Tietopalvelut
Sote-tieto ja -tiedonhallinta

20.12.2021

MÄÄRÄYS TIETOTURVASUUNNITELMAAN SISÄLLYTETTÄVISTÄ SELVITYKSISTÄ JA VAATIMUKSISTA

Valtuutussäännökset

Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (784/2021) 27 § 3 momentti, Laki sähköisestä lääkemääräyksestä (61/2007) 22 b §

Kohderyhmät

Sosiaali- ja terveydenhuollon palvelunantajat
Apteekit
Välittäjät
Kansaneläkelaitos

Voimaantulo

Tämä määräys tulee voimaan 20. päivänä joulukuuta 2021 ja on voimassa toistaiseksi.

Tämä määräys kumoaa THL:n aiemmin antaman määräyksen THL 2/2015 Omavalvontasuunnitelmaan sisällytettävistä selvityksistä ja vaatimuksista. Aiempi määräys on annettu sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetun lain (159/2007) nojalla. Lailla sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (784/2021) on kumottu laki (159/2007).

Sisällys

1 Määräyksen soveltamisala ... 3
2 Vastuut tietoturvan sekä asiakastietojen asianmukaisen käsittelyn varmistamisessa ... 4
3 Määritelmät ... 4
4 Suhde THL:n muihin määräyksiin, yleisiin viitekehyksiin sekä eräisiin muihin säädöksiin ... 6
5 Yleistä tietoturvasuunnitelmasta ... 6
6 Tietoturvasuunnitelmaan sisällytettävät selvitykset ja vaatimukset ... 8
6.1 Yleiset tietoturvakäytännöt ... 8
6.2 Menettelyt virhe- ja ongelmatilanteissa sekä jatkuvuudenhallinta ... 9
6.3 Henkilöstön koulutus sekä osaamisen ylläpito ja kehittäminen ... 10
6.4 Tietojärjestelmien käyttöohjeet ja ohjeiden mukainen käyttö ... 10
6.5 Tietojärjestelmien perustiedot, kuvaukset ja olennaisten vaatimusten täyttyminen ... 11
6.6 Tietojärjestelmien asennus, ylläpito ja päivitys ... 12
6.7 Käyttövaltuuksien hallinnan ja tunnistautumisen käytännöt ... 13
6.8 Asiakas- ja potilastietojärjestelmien pääsynhallinnan ja käytön seurannan käytännöt ... 15
6.9 Fyysinen turvallisuus osana tietojärjestelmien käyttöympäristön turvallisuutta ... 16
6.10 Työasemien, mobiililaitteiden ja käyttöympäristön tukipalveluiden hallinta ... 16
6.11 Alusta- ja verkkopalvelujen tietoturvallinen käyttö tietosuojan ja varautumisen kannalta ... 17
6.12 Kanta-palvelujen liittymisen ja käytön tietoturvakäytännöt ... 18
7 Ohjaus ja neuvonta ... 19
8 Voimaantulo ... 19

1 Määräyksen soveltamisala

Tämä määräys perustuu sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetun lain (784/2021), jäljempänä *asiakastietolaki* 27 ja 28 §:ään sekä sähköisestä lääkemääräyksestä annetun lain (61/2007) 22 b §:ään sellaisena kuin se on laissa 786/2021.

Terveyden ja hyvinvoinnin laitokselle on annettu asiakastietolain 27 §:n 3 momentissa valtuutus antaa tarkempia määräyksiä 1 ja 2 momentissa tarkoitetuista tietoturvasuunnitelmaan sisällytettävistä selvityksistä ja niitä koskevista vaatimuksista.

Määräys tietoturvasuunnitelmaan sisällytettävistä selvityksistä ja vaatimuksista koskee niitä, jotka asiakastietolain mukaan ovat velvollisia laatimaan tietoturvasuunnitelman: sosiaali- ja terveydenhuollon palvelunantajia, apteekkeja, välittäjiä sekä Kansaneläkelaitosta. Näiden tahojen on laadittava tietoturvaan, tietosuojaan ja tietojärjestelmien käyttöön liittyvä tietoturvasuunnitelma.

Tietoturvasuunnitelman laatimiseen velvoitetuista tahoista käytetään tässä määräyksessä ja määräyksen liitteessä yleisnimeä tietoturvallisuuden omavalvonnan kohde tai omavalvonnan kohde.

Määräyksen pääkohderyhmä ovat palvelunantajat ja apteekit, joiden roolia määräyksen sisällössä korostetaan termillä "palvelunantaja". Määräyksen eri kohdat sinällään koskevat kaikkia omavalvonnan kohteita, joita palvelunantajien ja apteekkien lisäksi ovat myös välittäjät ja Kansaneläkelaitos.

Määräyksessä kuvataan tietoturvasuunnitelmaan vähintään sisällytettävät selvitykset ja vaatimukset.

Tietoturvan toteutumisen varmistaminen, tietosuojasääntelyn noudattaminen ja asiakastietojen käsittelyn asianmukaisuuden varmistaminen ovat kaikkien sosiaali- ja terveydenhuollon palveluiden tuottamiseen ja tietojärjestelmäratkaisujen toteutukseen osallistuvien osapuolten tehtäviä.

Tietoturvasuunnitelmien avulla vahvistetaan sosiaali- ja terveydenhuollon toimijoiden tietoturvallisuuskäytäntöjä. Palvelunantajien, apteekkien, välittäjien ja Kansaneläkelaitoksen laatimissa tietoturvasuunnitelmissa on oltava selvitykset siitä, miten sosiaalihuollon asiakastietojen ja potilastietojen käsittelyyn ja tietojärjestelmiin liittyvät vaatimukset varmistetaan asiakastietolain 27 §:n 1 momentin kohtien 1-9 mukaisesti. Vaatimus koskee kaikkia asiakastietojen käsittelyyn osallistuvia palvelunantajia, apteekkeja, välittäjiä ja Kansaneläkelaitosta.

Omavalvonnan kohteen velvollisuutena on toimia tietoturvasuunnitelman mukaisesti sekä seurata aktiivisesti suunnitelman toteutumista. Kyse on jatkuvasta ja säännöllisestä riittävän tietoturvan ja asiakastietojen hallinnan asianmukaisten käytäntöjen varmistamisesta sekä toteuttamisesta.

Ennen liittymistään Kelan valtakunnallisten tietojärjestelmäpalvelujen (Kanta-palvelut) käyttäjäksi on omavalvonnan kohteen tietoturvasuunnitelmassa selvitettävä, miten tietosuoja ja Kanta-palvelujen tietoturvallisen käytön edellyttämät vaatimukset on varmistettu.

THL voi tarvittaessa julkaista tarkempia ohjeita tietoturvasuunnitelmaan liittyvistä aiheista.

2 Vastuut tietoturvan sekä asiakastietojen asianmukaisen käsittelyn varmistamisessa

Omavalvonnan kohteen tulee varmistaa, että tietoturvasuunnitelma toteutuu kaikissa sen palveluyksiköissä ja muiden sen lukuun palveluiden tuottamiseen tai toteuttamiseen osallistuvien tahojen toiminnassa.

Kaikkien sosiaalihuollon asiakastietojen ja potilastietojen käsittelyn osapuolien vastuut tulee olla selkeästi määritelty. Osa kuvatuista tai vaadituista asioista voi olla jonkun muun kuin omavalvonnan kohteen itsensä vastuulla erilaisten järjestelyjen (esimerkiksi palveluhankinta, yhtymä, sovellusvuokraus) kautta.

Jos tietoturvasuunnitelmaan kuuluvia vastuita on jonkun muun kuin omavalvonnan kohteen itsensä vastuulla, vastuut on määriteltävä osapuolten välisissä toimeksianto- tai muissa sopimuksissa. Selkeät tietoturvan ja asiakastietojen käsittelyn vastuut tulee ulottaa koskemaan myös alihankkijoita ja muita mahdollisia sopimuskumppaneita. Sopimuksista tulee myös ilmetä, mihin toimiin osapuolet ryhtyvät, jos tietoturvassa ilmenee puutteita, ongelmia tai toteutuneita riskejä.

