Määräys omavalvontasuunnitelmaan sisällytettävistä selvityksistä ja vaatimuksista

Valtuutussäännökset

Sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetun lain (159/2007) 19 h §, sellaisena kuin se on laissa 250/2014[1].

Laki sähköisestä lääkemääräyksestä (61/2007) 22 b §, sellaisena kuin se on laissa 251/2014 [2].

Kohderyhmät

Sosiaalihuollon palvelujen antajat
Terveydenhuollon palvelujen antajat
Kanta-välityspalveluiden tuottajat
Apteekit
Kansaneläkelaitos

Voimassaoloaika

Määräys tulee voimaan 1. päivänä helmikuuta 2015 ja se on voimassa toistaiseksi.

[1]Laki asiakastietojen sähköisestä käsittelystä http://www.finlex.fi/fi/laki/ajantasa/2007/20070159
[2]Laki sähköisestä lääkemääräyksestä www.finlex.fi/fi/laki/ajantasa/2007/20070061

Sisällys

1. Määräyksen soveltamisala

Määräys omavalvontasuunnitelmaan sisällytettävistä selvityksistä ja vaatimuksista koskee sosiaali- ja terveydenhuollon palvelun antajia, apteekkeja ja itsenäisiä ammatinharjoittajia, Kansaneläkelaitosta sekä Kanta-välityspalveluiden tuottajia. Kohteena olevista tahoista käytetään tässä määräyksessä yleisnimeä omavalvonnan kohde.

Määräys perustuu sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetun lain (159/2007) kohtiin 19 h § ja 19 i § sekä sähköisestä lääkemääräyksestä annetun lain (61/2007) 22 b §:ään, sellaisena kuin se on laissa 251/2014.

Terveyden ja hyvinvoinnin laitokselle on annettu lain 19 h §:n 4 momentissa valtuutus antaa tarkempia määräyksiä 1 ja 2 momentissa tarkoitetuista omavalvontasuunnitelmaan sisällytettävistä selvityksistä ja vaatimuksista.

Määräyksessä kuvataan omavalvontasuunnitelmaan vähintään sisällytettävät selvitykset ja vaatimukset. Omavalvontasuunnitelman laatiminen ja suunnitelman mukainen toiminta korvaa myös Kanta-palveluiden käyttöönoton yhteydessä tehdyt itseauditoinnit.

Omavalvonnan kohteen velvollisuutena on seurata ja toimia jatkuvasti suunnitelman mukaisesti. Kyse ei ole pelkästään valtakunnallisten tietojärjestelmäpalveluiden (Kanta-palvelut) käyttöönottovaiheessa tehtävistä toimenpiteistä vaan jatkuvasta riittävän tietoturvan ja asianmukaisten käytäntöjen varmistamisesta.

Omavalvontasuunnitelmien avulla vahvistetaan sosiaali- ja terveydenhuollon toimijoiden tietoturvakäytäntöjä. Niiden avulla varmistutaan, että kaikki asiakas- ja potilastietojen käsittelyyn osallistuvat palvelujen antajat ja muut tahot huolehtivat riittävästä henkilöstön osaamisesta, koulutuksesta ja käytön seurannasta sekä tietojärjestelmien vaatimustenmukaisuudesta.

2. Vastuut tietoturvan sekä asiakas- ja potilastietojen asianmukaisen käsittelyn varmistamisessa

Tietoturvan ja tietosuojan toteutumisen varmistaminen on kaikkien sosiaali- ja terveydenhuollon palveluiden tuottamiseen ja tietojärjestelmäratkaisujen toteutukseen liittyvien osapuolten tehtävä. Palvelujen antajan tulee varmistaa, että omavalvontasuunnitelma toteutuu kaikissa sen palveluyksiköissä ja muiden palveluiden tuottamiseen osallistuvien tahojen toiminnassa.

Kaikkien asiakas- ja potilastietojen käsittelyn osapuolien vastuut tulee olla selkeästi määritelty toiminnallisuuden, tietoturvallisuuden ja yhteistoiminnallisuuden osalta. Tietoturvallisuuden osalta vastuut määritellään osapuolten välisissä toimeksianto- tai muissa sopimuksissa.

Osa kuvatuista tai vaadituista asioista voi olla jonkun muun kuin omavalvonnan kohteen itsensä vastuulla erilaisten järjestelyjen (esimerkiksi palveluhankinta, yhtymä, sovellusvuokraus) kautta. Myös tällöin on kuvattava ja pystyttävä tarvittaessa todentamaan, kenen vastuulle asian kuvaaminen tai toteuttaminen kuuluu ja miten on varmistuttu siitä, että asia on kuvattu tai toteutettu vaaditulla tavalla.

Omavalvonnan kohde vastaa omavalvontasuunnitelmasta myös tilanteissa, joissa se hankkii käyttöympäristön tai tietotekniikkapalveluita esimerkiksi ostopalveluina muilta palveluiden antajilta tai tietojärjestelmäpalvelujen tuottajilta.

Viestinvälityksen / tietoliikenteen tietosuojaa koskevat vaatimukset ja vastuiden määrittely tulee olla osa palvelujen antajan ja viestinvälitysoperaattorin välistä sopimusta.

Mikäli viestinvälitys tai tietoliikenne on ulkoistettu ei-suomalaiselle yritykselle, tulee sen toteuttamisessa ja ulkoistettujen palvelujen toteuttamisessa noudattaa Suomen lainsäädäntöä. Mikäli viestinvälityksen tai tietoliikenteen toteutuksessa käytetään teknisiä tuotteita tai palveluita muilta kuin suomalaisilta valmistajilta tai palvelun tuottajilta, tulee varmistaa ettei toisen maan viranomaisille synny mahdollisuutta päästä käsiksi viestintään tai sen tietoihin.

