



**Valvira**

Sosiaali- ja terveysalan  
lupa- ja valvontavirasto

# Hyvinvointialueet tietojärjestelmien valvojina

**10.11.2022**

Antti Härkönen, yli-insinööri

# Valvonta perustuu lainsäädäntöön

- **Valvira** valvoo tietojärjestelmiä ns. asiakastietolakiin perustuen (Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä 784/2021)
- Lisäksi Verkk- ja tietoturvadirektiiviin (NIS) perustuva valvonta sekä
- Toisiolakiin perustuva valvontatehtävä
- **Fimea** valvoo CE-merkittyjä lääkinnällisiä laitteita, tarvikkeita sekä tietojärjestelmiä.

# Valviran asiakastietolakiin perustuvat tehtävät

Ylläpitää rekisteriä vaatimustenmukaisista A- ja B-luokan tietojärjestelmistä.

Ohjaa, valvoo ja edistää ennakoivasti tietojärjestelmien vaatimustenmukaisuutta

Käsittelee ilmoituksia merkittävistä asiakasturvaa tai tietoturvallisuutta vaarantavista poikkeamista.

Valviralla on oikeus tehdä valvonnan edellyttämiä tarkastuksia.

# Asiakastietolain muutoksia (784/2021)

- Yksityisten toimijoiden Kanta-liittymisvelvoitteen tarkennukset 7 §
  - ”Yksityisen sosiaali- ja terveydenhuollon palvelunantajan on liityttävä valtakunnallisten tietojärjestelmäpalvelujen käyttäjäksi, jos sillä on käytössään asiakas- ja potilastietojen käsittelyyn tarkoitettu tietojärjestelmä.”
- Uutena rekisteröintikohteena hyvinvointisovellukset
  - Mahdollisuus tallentaa hyvinvointitietoja omatietovarantoon
  - Myös nämä hyvinvointisovellukset tulee jatkossa ilmoittaa Valviran rekisteriin
- Muutoksia tietojärjestelmien luokitteluun
- Tarkentavat THL:n määräykset päivitetty samalla ([THL määräykset](#))

# Tietoturvasuunnitelma (THL 3/2021)

- Sosiaali- ja terveydenhuollon palvelujen antajan on laadittava tietoturvasuunnitelma (aikaisempi tietoturvallisuutta koskeva omavalvontasuunnitelma)
- Suunnitelmasta selvittävä, miten on varmistettu esimerkiksi:
  - Käyttäjien koulutus
  - Käyttöohjeiden saatavuus
  - Järjestelmien ylläpito ja päivitys
- Tietoturvasuunnitelman ei tarvitse (eikä pidäkään) olla julkisesti saatavilla.

# Muutostilanteet ja vastuut

- Tietojärjestelmäpalvelun tuottajalla vastuu tuotteestaan
  - Valviran rekisteröintitietojen ajantasaisuus
  - Luokasta riippuen lisäksi Kelan yhteistestaus ja
  - Tietoturvallisuuden arviointilaitoksen vaatimustenmukaisuustodistus
- Sote-palvelunantaja vastaa omasta toiminnastaan
  - Laadittava tietoturvasuunnitelma
  - ”Palvelunantajan käyttämien tietojärjestelmien on vastattava käyttötarkoitukseltaan palvelunantajan toimintaa ja täytettävä palvelunantajan toimintaan liittyvät olennaiset vaatimukset. Olennaiset vaatimukset voidaan täyttää yhden tai useamman tietojärjestelmän muodostaman kokonaisuuden kautta.”
  - Merkittävistä poikkeamista ilmoitettava tietojärjestelmäpalvelun tuottajalle sekä Valviralle.

# Poikkeamista ilmoittaminen

- Lääkinnällisillä laitteilla vaaratilanneilmoitusmenettely
- Asiakastietolaissa kuvattu poikkeamat ja niistä ilmoittaminen
- Jos poikkeama voi aiheuttaa merkittävän riskin asiakasturvallisuudella tai tietoturvalle, ilmoitetaan tietojärjestelmäpalvelun tuottajalle sekä Valviralle
  - Määräyksessä THL 5/2021 määritelty merkittävä poikkeama
- Valviran rekisterissä tulee näkyä:
  - Tieto luokkaan A kuuluvan tietojärjestelmän ja hyvinvointisovelluksen merkittävästä poikkeamasta poikkeaman keston ajan.

# Lisätietoja

- Tietojärjestelmiin liittyvä ohjeistus
  - <https://www.valvira.fi/terveydenhuolto/sosiaali-ja-terveydenhuollon-tietojarjestelmat>
- Asiakastietolaki
  - <https://www.finlex.fi/fi/laki/alkup/2021/20210784>
- THL:n määräykset
  - <https://thl.fi/fi/web/tiedonhallinta-sosiaali-ja-terveysalalla/maaraykset-ja-maarittelyt/maaraykset>
- NIS lisätietoja ja häiriöilmoituslomake
  - <https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/digitaaliset-palvelut-ja-infrastruktuuri?toggle=Ilmoita%20tietoturvapoikkeamasta%20%28NIS-ilmoitusvelvollisuus%29>
- Antti Härkönen, [etunimi.sukunimi@valvira.fi](mailto:etunimi.sukunimi@valvira.fi), p. 0295 209 530, @AnttiHarkonen