Palvelunantajalla on oltava sopimus muiden sen asiakas- tai potilastietojärjestelmiä käyttävien palvelunantajien ja mahdollisten ulkopuolisten ammatinharjoittajien keskinäisten vastuiden osalta asiakastietojen käsittelystä ja tietoturvallisuuden varmistamisesta.

Tietoturvallisuuden omavalvonnan kohde vastaa tietoturvasuunnitelmasta myös tilanteissa, joissa se hankkii käyttöympäristön tai tietotekniikkapalveluita esimerkiksi ostopalveluina muilta palveluiden antajilta tai tietojärjestelmäpalvelujen tuottajilta.

Keskinäisillä sopimuksilla ei kuitenkaan voida määritellä tai sopia vastuista asiakastietolaissa määritellystä poikkeavasti.

Tietoturvasuunnitelman varsinaisen sisällön tai siinä viitatuissa dokumenteissa esitetyn sisällön pohjalta on tarvittaessa pystyttävä todentamaan omavalvontaan liittyvät asiat: Tietoturvasuunnitelma on laadittu, se sisältää suunnitelmalta edellytettävät asiat tämän määräyksen mukaisesti, miten suunnitelmaa säännöllisesti päivitetään ja miten sen toteutumista seurataan. Palvelunantajan on pystyttävä osoittamaan tietoturvasuunnitelman olemassaolo, asianmukaisuus ja toteuttaminen esimerkiksi valvontaviranomaisille myös niissä tilanteissa, joissa palvelunantaja ei itse tuota palveluita. 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.

3 Määritelmät

Tässä määräyksessä tarkoitetaan:

- Palvelunantajalla
    - terveydenhuollon toimintayksikköä (potilaslaki 785/1992 2 §:n 1 mom. 4 kohta)
    - työnantajaa (työterveyshuoltolaki 1383/2001 7 § 2 mom.)
    - itsenäisenä ammatinharjoittajana toimivaa terveydenhuollon ammattihenkilöä (laki yksityisestä terveydenhuollosta 152/1990 2 § 3 mom.)

- sosiaalihuollon asiakasasiakirjalain 254/2015 3 §:n 1. mom. 3 kohdan mukaan sosiaalihuoltoa tai sosiaalipalveluja järjestävää, tuottavaa tai toteuttavaa viranomaista taikka yksityisistä sosiaalipalveluista annetussa laissa (922/2011) tarkoitettua palvelujen tuottajaa

- asiakastietolain mukaisen määritelmän lisäksi tässä määräyksessä palvelunantajaan kohdistuvat velvoitteet koskevat vastaavalla tavalla ja lain sähköisestä lääkemääräyksestä (61/2007, mukaan lukien lain 786/2021 mukaiset muutokset) mukaisessa laajuudessa myös lääkelain (395/1987) 38 §:n mukaista apteekkia;

- Tietojärjestelmällä tietojenkäsittelylaitteista, ohjelmistoista ja muusta tietojenkäsittelystä koostuvaa kokonaisjärjestelyä, jota tietojärjestelmän 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 (asiakastietolaki 3 §);

- Tietojärjestelmän valmistajalla tahoa, joka on vastuussa sosiaali- ja terveydenhuollon tietojärjestelmän suunnittelusta ja valmistuksesta (asiakastietolaki 3 §), riippumatta siitä toimiiko tämä taho myös tietojärjestelmäpalvelun tuottajana;

- Tietojärjestelmäpalvelun tuottajalla tahoa, joka tarjoaa tai toteuttaa palvelunantajalle tietojärjestelmää, jossa käsitellään asiakas- tai hyvinvointitietoa, ja joka vastaa tietojärjestelmän valmistajana, valmistajan lukuun tai yhden tai useamman valmistajan puolesta tietojärjestelmälle asetetuista vaatimuksista (asiakastietolaki 3 §);

- Tietojärjestelmän käyttöympäristöllä teknistä, organisatorista ja fyysistä ympäristöä, jossa yksi tai useampi palvelunantaja käyttää tietojärjestelmää tai osajärjestelmää sosiaali- ja terveydenhuollon palvelujen tuottamisessa ja asiakastietojen käsittelyssä;

    - käyttöympäristö sisältää mm. päätelaitteet, palvelimet, työasemat, käyttöjärjestelmä- ja varusohjelmistot sekä hallinta- ja tietoturvakäytännöt, jotka eivät ole osa tietojärjestelmää;

- Kanta-palveluilla sosiaali- ja terveydenhuollon valtakunnallisia tietojärjestelmäpalveluita, joita ovat asiakastietolain 6 §:n mukaiset palvelut;

- Välittäjällä palvelunantajan tietojärjestelmäpalvelujen tuottamisessa, tietojärjestelmien teknisen tai fyysisen käyttöympäristön toteuttamisessa tai valtakunnallisiin tietojärjestelmäpalveluihin liittymisessä käyttämää palveluntarjoajaa, jolla on tässä roolissa mahdollisuus nähdä salaamattomia asiakastietoja, esimerkiksi ylläpitotoimien yhteydessä;

- Valvontaviranomaisella sosiaali- ja terveysalan lupa- ja valvontavirastoa (Valvira), aluehallintovirastoja (AVI) sekä tietosuojavaltuutettua;

- Sertifioinnilla menettelyä, jolla todennetaan tietojärjestelmän täyttävän sitä koskevat tuotantokäyttöä varten vaadittavat olennaiset vaatimukset (asiakastietolaki 3 §). Luokkaan A kuuluvien järjestelmien vaatimusten todentaminen tehdään tietoturvallisuuden arvioinnin ja tarvittaessa yhteistestauksen kautta. Järjestelmälle hyväksytysti tehdystä sertifioinnista tehdään merkinnät valvontaviranomaisen rekisteriin (THL:n määräyksen 4/2021 mukaisesti);

- Apteekilla lääkelain (395/1987) 38 §:ssä tarkoitettua apteekkia.

4 Suhde THL:n muihin määräyksiin, yleisiin viitekehyksiin sekä eräisiin muihin säädöksiin

Tämän THL:n määräyksen 3/2021 lisäksi tietoturvasuunnitelman laatimisessa tulee soveltaa THL:n määräystä 5/2021 (ks. erityisesti luku 9) sosiaali- ja terveydenhuollon tietojärjestelmien olennaisista toiminnallisista ja tietoturvavaatimuksista kohdistuen asiakastietojen käsittelyyn tarkoitettuihin tietojärjestelmiin.

THL:n määräyksessä 4/2021 sosiaali- ja terveydenhuollon tietojärjestelmien luokittelusta ja sertifioinnista ja sen liitteessä 1, Esimerkkejä järjestelmien luokittelusta, on kuvattu tietojärjestelmien luokittelua käytännön esimerkkeineen.

Tietoturvasuunnitelman laatimisessa suositellaan käytettäväksi tietoturvallisuuden suunnitteluun tarkoitettuja standardeja ja viitekehyksiä, kuten esimerkiksi ISO 27000-sarjan standardeja.

THL:n määräyksen 3/2021 kohdealueena eivät ole lääkinnällisten laitteiden säädökset. Jos tietojärjestelmä täyttää lääkinnällisen laitteen määritelmän, on otettava huomioon sekä asiakastietolaki että lääkinnällisten laitteiden säädökset, kuten Euroopan parlamentin ja neuvoston asetus (EU) 2017/745[1].

THL:n määräyksen 3/2021 kohdealueena eivät ole sosiaali- ja terveystietojen toissijaisesta käytöstä annetun lain (552/2019), *toisiolain*, mukaiset käyttötarkoitukset. Palvelunantajan on kuitenkin mahdollista huomioida myös toisiolakiin liittyviä tiedonkäsittelyn vaatimuksia tietoturvasuunnitelmassaan. Joillakin tietojärjestelmillä voi olla sekä asiakastietolain että toisiokäytön mukaisia käyttötarkoituksia.