Organisaatiolla (kuten lääkäriasema) on oltava sopimus sen asiakas- tai potilastietojärjestelmiä käyttävien omien toimintayksiköiden ja mahdollisten ulkopuolisten ammatinharjoittajien tai palvelun antajien keskinäisten vastuiden osalta.

Selkeät tietoturvavastuut tulee ulottaa koskemaan myös alihankkijoita ja muita mahdollisia sopimuskumppaneita. Sopimuksista tulee myös ilmetä mihin toimiin osapuolet ryhtyvät jos tietoturvassa ilmenee puutteita, ongelma tai uhkaava vaara.

3. Määritelmät

Tässä määräyksessä tarkoitetaan:
- **Asiakastietolailla** ajantasaista sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annettua lakia (159/2007);
- **Lääkemääräyslailla** ajantasaista sähköisestä lääkemääräyksestä annettua lakia (61/2007);
- **Palvelun antajalla**

  - terveydenhuollon toimintayksikköä (potilaslaki 785/1992 2 §:n 4 mom.)[3]
  - työantajaa (työterveyshuoltolaki 1383/2001 7 §:n 2 mom.)[4]
  - itsenäisenä ammatinharjoittajana toimivaa terveydenhuollon ammattihenkilöä (asiakastietolaki 3 §; 28.3.2014/250)
  - sosiaalihuollon palvelujen antajalla asiakaslain 812/2000 3 §:n 2 momentissa[5] tarkoitettua sosiaalihuoltoa järjestävää viranomaista, julkista sosiaalipalvelujen tuottajaa sekä yksityisistä sosiaalipalveluista annetussa laissa (922/2011)[6] tarkoitettua palvelujen tuottajaa; (28.3.2014/250)
  - apteekkia;
- **Tietojärjestelmällä** ohjelmistoa (mukaan lukien dokumentaatio sekä asennus- ja konfigurointiohjeet sekä ohjelmiston osat kuten asiakas- tai palvelinohjelmistot, sovelluspalvelut tai sovelluspalvelimet ja tietokannat), jonka käyttötarkoituksena on asiakas- tai potilastietojen käsittely;
- **Tietojärjestelmäpalvelulla** palvelua, jonka kautta palvelujen antaja käsittelee asiakas- ja potilastietoja, riippumatta siitä onko palveluun kuuluvat ohjelmistot asennettu kokonaan tai osittain palvelujen antajan tai tietojärjestelmäpalvelun tuottajan hallitsemaan käyttöympäristöön;
- **Tietojärjestelmän valmistajalla** tahoa, joka on vastuussa sosiaali- ja terveydenhuollon tietojärjestelmän suunnittelusta ja valmistuksesta, riippumatta siitä toimiiko tämä taho myös tietojärjestelmäpalvelun tuottajana;
- **Käyttöympäristöllä** teknistä, organisatorista ja fyysistä ympäristöä, jossa yksi tai useampi palvelun antaja käyttää tietojärjestelmää tai tietojärjestelmäpalvelua sotepalvelujen tuottamisessa ja todellisten asiakas- tai potilastietojen käsittelyssä;
  - käyttöympäristö sisältää mm. päätelaitteet, palvelimet, työasemat, käyttöjärjestelmä- ja varusohjelmistot sekä hallinta- ja tietoturvakäytännöt, jotka eivät ole osa tietojärjestelmää tai tietojärjestelmäpalvelua;
- **Tietojärjestelmäpalvelun tuottajalla** tahoa, joka tarjoaa palvelun antajalle tietojärjestelmäpalvelua, jossa käsitellään asiakas- ja potilastietoja, ja joka vastaa tietojärjestelmän valmistajalle asetettuihin vaatimuksiin valmistajana, valmistajan lukuun tai valmistajan puolesta;
- **Kanta-palveluilla** ja **valtakunnallisilla tietojärjestelmäpalveluilla** sähköisen lääkemääräyksen, Reseptikeskuksen, Lääketietokannan, Potilastiedon arkiston ja tiedonhallintopalvelun sekä Omakanta-palvelun muodostamaa kokonaisuutta;
- **Kanta-välityspalvelulla** sosiaali- ja terveydenhuollon organisaation tai apteekin Kanta-palveluihin liittymisessä hyödyntämää palvelua, jonka tuottajalla on tässä roolissa mahdollisuus nähdä salaamattomia potilas- tai asiakastietoja esimerkiksi ylläpitotoimien yhteydessä;
- **Kanta-välityspalveluiden tuottajalla** edellä kuvatun välityspalvelun tuottajaa;

[3] Laki potilaan asemasta ja oikeuksista https://www.finlex.fi/fi/laki/ajantasa/1992/19920785
[4] Työterveyshuoltolaki https://www.finlex.fi/fi/laki/ajantasa/2001/20011383
[5] Laki sosiaalihuollon asiakkaan asemasta ja oikeuksista http://www.finlex.fi/fi/laki/alkup/2000/20000812
[6] Laki yksityisistä sosiaalipalveluista http://www.finlex.fi/fi/laki/alkup/2011/20110922

