Valvira
Sosiaali- ja terveysalan lupa- ja valvontavirasto

Tietojärjestelmien rekisteri ja valvonta

15.12.2021

Antti Härkönen, yli-insinööri

Valvonta perustuu lainsäädäntöön

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

Valvira

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.

Valvira

Asiakastietolaki

- Laki 784/2021 sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä
- Laki määrittelee yleiset vaatimukset tietojärjestelmille ja niiden valmistajille (tai tietojärjestelmäpalvelun tuottajille) sekä sosiaali- ja terveydenhuollon palvelujen antajille.
- Tietojärjestelmällä tarkoitetaan tietojenkäsittelylaitteista, ohjelmistoista ja muusta tietojenkäsittelystä koostuvaa kokonaisjärjestelyä, jota valmistajan suunnittelemien ominaisuuksien mukaisesti on tarkoitettu käytettäväksi asiakastietojen sähköiseen käsittelyyn, asiakasasiakirjojen tallentamiseen ja ylläpitoon tai valtakunnallisiin tietojärjestelmäpalveluihin liittämiseen tai jolla sosiaali- ja terveydenhuollon ammattihenkilö voi hyödyntää hyvinvointitietoja.
- Tietojärjestelmä voi samalla olla myös CE-merkitty lääkinnällinen laite.

Tietoturvasuunnitelma

- Palvelunantajan, välittäjän ja Kansaneläkelaitoksen 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.

Valvira

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 uudistetaan samalla

Valvira

Vuoden 2022 suunnitelmissa

- Tietojärjestelmärekisterin uudistaminen
  - Yksityiskohtainen aikataulu tarkentumatta
  - Pakolliset muutokset toteutetaan nykyiseen rekisteriin
- Rekisteri-ilmoitukselle ja liitteille valmisteilla turvalomakeratkaisu
- Verkkosivujen uudistaminen
- Tarkastustoiminnan kehittäminen
- Rekisteröintimaksut tulossa (maksuasetusta ei vahvistettu)
- Luokan B valvontakyselyn tulosten perusteella tehtävä jatkovalvonta
- KTK:n verkkoskannaukseen liittyvä palveluntarjoajien ohjaus

Valvira

Valviran tietojärjestelmärekisteri

- Asiakastietolain 30 §:n mukaan rekisterissä tulee olla tieto
  - tuotantokäyttöön tarkoitetuista tietojärjestelmistä ja hyvinvointisovelluksista, niiden käyttötarkoituksista sekä niiden täyttämistä olennaisista vaatimuksista;
  - luokkaan A kuuluvien tuotantokäyttöön hyväksyttyjen tietojärjestelmien ja hyvinvointisovellusten yhteentoimivuuden testauksen tuloksista;
  - luokkaan A kuuluvien tuotantokäyttöön hyväksyttyjen tietojärjestelmien ja hyvinvointisovellusten tietoturvallisuuden arvioinnista saadun tietoturvallisuuden arviointia koskevan todistuksen voimassaolosta; sekä
  - tuotantokäytössä olevan luokkaan A kuuluvan tietojärjestelmän ja hyvinvointisovelluksen merkittävästä poikkeamasta poikkeaman keston ajan.

Valvira

Vanhenevat tietoturvallisuustodistukset

- Jos järjestelmän tietoturvallisuustodistus (ennen vaatimustenmukaisuustodistus) on vanhentunut, Valvira merkitsee tietojärjestelmärekisteriin poikkeaman (asiakastietolaki 30 §:n 2 mom. 4 kohta)
  - *Tietoturvallisuustodistus voidaan myöntää vain suoritetusta tietoturvallisuuden arvioinnista, eikä todistuksen määräaikaa voi pidentää ilman lainsäädännöllistä perustetta (asiakastietolaki 37 §:n 2 mom).*
- Valvira selvittää asiaa valvontatehtävänsä mukaisesti
- Huomioi myös:
  - Tietojärjestelmäpalvelun tuottajan on ilmoitettava *tietojärjestelmän olennaisten vaatimusten merkittävistä poikkeamista kaikille järjestelmää käyttäville palvelunantajille (asiakastietolaki 32 §:n 1 mom.)*
  - Palvelunantaja ei saa ottaa käyttöön järjestelmää, johon Valviran tietojärjestelmärekisteristä löytyvien tietojen perusteella kohdistuu merkittävä poikkeama (THL:n määräys 4/2021, luku 9 Tietojärjestelmän käyttöönotto).

Valvira

Asiakastietojen välityspalvelu (1/2)

- Valviran tietojärjestelmärekisterissä on tällä hetkellä lukuisia potilastietojärjestelmiä, jotka eivät oletettavasti ole asiakastietojen välityspalveluita (THL:n määräys 4/2021, luku 3 Määritelmät):
  - *Asiakastietojen välityspalvelulla tarkoitetaan sosiaali- ja terveydenhuollon organisaation tai apteekin Kanta-palveluihin liittymisessä hyödyntämä tietojärjestelmää tai tietojärjestelmäpalvelua, jonka kautta teknisesti siirretään toisen tietojärjestelmän tai tietojärjestelmäpalvelun tuottamia tietoja Kanta-palveluihin tai hyödynnetään toisella tietojärjestelmällä tai tietojärjestelmäpalvelulla Kanta-palveluissa olevia tietoja, ja jossa ei ole Kanta-palveluihin liittyvän tietojärjestelmän loppukäyttäjille suunnattuja ominaisuuksia.*
- Esimerkkejä järjestelmien luokittelusta -liitteen kohdasta A1 löydät lisätietoa asiakastietojen välityspalvelun määritelmästä.

Valvira

Asiakastietojen välityspalvelu (2/2)

- Toimi näin, jos tietojärjestelmäsi on merkitty virheellisesti asiakastietojen välityspalveluksi Valviran tietojärjestelmärekisteriin:
  1. Tee Valviralle muutosilmoitus (rekisteri-ilmoitus), jossa kerrot, että järjestelmä ei ole asiakastietojen välityspalvelu.
  2. Huomioi tarvittaessa asia myös järjestelmälomakkeessa, jonka liität ilmoitukseen.
     - Käytän THL:n sivustolta uusinta järjestelmälomaketta.
  3. Lähetä ilmoitus liitteineen osoitteeseen kirjaamo@valvira.fi
  4. Jos järjestelmään on tehty muita muutoksia, ilmoita samalla myös niistä.

Valvira

Tietojärjestelmien valvontaresurssit 15.12.2021

- Ylitarkastaja Jenni Björkman
- Ylitarkastaja Marko Elo
- Ylitarkastaja Essi Haglund
- Yli-insinööri Antti Härkönen
- Haettavana uusi ylitarkastaja/yli-insinööri

Valvira

Lisätietoja

- Tietojärjestelmiin liittyvä ohjeistus
  - https://www.valvira.fi/terveydenhuolto/sosiaali-ja-terveydenhuollon-tietojarjestelmat
- Uusi asiakastietolaki
  - https://www.finlex.fi/fi/laki/alkup/2021/20210784
- 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, p. 0295 209 530, @AnttiHarkonen

Valvira