Laki julkisen hallinnon tiedonhallinnasta (906/2019), *tiedonhallintalaki*, on yleislaki, jota sovelletaan tiedonhallintaan ja tietojärjestelmien käyttöön, kun viranomaiset käsittelevät tietoaineistoja. Tiedonhallintalakia sovelletaan julkisen sektorin sosiaali- ja terveydenhuollossa siltä osin kuin erityislainsäädännössä (esim. asiakastietolaki) ei toisin säädetä. Asiakastietolaissa myös säädetään eräiltä osin tiedonhallintalakia täsmentävällä tavalla. Asiakastietolain 27 §:n mukainen tietoturvasuunnitelma on säädetty julkisten ja yksityisten sosiaali- ja terveydenhuollon palvelunantajien velvoitteeksi, jotta menettelyt olisivat yhdenmukaisia kaikille palvelunantajille. Lisäksi varmistetaan vastaavat menettelyt Kansaneläkelaitokselle (Kela) ja välittäjille. Tämän määräyksen mukaista tietoturvasuunnitelmaa noudatetaan tiedonhallintalain tietoturvavelvoitteiden toimeenpanossa julkisissa sosiaali- ja terveyspalveluissa asiakastietolain 27 §:n 1 ja 2 momentin kuvaamien seikkojen osalta.

5 Yleistä tietoturvasuunnitelmasta

Asiakastietolain 27 §:n mukaisesti palvelunantajan on laadittava tietoturvaan ja tietosuojaan sekä tietojärjestelmien käyttöön liittyvä tietoturvasuunnitelma.

Aiemman asiakastietolain 159/2007 mukaisesti palvelunantajien tuli tuottaa omavalvontasuunnitelma tietosuojasta, tietoturvallisuudesta ja tietojärjestelmien käytöstä. Muita omavalvontasuunnitelma-nimisiä dokumentteja koskevia säännöksiä on mm. terveydenhuoltolain (1326/2010) 8 §:ssä, yksityisestä terveydenhuollosta annetun lain 6 §:ssä, yksityisestä sosiaalihuollosta annetun lain 6 §:ssä, sosiaalihuoltolain (1301/2014) 47 §:ssä ja vanhuspalvelulain (980/2012) 23 §:ssä.

[1] Euroopan parlamentin ja neuvoston asetus (EU) 2017/745, annettu 5 päivänä huhtikuuta 2017, lääkinnällisistä laitteista, direktiivin 2001/83/EY, asetuksen (EY) N:o 178/2002 ja asetuksen (EY) N:o 1223/2009 muuttamisesta sekä neuvoston direktiivien 90/385/ETY ja 93/42/ETY kumoamisesta.

Tämän määräyksen mukaista tietoturvasuunnitelmaa ei tule sisällyttää tai yhdistää julkaistaviin tai julkisesti saatavilla oleviin omavalvontasuunnitelmiin. Tietoturvasuunnitelmaa ja siinä viitattuja liitedokumentteja tulee käsitellä ja säilyttää ottaen huomioon tarvittava suojaaminen sivullisilta ja tarvittaessa niihin tulee merkitä salassa pidettävä -tieto. Palvelunantaja, joka toimii viranomaisena, tulee huomioida viranomaisten toiminnan julkisuudesta annetun lain (621/1999), *julkisuuslain*, salassa pitoa koskevat säännökset (mm. 24 § 1 mom. 7 kohta, jonka mukaan tietojärjestelmien turvajärjestelyjä koskevat ja niiden toteuttamiseen vaikuttavat asiakirjat ovat pääsääntöisesti salassa pidettäviä).

Tietoturvasuunnitelmaan sisältyvien selvitysten avulla varmistetaan, että palvelunantajan henkilökunta hallitsee käytössään olevien tietojärjestelmien käytön ja ottaa huomioon sosiaalihuollon asiakastietojen ja potilastietojen salassapitoon ja tietoturvaan liittyvät vaatimukset sekä ymmärtää väärinkäyttöön liittyvät seuraamukset. Tietoturvasuunnitelmaan sisältyvien vaatimuksien tarkoituksena on varmistaa, että tietojärjestelmiä asentaa, ylläpitää ja päivittää vain henkilöstö, jolla on siihen tarvittava ammattitaito ja asiantuntemus.

Tietoturvasuunnitelmassa kuvatuilla menettelyillä ja keinoilla myös varmistetaan, että tietojärjestelmiin liitetyt muut tietojärjestelmät tai muut järjestelmät eivät vaaranna tietojärjestelmien suorituskykyä eivätkä niiden tietoturva- tai tietosuojaominaisuuksia. Lisäksi tietoturvasuunnitelmassa tulee ottaa huomioon tietojärjestelmien käyttöympäristöön, ylläpitoon ja päivityksiin liittyvät asiat.

Tietoturvasuunnitelman avulla tulee varmistaa, että asiakastiedon käsittelyssä otetaan kattavasti huomioon tietosuojaan ja tietoturvaan liittyvät seikat tietoturvallisuuden omavalvonnan kohteen toiminnassa ja tietojärjestelmien käyttöympäristössä. Tietoturvasuunnitelmassa kuvattujen menettelyiden ja keinojen avulla voidaan ehkäistä ja hallita riskejä. Tietoturvasuunnitelma tulisi laatia riskilähtöisesti arvioiden mahdollisia riskejä, niihin liittyviä todennäköisyyksiä sekä todettujen riskien vaikutuksia. Lisäksi tulisi arvioida riskien vähentämisen (hyväksyttävät jäännösriskit) tai niiden kokonaan poistamisen seuraukset.

Asiakastietolain 28 §:n mukaisesti sosiaali- ja terveydenhuollon palvelunantajan vastaavan johtajan on huolehdittava, että 27 §:ssä tarkoitettu tietoturvasuunnitelma laaditaan, sitä säännöllisesti ylläpidetään ja sitä noudatetaan. Osana suunnitelmaa on kuvattava se, kuinka suunnitelman toteuttaminen ja suunnitelman kohteena olevien seikkojen tietoturvallisuuden omavalvonta käytännössä järjestetään.

Kelan valtakunnallisten tietojärjestelmäpalvelujen käytön osalta tietoturvasuunnitelmassa on selvitettävä myös niihin liittyvät tietosuojan ja tietoturvan erityiskysymykset. Ennen liittymistään Kanta-palvelujen käyttäjäksi on palvelunantajan tietoturvasuunnitelmassa selvitettävä, miten Kanta-palvelujen tietoturvallisen käytön ja tietosuojan edellyttämät vaatimukset on varmistettu ja miten Kanta-palveluihin liittyvät tietosuojan ja tietoturvan erityiskysymykset (ks. luku 6.12) on järjestetty.

Tietoturvasuunnitelma on asioita yhteen kokoavana dokumenttina käytännön työväline tietoturvallisuuden kokonaiskuvan hahmottamisessa ja asiakastietojen käsittelyn hyvien käytäntöjen toteuttamisessa. Tietoturvasuunnitelman mukaiset selvitykset ja käytännöt voidaan yhdistää muihin palvelunantajan tietosuojaa ja tietoturvallisuutta ohjaaviin menettelyohjeisiin, laatukäsikirjoihin tai tietoturvapolitiikkoihin. Kuvaukset voivat olla tarvittaessa tietojärjestelmäkohtaisia tai yhteisiä useille saman suunnitelman piirissä toimiville tahoille. Kaikkien kuvausten ei tarvitse sisältyä tietoturvasuunnitelmaan, vaan suunnitelmassa voidaan viitata erillisiin saatavilla oleviin kuvauksiin, kuten tietoturvallisuuden omavalvonnan kohteen tietoturvaohjeisiin tai tietojärjestelmäsalkun kuvauksiin.

Luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2016/679 (*yleinen tietosuoja-asetus*).[2] 5 artiklan 2 kohdan mukaista osoitusvelvollisuutta toteutetaan esimerkiksi dokumentoimalla tehtyjä toimenpiteitä, laatimalla vaikutustenarviointi, tietotilinpäätös ja seloste käsittelytoimista sekä muilla vastaavilla menettelyillä, jolla osoitetaan rekisterinpitäjän ja henkilötietojen käsittelijän toiminnan säädösten mukaisuus. Näiden menettelyjen mukaisia sisältöjä on mahdollista yhdistää tietoturvasuunnitelmaan ja sen toteuttamisen ja omavalvonnan dokumentointiin. Tietoturvasuunnitelma on dokumentti, jolla rekisterinpitäjä voi täydentää yleisen tietosuoja-asetuksen mukaista osoitusvelvollisuuttaan.