- **Tietoturvallisuuden arviointilaitoksella** sellaista yritystä, yhteisöä tai viranomaista, jonka Viestintävirasto on hyväksynyt tietoturvallisuuden arviointilaitoksista annetun lain (1405/2011)[7] perusteella suorittamaan tietojärjestelmien vaatimustenmukaisuuden arviointeja;
- **Valvontaviranomaisella** sosiaali- ja terveysalan lupa- ja valvontavirastoa (Valvira) sekä aluehallintovirastoja (AVI);
- **Sertifioinnilla** vaatimustenmukaisuuden osoittamisen prosessia, jonka tuloksena täytetään ne edellytykset, joilla tietojärjestelmä tai tietojärjestelmäpalvelu voi saada vaatimustenmukaisuustodistuksen ja merkinnän valvontaviranomaisen rekisteriin vaatimukset täyttävästä tietojärjestelmästä tai tietojärjestelmäpalvelusta
    - Kanta-palveluihin liitettäviltä (luokkaan A kuuluvilta) tietojärjestelmiltä tai tietojärjestelmäpalveluilta edellytetään selvitystä toiminnallisuutta koskevien vaatimusten täyttämisestä, hyväksyttyä Kelan yhteistestausta ja pakollisten tietoturvallisuuden vaatimusten täyttämisen auditointia;
- **Auditoinnilla** sertifiointiprosessin osaa, jossa hyväksytty tietoturvallisuuden arviointilaitos suorittaa vaatimusten osa-alueen (kuten tietoturvavaatimukset) läpikäynnin tuottaen auditointiraportin ja auditointitodistuksen;
- **Vaatimustenmukaisuustodistuksella** hyväksytyn auditointilaitoksen antamaa todistusta siitä, että tietojärjestelmä tai tietojärjestelmäpalvelu on hyväksytysti läpäissyt sertifioinnin.

Lisäksi tässä määräyksessä käytetään ministeriöistä, virastoista ja laitoksista seuraavia lyhenteitä:

- STM (sosiaali- ja terveysministeriö);
- THL (Terveyden ja hyvinvoinnin laitos);
- Valvira (Sosiaali- ja terveysalan lupa- ja valvontavirasto);
- Kela (Kansaneläkelaitos).

4. Suhde muihin ohjaaviin määräyksiin ja ohjeisiin

Tämän määräyksen lisäksi omavalvontasuunnitelman laatimisessa voidaan hyödyntää seuraavia ohjeita:

- Aiemmin annetut ohjeet auditoinnista (Kanta-palveluihin liittyminen, Sähköisen lääkemääräyksen ja Potilastiedon arkiston käyttöönotto, Terveydenhuollon organisaation auditointivaatimusten läpikäynti)[8]
- Määräys A-luokkaan kuuluvien sosiaali- ja terveydenhuollon tietojärjestelmien olennaisista tietoturvavaatimuksista[9]

[7] Laki tietoturvallisuuden arviointilaitoksista http://www.finlex.fi/fi/laki/alkup/2011/20111405
[8] Käyttöönoton käsikirjat http://www.kanta.fi/web/ammattilaisille/kayttoonoton-kasikirjat

- Erikseen tarvittaessa annettavat ohjeet omavalvonnan kohteille kuten itsenäisille ammatinharjoittajille auditointivaatimusten ja omavalvonnan soveltamisesta

5. Yleistä

Asiakastietolain 19 h §:n mukaisesti palvelujen antajan on laadittava tietoturvaan ja tietosuojaan sekä tietojärjestelmien käyttöön liittyvä omavalvontasuunnitelma. Omavalvontasuunnitelman tarkoituksena on varmistaa, että palvelujen antajan henkilökunta hallitsee käytössään olevien tietojärjestelmien käytön ja ottaa huomioon asiakas- ja potilastietojen salassapitoon ja tietoturvaan liittyvät vaatimukset ja ymmärtää väärinkäyttöön liittyvät seuraamukset. Omavalvontasuunnitelman avulla varmistetaan myös siitä, että asiakas- ja potilastiedon käsittelyssä otetaan huomioon tarvittavat tietosuoja- ja tietoturvaseikat omavalvonnan kohteen toiminnassa ja tietojärjestelmien käyttöympäristössä. Valtakunnallisten tietojärjestelmäpalvelujen käytön osalta omavalvontasuunnitelmassa on selvitettävä myös niihin liittyvät tietosuojan ja tietoturvan erityiskysymykset.

Omavalvontasuunnitelmia koskevia säännöksiä on myös terveydenhuoltolaissa (1326/2010)[10], yksityisestä terveydenhuollosta annetussa laissa (152/1990)[11] ja yksityisestä sosiaalihuollosta annetussa laissa (922/2011)[12]. Tämän määräyksen mukainen omavalvontasuunnitelma voidaan tarvittaessa yhdistää muihin mahdollisiin omavalvontasuunnitelmiin sekä tietoturva- ja toimintaohjeisiin.

Omavalvonnassa kuvatut asiat on voitava tarpeen mukaan todentaa omavalvonnan toteutumisen tarkastusta suorittavalle valvontaviranomaiselle. Todentaminen koskee myös kohdan 2 mukaisia järjestelyitä.

Kuvaukset voivat olla tarvittaessa tietojärjestelmäkohtaisia tai yhteisiä useille omavalvonnan kohteille. Kuvausten ei tarvitse sisältyä omavalvontasuunnitelmaan, vaan suunnitelmassa voidaan viitata erillisiin saatavilla oleviin kuvauksiin, kuten omavalvonnan kohteen tietoturvaohjeisiin tai tietojärjestelmäsalkun kuvauksiin.

