävän riskin** asiakas- tai potilasturvallisuudelle tai tietoturvalle, on palvelunantajan, apteekin, tietojärjestelmäpalvelun tuottajan tai tietojärjestelmän/hyvinvointisovelluksen valmistajan, Kelan tai THL:n ilmoitettava siitä Valviralle.
- Myös muu taho voi ilmoittaa Valviralle havaitsemistaan riskeistä.
- Henkilötietojen tietoturvaloukkauksista ilmoittamisesta tietosuojavaltuutetulle säädetään tietosuoja-asetuksen 33 artiklassa.

Merkittävän poikkeaman määritelmä

- THL:n määräyksessä 5/2021 → uusi määräys tulossa
- Poikkeamat, jotka aiheuttavat esimerkiksi
 - Riskejä potilas- tai asiakasturvallisuudelle
 - Merkittäviä riskejä tietosuojalle, tietoturvallisuudelle tai palvelunantajan toiminnalle.

Ilmoituksen tekeminen

- Valviran sivulla oleva turvalomake tai vapaamuotoisesti kirjaamoon.
- Palvelunantajalla voi olla käytössä oma ilmoituskanava, josta ilmoitukset välitetään keskitetysti Valviraan.
- [Lisätietoja poikkeamailmoituksista ja ilmoituslomake](#)

[Tee poikkeamailmoitus Valviralle](#) ↗

Voit tehdä myös vapaamuotoisen poikkeamailoituksen ja toimittaa sen Valviran kirjaamoon sähköpostiosoitteeseen kirjaamo@valvira.fi. Jos lähetät salassa pidettävää tietoa, käytä suojattua sähköpostiyhteyttä <https://turvaviesti.valvira.fi>. Voit lähettää poikkeamailoituksen myös postilla osoitteeseen Valvira/Kirjaamo, PL 43, 00521 Helsinki.

Poikkeamailoituksen perusteella Valvira voi aloittaa valvonnan, joka voi kohdistua tietojärjestelmäpalvelun tuottajaan tai tietojärjestelmää käyttävään sosiaali- ja terveydenhuollon palvelunantajaan.

Ilmoita tietoturvapoikkeamasta (NIS-ilmoitus)

Sosiaali- ja terveydenhuollon tietoturvavauhkista ja -loukkauksista on suositeltavaa ilmoittaa Liikenne ja viestintävirasto Traficomin Kyberturvallisuuskeskukselle. Kyberturvallisuuskeskukselta ilmoitus välittyy myös Valviralle.

[Tee NIS-ilmoitus Kyberturvallisuuskeskukselle](#) ↗

Ilmoituksen sisältö

- Turvalomakkeessa kysytään seuraavat tiedot
 - Yhteystiedot lisätietoja varten
 - Onko ilmoitettu tietojärjestelmäpalvelun tuottajalle
 - Poikkeaman ajankohta ja kuvaus
 - Lisätietoja korjauksista tai jatkotoimenpiteistä
 - Muut toimijat, joille poikkeamasta on ilmoitettu
 - Aluehallintovirasto, Kyberturvallisuuskeskus, Fimea, Tietosuojavaltuutettu, Poliisi
 - Mahdolliset liitetiedostot

Vaaratilanneilmoitus ja NIS-häiriöilmoitus

- CE-merkittyjä lääkinnällisiä laitteita koskee vaaratilanneilmoitusmenettely
 - Sama tietojärjestelmä voi olla sekä lääkinnällinen laite että asiakastietolain mukainen järjestelmä
 - Läkinnällisten laitteiden toimivaltainen viranomainen on Fimea
 - Jos ei merkittävää riskiä → ilmoitus valmistajalle tai tietojärjestelmäpalvelun tuottajalle riittää
- Kyberturvallisuuslain perusteella lisäksi NIS-häiriöilmoitusmenettely
 - Ilmoittaminen tapahtuu Traficomien ilmoituslomakkeelle, josta terveydenhuoltosektoria koskeva ilmoitus välittyy Valviraan
 - [Lisätietoja Kyberturvallisuuskeskuksen verkkosivuilta](#)

Euroopan unionin kyberturvallisuusdirektiivi NIS2

- NIS2 tulee voimaan 17.10.2024
- Asiakastietolaissa huomioitu (90 § 2. momentti)
 - Palvelunantajan, apteekin, Kansaneläkelaitoksen ja tietojärjestelmäpalvelun tuottajan tai tietojärjestelmän valmistajan tai välittäjän on ilmoitettava viipymättä Valviralle sellaisesta sen käyttämiin **käyttöympäristöihin ja tietoverkkoihin kohdistuvasta merkittävästä tietoturvallisuuteen liittyvästä häiriöstä**, jonka seurauksena tietojärjestelmien käyttö ja sosiaali- ja terveystietojen toteuttaminen voi merkittävästi vaarantua.
- Toimijalla on oltava käytössä ajantasainen kyberturvallisuuden riskienhallinnan toimintamalli viestintäverkkojen ja tietojärjestelmien ja niiden fyysisen ympäristön suojaamiseksi poikkeamilta ja niiden vaikutuksilta.

Esimerkkejä poikkeamailmoituksista

- Tietojärjestelmän käyttöönottoihin liittyvät ongelmat
- Järjestelmän käytön yhteydessä löytyneet virheet
- Tietoturvaan ja tietosuojaan liittyvät puutteet
- Lisäksi esimerkiksi konesalipalveluihin tai muuhun palvelutuotantoon (fyysiseen infraan) liittyvät ongelmat

Poikkeamailmoitusten käsittely

- Valvira varmistaa, että tietojärjestelmäpalvelun tuottaja tai valmistaja on saanut tiedon ja ryhtynyt toimenpiteisiin
 - Yhteydenotto tietojärjestelmäpalvelun tuottajaan
 - Valmistajalla on oltava laatujärjestelmä ja menettelytapa virhetilanteiden käsittelyyn
- Tarvittaessa voidaan avata erillinen valvonta-asia
 - Selvityspyyntö
 - Tarkastus
 - Tarvittaessa määräys puutteiden korjaamiseksi

Lainsäädäntö ja lisämateriaali

- [Laki sosiaali- ja terveydenhuollon asiakastietojen käsittelystä eli asiakastietolaki \(703/2023\)](#)
- [Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista \(617/2009\)](#)
- [Sosiaali- ja terveysministeriön asetus käyttöoikeudesta asiakastietoon \(825/2022\)](#)
- [Laki sähköisestä lääkemääräyksestä \(61/2007\)](#)
- [Määräys 3/2024: Määräys tietoturvasuunnitelmaan sisällytettävistä selvityksistä ja vaatimuksista](#)
 - [Liite 1: Tietoturvasuunnitelman mallipohja](#)
- **Määräys 4/2021: Määräys sosiaali- ja terveydenhuollon tietojärjestelmien luokittelusta ja sertifioinnista**
- **Määräys 5/2021: Määräys sosiaali- ja terveydenhuollon tietojärjestelmien olennaisista toiminnallisista ja tietoturvavaatimuksista**
- [Valviran verkkosivusto Sosiaali- ja terveydenhuollon tietojärjestelmät](#)



Valvira

Sosiaali- ja terveysalan
lupa- ja valvontavirasto

Yhteystiedot

antti.harkonen@valvira.fi

valvira.fi

[@ValviraViestii](https://twitter.com/ValviraViestii)

Vaikuttava valvonta – vastuulliset toimijat