Tietoturvasuunnitelmassa kuvatut asiat on voitava tarpeen mukaan todentaa tietoturvallisuuden omavalvonnan toteutumisen tarkastusta tekevälle valvontaviranomaiselle.

Tietoturvasuunnitelman on katettava kaikki palvelunantajan käyttämät sosiaalihuollon asiakastietojen ja potilastietojen käsittelyyn tarkoitetut tietojärjestelmät. Palvelunantajan on osaltaan varmistettava tietojärjestelmiin liittyvien olennaisten vaatimusten toteutuminen tietojärjestelmiä hankkiessaan, kehittäessään ja käyttäessään. Olennaisten vaatimusten toteutumisen varmistamisessa tulisi hyödyntää Valviran tietojärjestelmärekisterissä olevia tietoja. Olennaisten vaatimusten toteuttamisesta tietojärjestelmään sekä tietojärjestelmien luokittelusta ja sertifioinnista vastaa tietojärjestelmäpalvelun tuottaja tai tietojärjestelmän valmistaja.

6 Tietoturvasuunnitelmaan sisällytettävät selvitykset ja vaatimukset

Tietoturvasuunnitelmassa on oltava selvitykset siitä, miten sosiaalihuollon asiakastietojen ja potilastietojen käsittelyyn ja tietojärjestelmiin liittyvät vaatimukset varmistetaan. Kyseiset vaatimukset ovat asiakastietolain 27 §:n 1 momentin kohdat 1-9 sekä 27 §:n 2 momentti.

Tietoturvasuunnitelmassa on kuvattava määräyksen luvun 6 mukaiset alakohdat 6.1-6.12 tietoturvallisuuden omavalvonnan kohteen omaan toimintaan ja käytössä oleviin IT-ratkaisuihin liittyen.

Tietoturvasuunnitelmaan on mahdollista täydentää asiakastietolain 27 §:n vaatimusten lisäksi myös muita omavalvonnan kohteen kannalta olennaisia seikkoja.

Tietoturvasuunnitelmassa voidaan aina viitata, kun se on mahdollista olemassa oleviin erikseen ylläpidettäviin ohjeisiin ja dokumentteihin. Olennaista on, että suunnitelman tietojen avulla on selvää, mistä dokumentaatio on löydettävissä tai miten vaatimuksen täyttyminen on todennettavissa. Mikäli muuta valmista dokumentaatiota ei ole olemassa tai saatavissa, on vaadittavat asiakokonaisuudet ja toimintatavat mahdollista kuvata suoraan tietoturvasuunnitelmaan.

6.1 Yleiset tietoturvakäytännöt

Tietoturvasuunnitelmaan tulee kuvata omavalvonnan kohteen yleiset tietoturvakäytännöt ja/tai voimassa olevat tietoturvapolitiikat. Lisäksi suunnitelmasta tulee löytyä tieto henkilötietojen käsittelytoimien selosteista, asiakastietojen käsittelyyn liittyvistä sopimuksista, keskeisistä tietoturvallisuusohjeista sekä tietosuojavastaavista. Tietoturvasuunnitelmasta on myös käytävä ilmi, kuinka dokumentaatiota kehitetään ja säännöllisesti tarkistetaan, miten tietoturvallisuustyössä on vastuita jaettu ja organisoitu toiminnan tavoitteiden saavuttamiseksi sekä riskien hallitsemiseksi.

[2] Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus).

Sähköisestä lääkemääräyksestä annetun lain 24 §:n 5 momentin mukaan palvelunantajan ja apteekin seuranta- ja valvontatehtävää varten nimettävästä tietosuojavastaavasta säädetään tietosuoja-asetuksen 37 artiklassa. Asiakastietolain 28 §:n 4 momentin mukaan tietosuojavastaavan nimittämisestä sekä tietosuojavastaavan asemasta ja tehtävistä säädetään tietosuoja-asetuksen 37–39 artiklassa. Tietoturvallisuuden omavalvonnan kohteella on siten oltava nimetty tietosuojavastaava (tai useita) sen mukaisesti kuin edellä mainituissa laeissa säädetään. Tietosuojavastaavalla tulisi olla selkeä ja dokumentoitu tehtäväkuva, jossa otetaan huomioon asiakas- ja potilastietojen käsittelyyn liittyvät velvoitteet. Tietosuojavastaavalla tulisi olla tehtävään soveltuva osaaminen ja riittävät resurssit hoitaa tehtävää omavalvonnan kohteessa ottaen muun muassa huomioon rekisterinpitoon ja henkilötietojen käsittelyyn liittyvät vastuut ja velvoitteet, organisaation koko ja toiminnan laajuus.

Tietoturvasuunnitelman tavoitteena on varmistaa, että tietoja käyttävät ja tuottavat asiakastietojen käsittelijät ymmärtävät asiakastietojen käsittelyyn liittyvät vastuut ja osaavat toimia siten, että asiakastietojen eheys, luottamuksellisuus, saatavuus, kiistämättömyys ja autenttisuus toteutuvat. Suunnitelma sisältää sekä henkilöstöön että tietohallintoon liittyviä sisältöjä, ja esimerkiksi henkilöstölle tarkoitetut sisällöt on mahdollista erottaa tietohallinnon asiantuntijoille tai kehitys- ja hankintatoiminnassa huomioon otettavista sisällöistä.

6.2 Menettelyt virhe- ja ongelmatilanteissa sekä jatkuvuudenhallinta

Tietoturvallisuuden omavalvonnan kohteen on varauduttava virhe- ja ongelmatilanteisiin, tietoturvapoikkeamiin, tietoturvaloukkauksiin sekä muihin häiriöihin siten, että asiakas- ja potilastietojen käsittelyn jatkuvuus voidaan erilaisissa olosuhteissa hallita ja turvata. Virhe- ja ongelmatilanteiden varalle tulee tietoturvallisuuden omavalvonnan kohteella olla ennalta määritellyt ja selkeät toimintatavat, toimintaohjeet ja vastuut kyseisten tilanteiden ennalta havainnointiin, tiedottamiseen, korjaamiseen ja tilanteista toipumiseen (tietoturvapoikkeaman hallinta - incident management). Myös tietojärjestelmien mahdollinen ennalta luokittelu kriittisyyden perustella vaikuttaa varautumisen käytännön toteuttamiseen. Nämä seikat voivat olla kuvattuna tietoturvasuunnitelmaan tai tietoturvasuunnitelmassa viitattaviin erillisiin jatkuvuus-, toipumis- ja varautumissuunnitelmiin, joiden mukaisia menettelyitä noudatetaan virhe- ja ongelmatilanteissa.

Palvelunantajan tulee suunnitella tietojärjestelmähäiriöiden edellyttämät jatkuvuuden toimenpiteet, ohjeet ja hankinnat. Menettelytapoja normaalista poikkeavien tilanteiden ja poikkeusolojen varalle tulee säännöllisesti läpikäydä, testata ja tarkistaa, jotta käytännön menettelyt toimivat virhe- ja ongelmatilanteissa, ja jotta muun muassa tarpeellisten ohjeiden saatavuus on turvattu näissä erityistilanteissa.

Selvittelykäytänteiden ja hallintamallien kuvaaminen sekä vastuiden määrittely tulee tehdä verkko- ja tietoliikenneongelmien, tietojärjestelmien käyttöongelmien sekä havaittujen ja toteutuneiden tietoturvaloukkausten varalta. Lisäksi tulee olla kuvattuna, kuinka palvelunantajan on mahdollista saada käyttöönsä häiriötilanteesta tarkempaa seurantatietoa, kuten esimerkiksi tapahtumalokeja aikaleimoineen tilanteen ja tapahtuneen selvittämiseen.