Tietojärjestelmäpalvelun tuottajan, joka tarjoaa tietojärjestelmiä omavalvonnan kohteelle, on toteutettava tietojärjestelmää koskevat olennaiset vaatimukset. Näiden vaatimusten täyttymisestä on huolehdittava osana omavalvontaa ja ne on otettava huomioitava esimerkiksi hankinnoissa ja sopimuksissa.

[9] Määräys 1/2015 THL/1305/4.09.00/2014 ja sertifiointi-sivut: http://www.kanta.fi/web/ammattilaisille/sertifiointi
[10] Terveydenhuoltolaki https://www.finlex.fi/fi/laki/ajantasa/2010/20101326
[11] Laki yksityisestä terveydenhuollosta http://www.finlex.fi/fi/laki/alkup/1990/19900152
[12] Laki yksityisistä sosiaalipalveluista http://www.finlex.fi/fi/laki/alkup/2011/20110922

Kanta-palveluihin liittyvien (luokkaan A kuuluvien) tietojärjestelmien ja tietojärjestelmäpalveluiden sertifioinnissa niille suoritetaan Kanta-yhteistestaus ja tietoturva-auditointi. Sertifioinnista vastaa kunkin järjestelmän valmistaja tai tietojärjestelmäpalvelun tuottaja. Tietoturva-auditoinnin suorittaa hyväksytty tietoturvallisuuden auditointilaitos. Hyväksytyn sertifioinnin tuloksena Kanta-palveluihin liittyvä tietojärjestelmä saa vaatimustenmukaisuustodistuksen ja merkinnän Valviran rekisteriin A-luokkaan kuuluvasta tietojärjestelmästä. Sertifiointi ei kuitenkaan kata kaikkia järjestelmän käyttöön liittyviä seikkoja eri käyttöympäristöissä tapahtuvassa sosisaali- ja terveyspalveluiden tuottamisessa. Omavalvontasuunnitelmat koskevat käyttöympäristöjä, joista omavalvonnan kohteet vastaavat.

Valvira ylläpitää myös rekisteriä luokkaan B kuuluvista tietojärjestelmistä, jotka sen saamien ilmoitusten perusteella täyttävät käyttötarkoituksensa mukaiset olennaiset vaatimukset. Tietojärjestelmäpalvelun tuottajan on ilmoitettava rekisteriä varten asiakas- tai potilastietojen käsittelyyn tuotantokäyttöön otettavasta tietojärjestelmästä. Omavalvontasuunnitelman on katettava myös nämä tietojärjestelmät. Omavalvontasuunnitelman ei tarvitse kattaa omavalvonnan kohteessa käytettäviä sovellusohjelmistoja tai tietojärjestelmiä, joiden käyttötarkoituksena ei ole asiakas- tai potilastietojen käsittely.

6. Omavalvontasuunnitelmaan sisällytettävät selvitykset ja vaatimukset

6.1. Tietojärjestelmien käyttäjiltä vaadittava koulutus ja kokemus

Omavalvontasuunnitelmaan on sisällytettävä selvitys siitä, kuinka tietojärjestelmiä käyttä-ville henkilöille varmistetaan järjestelmien käytön vaatima koulutus ja kokemus. Henki-löillä on oltava koulutusta tietojärjestelmien käytön lisäksi mm. potilastietojen käsitte-lyyn sekä tietosuoja- ja tietoturva-asioihin. Koulutuksen määrän ja sisällön on oltava tarkoituksenmukainen henkilön tai henkilöstöryhmän työ- ja tietojenkäsittelytehtävien kannalta.

Palvelujen antajalla on oltava koulutussuunnitelma ja toimintamalli perehdyttämiseen, koulutukseen ja niiden seurantaan. Koulutussuunnitelmassa on kuvattava vaadittavan koulutuksen sisältö ja toteuttamistavat. Tietojärjestelmän käyttäjiltä vaadittava koulutus voidaan todentaa joko todistuksilla tai merkinnöillä koulutuksiin osallistumisesta tai muulla organisaatiossa sovitulla tavalla.

Lain mukaan tietojärjestelmien käyttäjillä on oltava myös niiden käytön vaatima kokemus. Kokemuksen varmistamisen palvelujen antaja voi toteuttaa toistuvalla osaamisen seurannalla tai seuraamalla järjestelmiä käyttävien henkilöiden kokemusta tietojärjestelmien käytöstä. Niille työntekijöille, joilla on vähäinen kokemus käytössä ole-

vasta tietojärjestelmästä, tai uusien tietojärjestelmien tullessa käyttöön tulee järjestää riittävä perehdytys ja tarvittaessa ohjausta tietojärjestelmän käyttöön.

6.2. Tietojärjestelmien asianmukaisen käytön kannalta tarpeelliset käyttöohjeet

Omavalvontasuunnitelmassa on selvitettävä miten on varmistettu, että tietojärjestelmän käyttäjällä on saatavilla tarpeelliset käyttöohjeet vähintään sillä kielellä, jonka osaaminen on vähimmäisvaatimus työtehtävässä toimimiselle. Kirjalliset ohjeet asiakas- ja potilastietojen käsittelystä tulee olla annettu niitä käsitteleville työntekijöille. Tämä osoitetaan ymmärrettävillä, yksiselitteisillä ja tietojärjestelmän käytössä olevaa versiota vastaavilla käyttöohjeilla ja muilla tarvittavilla ohjeilla sekä selvittämällä, miten ohjeet ovat käyttäjien saatavilla (jakelukanavat). Lisäksi on oltava kuvattuna toimintamalli, miten käyttöohjeiden päivittäminen ja jakelu toteutetaan ohjelmistojen versiopäivitysten sekä muiden muutosten yhteydessä.

