Valvira
Sosiaali- ja terveysalan lupa- ja valvontavirasto

Tietoturvasuunnitelma

Marko Elo, ylitarkastaja

11.4.2024

Tietoturvasuunnitelma

- Tieturvasuunnitelmasta on säädetty laissa sosiaali- ja terveydenhuollon asiakastietojen käsittelystä (703/2023, jäljempänä asiakastietolaki):
  - Tietoturvasuunnitelma 77 § sekä
  - Tietoturvallisuuden omavalvonnan toteuttaminen ja vastuu 78 §

- Terveyden ja hyvinvoinnin laitoksen määräys 3/2024 tietoturvasuunnitelmaan sisällytettävistä selvityksistä ja vaatimuksista
  - Liite 1: Tietoturvasuunnitelman mallipohja

Valvira

Tietoturvasuunnitelma 77 § (1/2)

- Palvelunantajan, apteekin, välittäjän ja Kansaneläkelaitoksen on laadittava tietoturvaan ja tietosuojaan sekä tietojärjestelmien käyttöön liittyvä tietoturvasuunnitelma
- Tietoturvasuunnitelmassa on selvitettävä, miten asiakas- ja potilastietojen käsittelyyn ja tietojärjestelmiin liittyvät vaatimukset varmistetaan:
  1. henkilöillä, jotka käyttävät tietojärjestelmiä, on niiden käytön vaatima koulutus;
  2. tietojärjestelmien yhteydessä on saatavilla niiden asianmukaisen käytön kannalta tarpeelliset käyttöohjeet;
  3. tietojärjestelmiä käytetään tietojärjestelmäpalvelun tuottajan antaman ohjeistuksen mukaisesti;
  4. tietojärjestelmiä ylläpidetään ja päivitetään tietojärjestelmäpalvelun tuottajan ohjeistuksen mukaisesti;

Valvira

Tietoturvasuunnitelma 77 § (2/2)

5. tietojärjestelmän käyttöympäristö soveltuu tietojärjestelmien asianmukaiseen sekä tietoturvan ja tietosuojan varmistavaan käyttöön ja käyttöympäristöön ja tietojärjestelmiin kohdistuvien riskien hallinnasta huolehditaan;
6. tietojärjestelmiin liitetyt muut tietojärjestelmät tai muut järjestelmät eivät vaaranna tietojärjestelmien suorituskykyä eivätkä niiden tietoturva- tai tietosuojaominaisuuksia;
7. tietojärjestelmiä asentaa, ylläpitää ja päivittää vain henkilö, jolla on siihen tarvittava ammattitaito ja asiantuntemus ja jonka luotettavuus on varmistettu julkisen hallinnon tiedonhallinnasta annetun lain (906/2019) 12 §:ssä tarkoitetulla tavalla, jos henkilö tehtävissään pääsee käsittelemään asiakastietoja tai jos hän muuten tehtävissään voi vaarantaa sosiaali- ja terveydenhuollon jatkuvuuden kannalta kriittisten tietojärjestelmien toimintaa;
8. tietojärjestelmät täyttävät käyttötarkoituksensa mukaiset 84 §:ssä säädetyt olennaiset vaatimukset; sekä
9. palvelunantajalla, apteekilla, välittäjällä ja Kansaneläkelaitoksella on suunnitelma siitä, miten tietoturvan ja tietosuojan omavalvonta järjestetään ja toteutetaan sen toiminnassa.

Valvira

Tietoturvallisuuden omavalvonnan toteuttaminen ja vastuu 78 §

- Sosiaali- ja terveydenhuollon palvelunantajan vastaavan johtajan ja apteekkarin on huolehdittava, että 77 §:ssä tarkoitettu tietoturvasuunnitelma laaditaan ja sitä noudatetaan
- Palvelunantajan, apteekin ja Kansaneläkelaitoksen tulee oma-aloitteisesti ryhtyä tarvittaviin toimenpiteisiin, jos joku on lainvastaisesti käsitellyt asiakastietoja
- Tietosuojavastaavan nimittämisestä sekä tietosuojavastaavan asemasta ja tehtävistä säädetään tietosuoja-asetuksen 37–39 artiklassa

Valvira

THL määräys 3/2024 tietoturvasuunnitelmaan sisällytettävistä selvityksistä ja vaatimuksista

- Määräys perustuu sosiaali- ja terveydenhuollon asiakastietojen käsittelystä annetun lain (703/2023) 77 ja 78 §:ään
- Määräys tarkentaa sosiaali- ja terveydenhuollon digitaalista tai ei-digitaalista asiakastietojen turvallista käsittelyä
- Tietoturvasuunnitelman avulla kootaan sosiaali- ja terveydenhuollon toimijoiden tietoturvallisuuskäytäntöjä. Palvelunantajien laatimissa tietoturvasuunnitelmissa on oltava selvitykset siitä, miten asiakastietojen käsittelyyn ja tietojärjestelmiin liittyvät vaatimukset varmistetaan asiakastietolain 77 §:n 1 momentin kohtien 1–9 mukaisesti
- Palvelunantajan velvollisuutena on toimia laatimansa tietoturvasuunnitelman mukaisesti, säännöllisesti ylläpitää ja katselmoida suunnitelmaansa sekä seurata aktiivisesti sen toteutumista

Valvira

THL:n määräys tietoturvasuunnitelmaan sisällytettävistä selvityksistä ja vaatimuksista on julkaistu

- Tietoturvasuunnitelmien avulla sosiaali- ja terveydenhuollon toimijoita ohjataan riittäviin ja yhdenmukaisiin tietoturva- ja tietosuojakäytäntöihin
- Kyse on jatkuvasta ja säännöllisestä riskien hallinnasta, asianmukaisten tietoturvallisuuteen ja asiakastietojen käsittelyyn liittyvien käytäntöjen varmistamisesta sekä niiden toteutumisesta
- Tietoturvasuunnitelma on aina ei-julkinen asiakirja
- Määräys 3/2024: Määräys tietoturvasuunnitelmaan sisällytettävistä selvityksistä ja vaatimuksista
  - Liite 1: Tietoturvasuunnitelman mallipohja

Valvira

Sisällys

Terveyden ja hyvinvoinnin laitoksen määräys 3/2024 tietoturvasuunnitelmaan sisällytettävistä selvityksistä ja vaatimuksista

THL järjestää koulutustilaisuuden tietoturvasuunnitelmasta 4.6.2024 klo 9-11.30

Valvira

Valvira
Sosiaali- ja terveysalan lupa- ja valvontavirasto

Yhteystiedot

valvira.fi
@ValviraViestii

Vaikuttava valvonta – vastuulliset toimijat