Potilasturvallisuutta ja tietoturvallisuutta uhanneista tapahtumista tulisi kerätä oleelliset tiedot, jotta toimintaa voidaan kehittää edelleen.

Terveydenhuollon palvelunantajan on määriteltävä tärkeimpien tietojärjestelmien ja niiden komponenttien kriittisyys potilasturvallisuuden näkökulmasta. Olennaista on tunnistaa kriittiset tietojärjestelmät ja tietojärjestelmien toimivuuden kannalta kriittiset osajärjestelmät, laitteet ja muut resurssit. Järjestelmien luotettavuudesta tulee huolehtia esimerkiksi toimivien kahdennusten, suunniteltujen tilapäisratkaisujen, varaosien, erityiskomponenttien ja aktiivisten valvonta- ja huoltotoimien avulla. Tietojärjestelmien, laitteiden ja verkkojen huolto, päivitykset ja tarvittaessa uusiminen tulee suunnitella. Näin varmistetaan, että tarvittavat komponentti- ja ohjelmistopäivitykset hoidetaan hyvissä ajoin ennen mahdollisia vikaantumisia. Komponenttien kriittisyyttä tulee tarkastella vähintään asiakas- ja potilasturvallisuuden näkökulmasta.

Asiakastietolain 41 §:n mukaisesti tulee tietojärjestelmän olennaisten vaatimusten merkittävistä poikkeamista ilmoittaa tietojärjestelmäpalvelun tuottajalle. Merkittäviä poikkeamia on kuvattu THL:n määräyksen 5/2021 luvussa 10.4. Tietojärjestelmien merkittävistä poikkeamista tulee ilmoittaa Valviralle, erityisesti tilanteissa, joissa poikkeama voi aiheuttaa merkittävän riskin asiakas- tai potilasturvallisuudelle tai tietoturvalle. Merkittävien poikkeamien korjaamiseksi on ryhdyttävä korjaaviin toimenpiteisiin.

Asiakastietolain 41 §:n mukaan, jos palvelunantaja tai muu taho havaitsee tietojärjestelmän olennaisten vaatimusten täyttymisessä tietosuojapoikkeamia, sen on ilmoitettava asiasta tietosuojavaltuutetulle. Henkilötietojen tietoturvaloukkauksesta ilmoittamisesta säädetään EU:n yleisen tietosuoja-asetuksen 33 ja 34 artikloissa. Henkilötietojen tietoturvaloukkausten hallinta tietoturvallisuuden omavalvonnan kohteessa tulee olla dokumentoitu joko suoraan tietoturvasuunnitelmaan tai muihin asiakirjoihin, joihin viitataan tietoturvasuunnitelmassa.

6.3 Henkilöstön koulutus sekä osaamisen ylläpito ja kehittäminen

Tietoturvasuunnitelmaan on sisällytettävä selvitys siitä, kuinka tietojärjestelmiä käyttäville henkilöille varmistetaan järjestelmien käytön vaatima koulutus ja osaaminen. Tietojärjestelmiä käyttävillä henkilöillä on oltava koulutusta sekä asiakastietojen käsittelyyn että tietosuoja- ja tietoturva-asioihin. Organisaatiossa tarjolla olevan koulutuksen määrän ja sisällön on oltava riittävä ja tarkoituksenmukainen henkilön tai henkilöstöryhmän työ- ja tietojenkäsittelytehtävien kannalta. Koulutusta on tarjottava säännöllisesti sekä olemassa olevien taitojen ylläpitämiseksi että uusien tehtävien tai tilanteiden hoitamiseksi.

Omavalvonnan kohteella on oltava koulutussuunnitelma tai vastaava asiakirja, jossa kuvataan toimintamalli henkilöstön perehdyttämiseen, koulutukseen sekä osaamisen ylläpitoon, seurantaan ja ajantasaisuuden varmistamiseen asiakastietojen käsittelyssä sekä tietosuoja- ja tietoturva-aiheissa. Koulutussuunnitelmassa on kuvattava erilaisissa työtehtävissä ja rooleissa vaadittavan koulutuksen sisältö ja toteuttamistavat. Tietojärjestelmän käyttäjiltä vaadittava koulutus ja osaaminen voidaan todentaa joko todistuksilla tai merkinnöillä koulutuksiin osallistumisesta tai muulla organisaatiossa sovitulla tavalla.

Tietoturvasuunnitelmassa on kuvattava, kuinka omavalvonnan kohteen toiminnassa asiakastietoja käsitteleville työntekijöille selkeytetään ja informoidaan asiakastietojen käsittelyn perusteet kuten asiakastietojen kirjaamisen, käytön ja suojaamisen merkitys, tietojen käsittelijän vastuu sekä tietojen käsittelyyn liittyvän omavalvonnan ja viranomaisvalvonnan olemassaolo ja merkitys.

Tietojen luovutusperusteista säädetään laissa. Tietoja luovutettaessa tulee selvittää laillinen peruste, jonka nojalla asiakastieto voidaan luovuttaa vastaanottajalle ja lisäksi selvittää, että tiedonvastaanottaja saa asiakas- tai potilastiedon ainoastaan niiltä osin kuin hänellä on lain mukaan oikeus saada. Asiakastietoja luovuttavien henkilöiden ja järjestelmien on myös varmistettava, että tietojen luovutuksista syntyy luovutusilmoitus tai luovutusloki. Näihin seikkoihin liittyvä osaaminen tulisi olla osa koulutusta ja perehdytystä.

6.4 Tietojärjestelmien käyttöohjeet ja ohjeiden mukainen käyttö

Tietoturvasuunnitelmassa on kuvattava, miten tietojärjestelmän asianmukainen ja tietoturvallinen käyttö varmistetaan tietoturvallisuuden omavalvonnan kohteen käyttöympäristössä tietojärjestelmäpalvelun tuottajan (tai tietojärjestelmän valmistajan) antaman ohjeistuksen mukaisesti.

Tietoturvasuunnitelmassa on selvitettävä, miten on varmistettu, että tietojärjestelmän käyttäjällä on saatavilla tarpeelliset käyttöohjeet vähintään sillä kielellä, jonka osaaminen on vähimmäisvaatimus kyseisessä työtehtävässä toimimiselle. Ohjeita tarvitaan sekä organisaatio- että tietojärjestelmälähtöisesti: sosiaali- tai terveydenhuollon henkilöstölle tarkoitetut organisaation ohjeet omavalvonnan kohteen omassa toiminnassa sekä tietojärjestelmien

varsinaiset käyttöohjeet. Ajantasaisten käyttöohjeiden saatavuudesta ja niiden sijainnista tulee jakaa tietoa käyttäjille.

Sosiaalihuollon asiakastietojen ja potilastietojen käsittelystä tulee olla annettu kirjalliset ohjeet kaikille asiakastietoja käsitteleville työntekijöille. Käyttöohjeiden ja muiden tarvittavien ohjeiden on oltava ymmärrettäviä ja vastattava organisaatiossa käytössä olevan tietojärjestelmän versiota. Ohjeistuksissa tulee ottaa huomioon erilaiset työtehtävät ja roolit ja pyrkiä yksiselitteisyyteen.

Tietoturvasuunnitelmassa tulee selvittää, mistä löytyvät tietojärjestelmäpalvelun tuottajan antamat ohjeistukset ja tiedot koulutuksista käyttäjäorganisaation eri jakelukanavissa. Suunnitelmassa on kuvattava myös omavalvonnan kohteen omat menettelytavat, joilla seurataan tietojärjestelmäpalvelun tuottajan antamien ohjeistusten mukaista käyttöä tai täydennetään ohjeistuksia. Lisäksi tietoturvasuunnitelmassa on oltava kuvattuna toimintamalli, miten käyttöohjeiden päivittäminen ja jakelu käytännössä toteutetaan tietojärjestelmien ja ohjelmistojen versiopäivitysten sekä muiden muutosten yhteydessä.