6.3. Tietojärjestelmien käyttö valmistajan antaman ohjeistuksen mukaisesti

Omavalvontasuunnitelmassa on kuvattava, miten varmistetaan se, että tietojärjestelmiä käytetään valmistajan antaman ohjeistuksen mukaisesti tai ohjeistusta tarkoituksenmukaisesti käyttöympäristöön soveltaen. Omavalvontasuunnitelmassa kuvataan mistä löytyvät tietojärjestelmien valmistajien antamat ohjeistukset ja tiedot koulutuksista sekä palvelujen antajan omat menettelytavat, joilla seurataan valmistajien antamien ohjeistusten mukaista käyttöä tai täydennetään ohjeistuksia.

6.4. Menettelytavat virhe- ja ongelmatilanteissa

Virhe-, ongelma- ja erityistilanteiden varalta palvelujen antajalla tulee olla selkeät menettelytavat, ohjeet ja vastuut tällaisten tilanteiden havainnointiin, tiedottamiseen, korjaamiseen ja jälkihoitoon. Lisäksi on kuvattava, kuinka varmistetaan ohjeiden saatavuus poikkeustilanteesta huolimatta silloin, kun niitä tarvitaan.

Omavalvontasuunnitelmassa kuvataan, millaisia tukipalveluja on saatavissa järjestelmien käytön tueksi ja kuinka käyttäjät saavuttavat nämä tukipalvelut.

6.5. Tietojärjestelmien asennus, ylläpito ja päivitys

Omavalvonnan kohteen on selvitettävä omavalvontasuunnitelmassa, miten on varmistettu, että tietojärjestelmiä ylläpidetään ja päivitetään valmistajan ohjeiden mukaisesti. Vastaavasti omavalvontasuunnitelmassa on selvitettävä, miten on varmistettu, että tietojärjestelmiä asentaa, ylläpitää ja päivittää henkilöstö, jolla on siihen tarvittava ammattitaito ja asiantuntemus.

Edellä mainitut tietojärjestelmien asennukseen, ylläpitoon ja päivitykseen liittyvät seikat voidaan osoittaa suunnitelmalla, joka sisältää kuvaukset päivitys-, muutoksenhallinta- ja korjausprosesseista sekä virhe- ja poikkeustilanteisiin liittyvistä menettelytavoista. Päivitysprosessin kuvaamisessa on otettava huomioon mm. versio- ja korjauspäivitykset sekä muiden muutosten mahdollisesti vaatimat menettelyt. Muutoksenhallintaprosessissa voidaan kuvata mm. järjestelmien muutosten ja uusien versioiden testaus- ja hyväksymismenettelyt. Asennus-, päivitys- ja ylläpitotoimenpiteiden ongelma- ja virhetilanteiden hallinta on osa suunnitelmaa.

Lisäksi on kuvattava tietojärjestelmiä asentavan, ylläpitävän ja päivittävän henkilön rooli ja vastuut suhteessa omavalvonnan kohteeseen sekä tietojärjestelmäpalvelun tuottajaan.

Omavalvontasuunnitelmassa on soveltuvin osin kuvattava, miten tietojärjestelmien ylläpidossa ja käyttöympäristössä on otettu huomioon tai kuvattu myös seuraavat seikat:

- Mitä palveluita ja mitä sovelluksia tietojärjestelmissä on ja kuka vastaa niiden asentamisesta ja ylläpidosta.
- Kuinka estetään se, että tietojärjestelmissä olisi aktiivisia oletustunnuksia tai muita oletuksena tulevia tietoturvallisuuden kannalta huonoja asetuksia.
- Kuinka ne palvelimet, joilla tietojärjestelmät toimivat suojataan haittaohjelmilta, ja millainen on haittaohjelmien torjunnassa olevien ohjelmien päivityskäytäntö.
- Kuinka palvelimien tietoturvapäivitysten asentaminen on kuvattu ja järjestetty, ja miten päivitysten kriittisyys ja tarve arvioidaan sekä päivitykset hyväksymistestataan mahdollisuuksien mukaan erillisessä ympäristössä ennen tuotantoympäristöön asentamista.
- Kuinka tietojärjestelmät soveltuvin osin suojataan tyypillisimmiltä tietoturvapuutteilta ja www-sovellusten haavoittuvuuksilta (esim. OWASP top 10).

6.6. Tietojärjestelmien käyttöympäristö

Omavalvontasuunnitelmassa on kuvattava, miten tietojärjestelmän asianmukainen sekä riittävän tietoturvallinen käyttö varmistetaan omavalvonnan kohteen käyttöympäristössä.

Omavalvonnan kohteen on määriteltävä noudattamansa tietoturvapolitiikka, josta ilmenee miten sitä tarkastetaan ja kehitetään, miten tietoturva on vastuutettu ja organisoitu toiminnan tavoitteiden saavuttamiseksi, riskien hallitsemiseksi ja kansallisten vaatimusten mukaisesti.

Omavalvonnan kohteella on nimetty tietosuojavastaava, joka toimii tietosuoja-asioiden asiantuntijana. Tietosuojavastaavalla on oltava selkeä, dokumentoitu tehtäväkuva sekä riittävät resurssit hoitaa tehtävää.

Tietoturvan ja tietosuojan seuranta ja valvonta

Omavalvonnan kohteella on oltava laadittuna tietosuojaan liittyvä seuranta- ja valvontasuunnitelma, jossa otetaan kantaa esimerkiksi miten tehdään säännöllistä henkilötietojen käytön seurantaa ja miten toimitaan, jos väärinkäytöksiä ilmenee. Nämä seikat voivat olla osa omavalvontasuunnitelmaa tai erillisiä dokumentteja.