6.5 Tietojärjestelmien perustiedot, kuvaukset ja olennaisten vaatimusten täyttyminen

Palvelunantajan tulee sisällyttää tietoturvasuunnitelmaansa tai sen liitteisiin perustiedot ja tarkemmat kuvaukset kaikista sen käytössä olevista, asiakastietolain mukaisista tietojärjestelmistä. Näitä ovat tietojärjestelmät, jotka on tarkoitettu käytettäväksi sosiaalihuollon asiakastietojen ja potilastietojen sähköiseen käsittelyyn, asiakasasiakirjojen tallentamiseen ja ylläpitoon tai valtakunnallisiin tietojärjestelmäpalveluihin liittämiseen tai joilla sosiaali- ja terveydenhuollon ammattihenkilö voi hyödyntää hyvinvointitietoja.

Tietojärjestelmäpalvelun tuottajan ja tietojärjestelmän valmistajan on toteutettava olennaiset vaatimukset tietojärjestelmiin, joita käytetään palvelunantajan toiminnassa (vrt. THL:n määräys 5/2021). Palvelunantajan on osaltaan huolehdittava näiden vaatimusten täyttymisestä tietojärjestelmiin liittyvissä järjestelyissä, kuten esimerkiksi hankinnoissa ja sopimuksissa. Tietoturvallisuuden omavalvonnan kohde vastaa osaltaan olennaisten vaatimusten täyttymisestä omassa toiminnassaan. Olennaisten vaatimusten täyttymisen varmistamiseen liittyvät menettelyt kuvataan tietoturvasuunnitelmaan.

Palvelunantajan tulee asiakastietolain 27 §:n 1 momentin kohdan 8 mukaisesti varmistaa, että 29 §:ssä tarkoitetut tietojärjestelmät täyttävät käyttötarkoituksensa mukaiset olennaiset vaatimukset 34 §:n 2 momentin mukaisesti. 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.

Valvira ylläpitää julkista rekisteriä sosiaalihuollon asiakastietojen ja potilastietojen käsittelyyn tarkoitetuista tietojärjestelmistä. Valviran tietojärjestelmärekisteri perustuu tietojärjestelmäpalvelujen tuottajien ilmoituksiin ja luokan A järjestelmien sertifioinnin tuloksiin. Tietojärjestelmiin liittyvissä tietoturvasuunnitelman sisällöissä tulisi nojautua Valviran tietojärjestelmärekisterin hyödyntämiseen. Valviran tietojärjestelmärekisteri sisältää tietoja siitä, mitä olennaisia vaatimuksia eri tietojärjestelmiin on toteutettu ja kuinka luokan A järjestelmissä on todennettu olennaisten vaatimusten täyttyminen.

Tietoturvallisuuden omavalvonnan kohteen on kuvattava tietoturvasuunnitelmaan tai siinä viitatuissa dokumenteissa, mistä löytyy tieto seuraavan tyyppisistä tietojärjestelmistä ja niiden versioista, joita tietoturvallisuuden omavalvonnan kohteen toiminnassa käytetään (vrt. THL:n määräys 4/2021):

- sertifioidut – tietoturva-auditoidut ja yhteistestatut Kanta-palveluihin liitettävät luokkaan A2 tai A3 kuuluvat sosiaalihuollon asiakastietojen tai potilastietojen käsittelyyn tarkoitetut tietojärjestelmät

- sertifioidut – tietoturva-auditoidut luokkaan A1 kuuluvat sosiaalihuollon asiakastietojen tai potilastietojen käsittelyyn tarkoitetut tietojärjestelmät

- sosiaalihuollon asiakastietojen tai potilastietojen käsittelyyn tarkoitetut luokkaan B kuuluvat tietojärjestelmät

- muut tietojärjestelmät, joilla on vaikutusta ja jotka on otettava huomioon tietoturvasuunnitelman mukaisissa asennuksissa, ylläpidossa ja päivityksissä arkaluonteisten asiakastietojen suojaamisen kannalta.

Lisäksi tietojärjestelmistä on kuvattava niiden versiotiedot tai muut tietojärjestelmän statusta kuvaavat tiedot.

Tietoturvallisuuden omavalvonnan kohteen on selvitettävä tietoturvasuunnitelmassa, miten varmistetaan se, että Kanta-palveluihin liittyviin tietojärjestelmiin liitetyt tai käyttöympäristössä hyödynnettävät muut sovellukset tai tietojärjestelmät eivät vaaranna tietojärjestelmien suorituskykyä eivätkä niiden tietoturva- tai tietosuojaominaisuuksia. Muilla sovelluksilla ja tietojärjestelmillä tarkoitetaan esimerkiksi tietokoneohjelmia, jotka eivät käsittele asiakas- ja potilastietoja, eivätkä siten ole asiakastietolain 29 §:n mukaisia luokan A tai B tietojärjestelmiä.

Määräyksen 5/2021 mukaisesti palvelunantajan on huomioitava omassa toiminnassaan ja tietojärjestelmien käyttöönotossa, tuotantokäytössä sekä tietoturvasuunnitelman mukaisessa toiminnassa ne olennaisiin vaatimuksiin kohdistuvat huomioitavat seikat ja sertifioinnissa esiin nousseet havainnot ja edellytykset, jotka vaikuttavat olennaisten vaatimusten toteutumiseen palvelunantajan käyttämissä tietojärjestelmissä. Erityisesti on huomioitava Valviran tietojärjestelmärekisterin kautta julkaistavat tarkennukset järjestelmien vaatimustenmukaisuuden toteutumiseen.

Tietoturvasuunnitelman ei tarvitse kattaa omavalvonnan kohteessa käytettäviä sovellusohjelmistoja tai tietojärjestelmiä, joiden käyttötarkoituksena ei ole asiakas- tai potilastietojen käsittely, mutta myös niitä on mahdollista sisällyttää suunnitelmaan.

6.6 Tietojärjestelmien asennus, ylläpito ja päivitys

Asiakastietojen käsittelyyn tarkoitettua tietojärjestelmää ei saa ottaa tuotantokäyttöön, ellei siitä ole voimassa olevia tietoja Valviran tietojärjestelmärekisterissä. Luokkaan A kuuluvan tietojärjestelmän tai hyvinvointisovelluksen saa ottaa tuotantokäyttöön sen jälkeen, kun Valviran rekisteristä löytyy tieto järjestelmän sertifioinnista ja voimassa olevasta tietoturvallisuustodistuksesta. Tietojärjestelmää ei saa ottaa tuotantokäyttöön, jos luokkaan A kuuluvan tietojärjestelmän tietoturvallisuustodistus on vanhentunut, tai jos Valviran tietojärjestelmärekisterissä on järjestelmän käyttöönoton estävä poikkeama. Myös muut Valviran tietojärjestelmärekisterissä järjestelmään kohdistuvat olevat rajoitukset ja edellytykset on otettava huomioon (THL:n määräys 4/2021).

Tietoturvasuunnitelmaan on kuvattava tietoturvallisuuden omavalvonnan kohteeseen liittyvien tietojärjestelmien asennusten, ylläpidon ja päivitysten menettelytavat sekä niihin liittyvä tietoturvallisuuden varmistaminen. Kuvaukseen kuuluu myös henkilöstön roolit asennuksissa, ylläpidossa ja päivityksissä. Muutoksenhallinnan, testauksien ja hyväksymisten menettelyt sekä vastuut asennus-, ylläpito- ja päivitystyössä on sisällytettävä suunnitelmaan. Kuvaus on tehtävä sellaisella tarkkuustasolla, joka parhaiten tukee tietoturvallisuuteen ja asiakastietojen käsittelyyn liittyvää riskienhallintaa omavalvonnan kohteessa.

Tietoturvallisuuden omavalvonnan kohteen on selvitettävä tietoturvasuunnitelmassa, miten on varmistettu, että tietojärjestelmiä asennetaan, ylläpidetään ja päivitetään tietojärjestelmäpalvelun tuottajan ohjeiden mukaisesti. Tietojärjestelmäpalvelun tuottajien kanssa tehtävissä sopimuksissa tulisi kuvata tietoturvallisuuden omavalvonnan kohteen käyttöympäristön kannalta olennaiset seikat ja ohjeistukset liittyen tietojärjestelmien asennuksiin, ylläpitoon ja päivityksiin.