Sosiaali- ja terveydenhuollon palvelujen antajan on omalta osaltaan seurattava ja valvottava, että potilastietojärjestelmässä, Potilastiedon arkistossa ja Reseptikeskuksessa olevia tietoja voivat katsella ja käsitellä vain siihen oikeutetut henkilöt. Vastaava koskee soveltuvin osin myös sosiaalihuollon palvelun antajia. Järjestelmät estävät ei-sallitun käytön silloin, kun se on teknisesti mahdollista, ja omavalvonnan kohteen omat ohjeet ja toimintatavat ohjaavat oikeaan toimintaan ja käsittelyyn.

Omavalvonnan kohteella on oltava määritellyt toimintatavat tietoturvapoikkeamien havainnointiin ja eskalointiin (incident management) ja tietojärjestelmien käytön seurantaan (esimerkiksi lokien analysointikäytäntö).

Lokitietojen luomisen ja käsittelyn prosessin tulee taata riittävällä tasolla, että tarpeelliset lokit syntyvät ja pysyvät muuttumattomina ja todistusvoimaisina. Soveltuvin osin voidaan hyödyntää esimerkiksi valtionhallinnon tietoturvallisuuden johtoryhmän ohjetta VAHTI 3/2009 "Lokiohje".

Käyttövaltuushallinta ja tunnistautuminen järjestelmiin

Omavalvontasuunnitelmassa tulee kuvata käyttövaltuuksien hallintakäytännöt. Käytännössä on kuvattava esimerkiksi, hallinnoidaanko käyttövaltuuksia asiakas- tai potilastietojärjestelmän vai ulkoisen tietojärjestelmän (kuten IAM-järjestelmä) avulla. Kantapalvelujen osalta omavalvonnan kohteessa tulee hallinnoida huolellisesti tietojärjestelmän käyttäjien oikeuksia käyttää sähköiseen lääkemääräykseen, valtakunnalliseen Potilastiedon arkistoon ja muuhun potilastietojen käsittelyyn liittyviä toimintoja ja Reseptikeskuksen tietoja. Käyttöoikeuksista ja niihin tehdyistä muutoksista tulee pitää kirjaa / lokia.

Omavalvonnan kohteessa käytettävästä tietojärjestelmästä tulee olla laadittuna dokumentoidut käyttöoikeuskuvaukset rajauksineen. Käyttöoikeuksien myöntäminen ja käyttöoikeuksien hallintaprosessi voi perustua esimerkiksi roolipohjaisiin käyttöoikeuksiin. Poikkeamat roolikohtaisista oikeuksista tulee tällöin asianmukaisesti hyväksyä ja

dokumentoida. Omavalvontasuunnitelmassa on kuvattava, kuinka dokumentoidaan henkilöt ja roolit, joilla on oikeus hyväksyä käyttöoikeuspyyntöjä.

Käyttövaltuuksien hallintakäytönnöissä on otettava huomioon seuraavat seikat:

- Kanta-palveluihin liittyvissä järjestelmissä ei saa olla yhteiskäyttöisiä tunnuksia asiakas- tai potilastietojen muokkaamiseen, katseluun tai sähköiseen reseptiin liittyvien toiminnallisuuksien osalta. Vaatimus koskee myös ylläpito- ja muita vastaavia voimakkaita käyttöoikeuksia.
- Pääkäyttäjillä ja tietojärjestelmäasiantuntijoilla ei ole oikeutta Kanta-palveluissa olevien tietojen käsittelyyn (kuten luovutushaku ja asiakirjan hakeminen omaan käyttöön) paitsi virhetilanteiden selvityksissä, jolloin on oikeus tarkistaa oman organisaationsa tai sen organisaation, jonka lukuun tietojärjestelmäasiantuntijat selvityksen aikana toimivat, tietoja potilastiedon arkistosta. Kanta-oikeudet rajataan edellä mainituissa virhetilanneselvityksissä ainoastaan omien tietojen hakuun. Kaikki selvityksessä tehdyt haut tulee näkyä lokeista.

Kanta-palveluihin liittyvissä tietojärjestelmissä tulee sallia kirjautuminen sähköiseen reseptiin ja valtakunnalliseen Potilastiedon arkistoon liittyviin toiminnallisuuksiin ainoastaan vahvaa tunnistusmekanismia käyttäen tai poikkeustapauksessa vahvaa salasanaa käyttäen. Salasanalla tunnistautuessa voi käyttää ainoastaan omavalvonnan kohteen omia asiakas- tai potilastietoja.

Tekniset vaatimukset

Kanta-palveluihin liittyvissä tietojärjestelmissä käytettävien tietoliikenneyhteyksien tietoturva tulee olla toteutettu omavalvonnan kohteen käyttämän tietoturvapolitiikan mukaisesti ja siten, että Kelan "Kanta-tietoliikenteen tietoturva"-ohjeen (esimerkiksi hyväksyttävä TSL-toteutus ja salauksen taso) ja omavalvonnan kohteen oman tietoturvapolitiikan vaatimukset toteutuvat.

Omavalvonnan kohteen tietojärjestelmien tulee tukea hyvien käytäntöjen mukaista salausavainten ja sertifikaattien hallintaa, jonka tulee kattaa avainten / sertifikaattien a) luonti (tai siirto järjestelmään), b) säilytys, c) käyttö, sekä d) tuhoaminen / arkistointi / poisto.

Kanta-palveluihin liittyvän omavalvonnan kohteen käyttämien tietojärjestelmien tulee olla palomuurilla suojatut. Kyseeseen voi tulla joko tilallinen palomuuri tai erilliset sovelluspalomuurit. Mikäli omavalvonnan kohteella on useita yhteyksiä Reseptikeskukseen tai Potilastiedon arkistoon, riittää kun ne ovat saman palomuurin takana.

Mikäli Kanta-palveluun liittyvään tietojärjestelmään ylläpidollisista tai muista syistä sallitaan etäyhteyksiä, yhteydet tietojärjestelmään tulee olla toteutettu turvallisesti.

Yllä lueteltujen teknisten vaatimusten toteuttamistapa on kuvattava omavalvonta-suunnitelmassa ja oltava todennettavissa valvontatilanteessa.

Fyysisten tilojen, laitteiden ja tulosteiden turvallisuus

Omavalvonnan kohteen on kiinnitettävä huomiota tietosuojan ja tietoturvan takaavaan fyysiseen käyttöympäristöön, kuten toimitiloihin ja niiden sijoittelu-, sisustus-, ääni-eristys- tai muihin vastaaviin toimenpiteisiin, sekä mm. näyttöjen ja tulostimien sijoitteluun ja suojaamiseen sivullisilta. Omavalvontasuunnitelmassa kuvataan, kuinka nämä seikat on otettu huomioon. Lisäksi on kuvattava, kuinka työasemien suojaus sivullisilta on toteutettu.

Omavalvontasuunnitelmassa on kuvattava, miten omavalvonnan kohteen mahdollisesti käytössä olevien liikuteltavien asiakas- tai potilastietoja sisältävien laitteiden tietosuojasta ja tietoturvasta on huolehdittu ja miten se on todennettavissa.

Tietojärjestelmistä paperille tulostettavien asiakas- ja potilastietojen asianmukaisesta säilyttämisestä ja hävittämisestä tulee olla kuvattuna menettelytavat joilla estetään se, että sivulliset saisivat omavalvonnan kohteelta haltuunsa asiakas- tai potilastietoja.

Työasemien turvallisuus

Omavalvonnan kohteen on huolehdittava, että tietosuojan toteuttamisessa on otettu huomioon työaseman tai potilas- tai asiakastietojärjestelmän käyttöliittymän lukittuminen, kun käyttäjä ei käytä sitä aktiivisesti enintään 30 minuutin kuluessa. Viimeistään 30 minuutin jälkeen käyttäjän pitää kirjautua tai tunnistautua (esimerkiksi antaa PIN-koodi) uudelleen käyttöliittymän avaamiseksi. Mikäli aikakatkaisun raja on pidempi kuin 30 minuuttia, omavalvontasuunnitelmassa tulee perustella tai kuvata mistä perustelut aikarajan ylitykselle löytyvät.

6.6. Asiakas- ja potilastietojärjestelmät, niihin liitetyt tietojärjestelmät ja muut tietojärjestelmät

Omavalvonnan kohteen on yksilöitävä omavalvontasuunnitelmassa tai kuvattava, missä on tieto seuraavantyyppisistä tietojärjestelmistä ja niiden versioista joita omavalvonnan kohteen toiminnassa käytetään:

- suoraan Kanta-palveluihin liitettävät luokkaan A kuuluvat tietojärjestelmät
- asiakas- tai potilastietoja käsittelevät luokkaan B kuuluvat tietojärjestelmät
- muut tietojärjestelmät, joilla on vaikutusta ja jotka on otettava huomioon kohdassa 6.5 kuvatuissa asennuksissa, ylläpidossa ja päivityksissä arkaluonteisten asiakas- ja potilastietojen suojaamisen kannalta.

Omavalvonnan kohteen on selvitettävä omavalvontasuunnitelmassa, miten on varmistettu se, että Kanta-palveluihin liittyviin tietojärjestelmiin liitetyt tai käyttöympäristössä hyödynnettävät muut sovellukset tai tietojärjestelmät eivät vaaranna tietojärjestelmien suorituskykyä eivätkä niiden tietoturva- tai tietosuojaominaisuuksia. Muilla tietojärjestelmillä tarkoitetaan mm. tietokoneohjelmia, jotka eivät käsittele asiakas- ja potilastietoja, eivätkä siten ole asiakastietolain 19 b §:n mukaisia luokan A tai B tietojärjestelmiä.

6.7. Valtakunnallisiin tietojärjestelmäpalveluihin liittyminen

Jos omavalvonnan kohde on liittynyt Kanta-palveluiden käyttäjäksi, on omavalvontasuunnitelmassa selvitettävä, miten valtakunnallisten tietojärjestelmäpalveluiden tietoturvallisen käytön edellyttämät vaatimukset varmistetaan. Valtakunnallisten tietojärjestelmäpalveluiden käyttö edellyttää erityistä seurantaa ja valvontaa, koska niihin on tallennettu muiden palvelun antajien laatimia asiakas- ja potilastietoja. Tietovaranto on myös jatkuvasti kasvava ja sisältää suuren määrän arkaluonteisia salassa pidettäviä asiakas- ja potilastietoja.

Palvelujen antajan on huolehdittava siitä, että henkilöstö hallitsee Kanta-palveluiden käyttöön liittyvät toimintamallit ja periaatteet sekä tietää väärinkäytösten seuraamukset. Omavalvontasuunnitelmassa on selvitettävä, miten potilaiden informointi Kanta-palveluista ja tietojen käytöstä tapahtuu ja on palvelujen antajan todennettavissa. Lisäksi on kuvattava miten Kanta-palveluiden käyttö on otettu huomioon henkilöstön koulutusmateriaaleissa, koulutuksissa ja ohjeistuksissa.