Vastaavasti tietoturvasuunnitelmassa on selvitettävä, miten on varmistettu, että tietojärjestelmiä asentaa, ylläpitää ja päivittää henkilöstö, jolla on siihen tarvittava ammattitaito ja asiantuntemus. Tietojärjestelmiä asentavien, ylläpitävien ja päivittävien henkilöiden roolit ja vastuut suhteessa tietoturvallisuuden omavalvonnan kohteeseen sekä tietojärjestelmäpalvelun tuottajaan on määriteltävä. Kuvauksiin voi kuulua myös mahdolliset tietojärjestelmien asennus-, ylläpito- ja päivitystyötä tekeviin henkilöihin kohdistuvat turvallisuusselvitykset. Tietojärjestelmäpalvelun tuottajan ja omavalvonnan kohteen välisissä sopimuksissa tulee ottaa kantaan näihin asioihin.

Edellä mainitut tietojärjestelmien asennukseen, ylläpitoon ja päivityksiin liittyvät seikat voidaan osoittaa tietoturvasuunnitelmaan sisältyvällä tai erillisellä suunnitelmalla, joka sisältää kuvaukset päivitys-, muutoksenhallinta- ja korjausprosesseista. Samassa suunnitelmassa on mahdollista esittää myös kuvaukset luvun 6.2 mukaisista virhe- ja poikkeustilanteisiin liittyvistä menettelytavoista. Päivitysprosessin kuvaamisessa on otettava huomioon muun muassa versio- ja korjauspäivitykset sekä muiden muutosten mahdollisesti vaatimat menettelyt. Muutoksenhallintaprosessissa voidaan kuvata muun muassa tietojärjestelmien muutosten ja uusien versioiden testaus- ja hyväksymismenettelyt. Asennus-, ylläpito- ja päivitystoimenpiteiden ongelma- ja virhetilanteiden hallinta tulee olla osa suunnitelmaa.

6.7 Käyttövaltuuksien hallinnan ja tunnistautumisen käytännöt

Tietoturvasuunnitelmassa ja sen liitedokumenteissa on kuvattava käyttövaltuuksien, tunnistautumisen ja pääsynhallinnan (ks. luku 6.8) käytännöt rajauksineen. Tietojärjestelmien käyttäjät ja erilaiset käyttäjäryhmät, käyttäjäroolit ja rooleihin liittyvät käyttövaltuudet on kuvattava. Keskeistä on kuvata myös se, missä määrin käyttövaltuuksia hallinnoidaan asiakas- tai potilastietojärjestelmien tai ulkoisen tietojärjestelmän, kuten identiteetin ja pääsynhallinta (IAM) -järjestelmän avulla.

Tietoturvasuunnitelmassa kuvataan se, kuinka hyväksytään ja dokumentoidaan muutokset esimerkiksi työroolien muutoksista johtuvissa asiakastietojen käyttövaltuuksissa. Tietoturvasuunnitelmassa on lisäksi kuvattava ne henkilöt tai roolit, joilla on oikeus hyväksyä käyttöoikeuspyyntöjä. Käyttövaltuuksia tulee läpikäydä ja seurata säännöllisesti niiden ajantasaisuuden varmistamiseksi.

Käyttövaltuuksien hallinnointiin liittyvät toimintatavat on kuvattava käyttövaltuuksien hakemisen, myöntämisen, seurannan, muuttamisen, tarkistamisen/varmistamisen ja poistamisen käytäntöjen osalta. Esimerkiksi, kuinka uudelle työntekijälle tai sijaiselle tietoturvallisesti järjestetään käyttöoikeudet erilaisissa käytännön tilanteissa ja ajankohdissa. Vastaavasti on kuvattava, kuinka, milloin ja millä tavalla poistuneiden työntekijöiden käyttöoikeudet poistetaan. Myös pääsyoikeuksien erityisen nopea poistaminen tarvittaessa yksittäisten tai useiden tunnusten osalta tulee kuvata. Asiakastietoon liittyvistä käyttöoikeuksista ja niihin tehdyistä muutoksista tulee pitää kirjaa ja lokia.

Kanta-palvelujen osalta omavalvonnan kohteen tulee hallinnoida huolellisesti tietojärjestelmän käyttäjien oikeuksia käyttää sähköiseen lääkemääräykseen, valtakunnalliseen potilastiedon arkistoon, sosiaalihuollon asiakastiedon arkistoon ja muuhun potilastietojen käsittelyyn liittyviä toimintoja.

Tunnisteellisten asiakastietojen katselu on rajoitettava vain niihin henkilöihin, jotka työtehtävissään tietoja tarvitsevat. STM:n valmisteilla oleva sosiaali- ja terveydenhuollon asiakastietojen käyttöoikeuksia koskeva asetus[3] ohjaa käyttövaltuuksien myöntämistä.

Pääkäyttäjillä ja tietojärjestelmäasiantuntijoilla ei ole oikeutta Kanta-palveluissa olevien tietojen käsittelyyn, kuten luovutushaku ja asiakirjan hakeminen omaan käyttöön. Poikkeuksen tähän muodostaa virhetilanteiden selvitykset, joissa pääkäyttäjillä ja tietojärjestelmäasiantuntijoilla on oikeus tarkastaa oman organisaationsa tai sen organisaation, jonka lukuun tietojärjestelmäasiantuntijat selvityksen aikana toimivat, tietoja Kanta-palveluista. Kanta-oikeudet rajataan edellä mainituissa virhetilanneselvityksissä ainoastaan oman organisaation tietojen hakuun Kanta-arkistointipalveluissa. Kaikki selvityksissä tehdyt haut tulee näkyä lokeista.

Asiakastietolain 17 §:n mukaan asiakastietojen käsittelyn osapuolet on tunnistettava luotettavasti ja asiakastietoja käsittelevät henkilöt on todennettava. Tietoturvasuunnitelmaan on kuvattava erilaisten tunnistautumisvälineiden, kuten toimikorttien hallinta.

Tietoturvasuunnitelmassa on kuvattava tietojärjestelmiä käyttävien henkilöiden tunnistautumistavat asiakastietoja käsittelevien tietojärjestelmien käyttöön. Asiakaskohtaisten tietojen tarkastelussa käyttäjä on tunnistettava ja todennettava yksiselitteisesti riippumatta siitä, minkä tyyppinen tietojärjestelmä on kyseessä (esimerkiksi asiakas- tai potilastietojärjestelmä, apteekkijärjestelmä, Kanta-palveluista tai paikallisista tietovarannoista tai tietoaltaista tietoja asiakaskohtaisesti yhdistävä katselin).

Tietojärjestelmien käytön tarkastelun lisäksi tulee kuvata ainakin työasemiin ja mobiililaitteisiin liittyvät kirjautumis- ja tunnistautumiskäytännöt sekä mahdolliset kulunvalvontaan liittyvät pääsynhallinnan ratkaisut. Toimitilojen fyysisen turvallisuuden ratkaisut voidaan yhdistää tietojärjestelmiin liittyviin turvakäytäntöihin.

Tietoturvasuunnitelmassa tulisi kuvata, missä järjestelmissä, tiedoissa, laitteissa tai tilanteissa edellytetään monivaiheista tunnistautumista (Multi-Factor Authentication, MFA) ja erityisesti toimikorttitunnistautumista sote-varmenteita käyttäen asiakastiedon luottamuksellisuuden ja eheyden varmistamiseksi.

Henkilön vahva sähköinen tunnistaminen on edellytys tietosuojan ja tietoturvan toteutumiselle Kanta-palveluissa. Kanta-palveluihin liittyvissä tietojärjestelmissä kirjautuminen valtakunnalliseen potilastiedon ja sosiaalihuollon asiakastiedon arkistoon liittyviin toiminnallisuuksiin, joilla saadaan luovutuksella saatavia tietoja, on sallittu ainoastaan vahvaa sähköistä tunnistautumista (sosiaali- ja terveydenhuollon toimikorttien varmenteet) käyttäen.