Virhe-, ongelma- ja erityistilanteiden varalta omavalvonnan kohteella tulee olla selkeät menettelytavat ja vastuut tällaisten tilanteiden havainnointiin, tiedottamiseen, korjaamiseen ja jälkihoitoon.

Kohdan 6.4 mukaisissa häiriö- ja erityistilanteiden toimintaohjeissa on otettava huomioon Kanta-palvelut. Vastuutahot häiriötilanteiden ilmoittamisesta myös Kanta-palveluiden tekniseen tukeen on oltava todennettavissa. Palvelujen antajan on ilmoitettava Kelalle sen antamien ohjeiden mukaisesti muutoksista sen käyttämissä tietojärjestelmäversioissa.

Omavalvonnan kohteella on oltava kuvaus toimintamallista, jonka mukaisesti se seuraa aktiivisesti Kanta-palveluiden käyttöä. Osana toimintamallia on kuvattava, miten seurataan asiakirjojen arkistoitumista asianmukaisesti ja Kanta-palvelujen lähettämiä virheilmoituksia.

Omavalvonnan kohteen on kuvattava, kuinka Kanta-palveluista haettujen asiakas- tai potilastietojen käyttöä seurataan. Tämä koskee erityisesti ns. hätätilahaun käyttöä, erityissuojattavien tietojen hakua ja käyttöä sekä ilman teknistä hoitosuhteen varmis-

tusta (ns. erityinen syy) tehtyjä hakuja. Henkilöstön on oltava tietoisia seurannasta ja väärinkäytön seuraamuksista.

Omavalvonnan kohteen on varmistettava, että Kanta-palveluihin arkistoidaan ainoastaan sosiaali- ja terveydenhuollon rekistereihin kuuluvia potilas- ja asiakasasiakirjoja.

Edellä kuvatut seikat tulee olla tarvittaessa todennettavissa valvontatilanteessa.

7. Ohjaus ja neuvonta

Terveyden ja hyvinvoinnin laitoksen operatiivisen toiminnan ohjaus -yksikkö (OPER) ohjaa ja neuvoo pyynnöstä tämän määräyksen soveltamisessa ja ylläpitää mallipohjia omavalvontasuunnitelmasta sekä selvityksistä, joiden avulla palvelujen antaja voi todentaa omavalvontasuunnitelman toteutumista. Mallipohjia ylläpidetään kanta.fi-verkkosivuilla Kanta-palveluiden käyttöönoton käsikirjoissa.

Lisätietoja:
http://www.kanta.fi/web/ammattilaisille/kayttoonoton-kasikirjat
http://www.kanta.fi/web/ammattilaisille/sertifiointi

8. Voimaantulo

Tämä määräys tulee voimaan 1.2.2015 ja on voimassa toistaiseksi.

Tietojohtaja Pekka Kahri

Yksikönpäällikkö Vesa Jormanainen

Jakelu

Sosiaalihuollon palvelujen antajat
Terveydenhuollon palvelujen antajat
Kanta-palveluiden välittäjänä toimivat välityspalveluiden tuottajat
Suomen Apteekkariliitto ry
Itä-Suomen yliopiston apteekki
Yliopiston apteekki
Kansaneläkelaitos

Tiedoksi

Sosiaali- ja terveysministeriö
Lääkealan turvallisuus- ja kehittämiskeskus
Sosiaali- ja terveysalan lupa- ja valvontavirasto
Väestörekisterikeskus
Aluehallintovirastot
Statens ämbetsverk på Åland
Suomen Kuntaliitto
Sosiaali- ja terveydenhuollon asiakas- ja potilastietojärjestelmien valmistajat
Apteekkien tietojärjestelmien valmistajat
Suomen Lääkäriliitto ry
Suomen Hammaslääkäriliitto ry
Lääkäripalveluyritykset ry
Terveyspalvelualan Liitto ry
Tietosuojavaltuutetun toimisto
Suomen Fysioterapia- ja kuntoutusyritykset FYSI ry
Suomen Optinen Toimiala
Suomen Työterveys ry
Kuntoutuksen Toimialayhdistys ry
Suomen lähi- ja perushoitajaliitto SuPer ry
Suomen Psykologiliitto ry
Suomen Puheterapeuttiliitto ry
Ravitsemusterapeuttien yhdistys ry
Suomen Terveydenhoitajaliitto ry
Suomen Suuhygienistiliitto SSHL ry
Suomen Hammasteknikkoseura ry
Erikoishammasteknikkoliitto ry
Suomen Toimintaterapeuttiliitto ry
Suomen Naprapaattiyhdistys ry
Suomen Osteopaattiliitto ry
Koulutettujen Hierojien Liitto
Suomen Jalkojenhoitaja- ja Jalkaterapeuttiliitto SJJL ry

Tehy ry
Suomen Bioanalyytikkoliitto ry
Suomen Ensihoitoalan liitto ry
Suomen Fysioterapeutit ry
Suomen Kätilöliitto ry
Suomen Lastenhoitoalan Liitto ry
Suomen Mielenterveyshoitoalan Liitto ry
Suomen Röntgenhoitajaliitto ry
Suomen Sairaanhoitajaliitto ry
Suun Terveydenhoidon Ammattiliitto STAL ry
Suomen Lähihoitajat ry

Liite1. Omavalvontasuunnitelman mallipohja