Käyttäjän henkilöllisyys on aina varmistettava ennen käyttöoikeuksien tai tunnistusvälineiden myöntämistä. Varmistamisen ja todentamisen tapa kuvataan tietoturvasuunnitelmassa.

Käyttäjätunnuksella ja salasanalla tunnistautumista voidaan käyttää ainoastaan paikallisesti omavalvonnan kohteen asiakas- ja potilastietojärjestelmissä tapahtuvassa asiakastietojen käsittelyssä.

Potilastietoja tai sosiaalihuollon asiakastietoja käsittelevissä tietojärjestelmissä, riippumatta siitä liittyykö järjestelmä Kanta-palveluihin, ei saa olla käytössä yhteiskäyttöisiä tunnuksia asiakastietojen muokkaamiseen, katseluun tai sähköiseen reseptiin liittyvien toiminnallisuuksien osalta. Vaatimus koskee myös ylläpito- ja muita vastaavia käyttöoikeuksia.

[3] https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=d6c17aaa-a4c9-4ecb-99f6-67cfcbcf4b87

Yhteiskäyttöisten tunnusten käyttö on sallittu tilanteissa, joissa tarkastellaan resurssien käyttöä tai muita prosesseihin liittyviä ei-tunnisteellisia, yksittäisiin henkilöihin liittymättömiä tietoja tai yhteenvetotietoja useista asiakkaista.

Usean käyttäjän näkymiä tunnisteellisiin asiakastietoihin on mahdollista käyttää osaston potilaspaikkojen koontinäyttöissä tai vastaavissa käytännön työn kannalta välttämättömissä potilashallinnollisissa, ei-hoidollisissa ratkaisuissa. Joka tapauksessa tällaiset tiedot ja näkymät tulee aina suojata sivullisilta esimerkiksi tila- ja kulunhallintaratkaisuilla ja tietojen tarkastelijat on pystyttävä tarvittaessa jäljittämään esimerkiksi työvuorojen hallinnan kautta.

6.8 Asiakas- ja potilastietojärjestelmien pääsynhallinnan ja käytön seurannan käytännöt

Sosiaalihuollon asiakastietoja ja potilastietoja käsittelevien tietojärjestelmien tulee estää ei-sallittu käyttö aina silloin, kun se vain on teknisesti mahdollista, ja omavalvonnan kohteen omien ohjeiden ja toimintatapojen tulee ohjata asiakastietojen käsittelijöitä oikeisiin toimintatapoihin ja tietojenkäsittelyyn.

Palvelunantajan on kerättävä lokitiedot asiakasrekisterikohtaisesti kaikesta asiakastietojen käytöstä ja luovutuksesta seurantaa ja valvontaa varten (asiakastietolaki 25 §). Asiakaskohtaisten tietojen tarkastelusta on jäätävä lokimerkinnät tietojen käytöstä. Lokitiedot on kerättävä, jos tietojärjestelmän käyttö edellyttää tunnistautumista tai muuta kirjautumista.

Lokitietojen käyttötarkoituksena on tietojärjestelmissä olevien tietojen käytön ja luovutuksen seuranta sekä tietojärjestelmän teknisten virheiden selvittäminen (asiakastietolaki 25 § ja viranomaistoiminnassa myös tiedonhallintalaki 17 §). Lokitietojen luomisen ja käsittelyn prosessin tulee taata riittävällä tasolla, että tarpeelliset lokit syntyvät ja pysyvät muuttumattomina ja todistusvoimaisina.

Sosiaali- ja terveydenhuollon palvelunantajan on seurattava ja valvottava, että asiakas- ja potilastietojärjestelmissä, potilastiedon arkistossa, sosiaalihuollon asiakastiedon arkistossa ja reseptikeskuksessa olevia tietoja voivat katsella ja käsitellä vain siihen oikeutetut henkilöt. Käytön seurannan tulee perustua käytönhallintaa varten laadittuihin yhtenäisiin ammattiryhmä- ja tehtäväkohtaisiin käyttövaltuuslinjauksiin ja käyttäjärooleihin (ks. luku 6.7).

Omavalvonnan kohteella on oltava tietosuojaan ja asiakastietojen käsittelyn valvontaan liittyvä seuranta- ja valvontasuunnitelma, joka voi sisältyä tietoturvasuunnitelmaan. Suunnitelmassa otetaan kantaa vähintään siihen, miten tehdään säännöllistä henkilötietojen käytön seurantaa ja miten toimitaan tilanteissa, joissa väärinkäytöksiä ilmenee. Seuranta- ja valvontasuunnitelma voi olla esimerkiksi vuosikohtainen. Tietosuojan ja asiakastietojen käytön omavalvontaa toteutetaan käytännössä suunnitelman kautta. Asiakastietojen käytönvalvonnan raportoinnissa voidaan hyödyntää tietotilinpäätösmenettelyä tai muuta vastaavaa vuosittaista raportointia, jolla voidaan täyttää myös EU:n yleisen tietosuoja-asetuksen mukaista rekisterinpitäjän osoitusvelvollisuutta.

Lokien hallinnan ja käytön seurannan yksityiskohtaiset toimintakäytännöt, kuten esimerkiksi asiakkaiden ja viranomaisen tietopyyntöihin vastaaminen, lokiraporttien kokoaminen ja hallinta sekä valvontatoiminnassa mukana olevien henkilöiden roolit tulee kuvata joko tietoturvasuunnitelmaan tai erillisiin dokumentteihin.

On myös kuvattava yksityiskohtaiset toimintatavat, kuinka menetellään, mikäli käyttölokitiedoista paljastuu virhetilanteita tai epäilyjä rikkomuksista tai epäasianmukaisesta asiakastietojen käytöstä. Lisäksi tulee kuvata toimintamalli ja käytännön menettelyt rekisterinpitäjän ja Kelan välisen luovutuslokirekisterin tietojen luovuttamisesta rekisterinpitäjälle.

6.9 Fyysinen turvallisuus osana tietojärjestelmien käyttöympäristön turvallisuutta

Omavalvonnan kohteen on kiinnitettävä huomiota tietosuojan ja tietoturvan takaavaan fyysiseen käyttöympäristöön, joissa asiakastietoja käsitellään. Omavalvonnan kohteen tulee tarkastella toimitiloja ja niiden tilaratkaisu-, sisustus-, äänieristys- tai muita vastaavia toimenpiteitä, joilla voidaan vaikuttaa tietoturvallisuuteen. Lisäksi on huolehdittava palvelinten käyttöympäristön fyysisestä turvallisuudesta.

Tietoturvallisen käyttöympäristön varmistamiseksi tulee ottaa huomioon mm. näyttöjen, työasemien ja tulostimien sijoittelu sekä niiden suojaaminen sivullisilta. Kokonaisuuteen liittyy tekninen ja fyysinen kulunvalvonta ja mahdolliset fyysisen pääsyn rajoittamistoimenpiteet. Tietoturvasuunnitelmassa on yleisellä tasolla kuvattava, kuinka nämä seikat on otettu huomioon ja mistä on tarvittaessa saatavilla yksityiskohtaisempaa tietoa.

Tietoturvasuunnitelmassa on lisäksi kuvattava, miten omavalvonnan kohteen mahdollisesti käytössä olevien liikuteltavien asiakastietoja sisältävien laitteiden tietosuojasta ja tietoturvasta on huolehdittu ja miten se on todennettavissa.

Tietoturvasuunnitelmassa tulee myös kuvata, kuinka hallitaan ja suojataan ulkoisten tallennusvälineiden käyttöä sekä oman henkilökunnan että ulkopuolisten osalta.

Tietojärjestelmistä paperille tulostettavien sosiaalihuollon asiakastietojen ja potilastietojen asianmukaisesta säilyttämisestä ja hävittämisestä tulee olla kuvattuna menettelytavat, joilla estetään se, etteivät sivulliset saa haltuunsa omavalvonnan kohteelta asiakastietoja. Turvatulostuksen käyttäminen on suositeltavaa perinteisten tulostusratkaisujen sijaan.

Arkistotoimella tulee olla tehtäviinsä nähden asianmukainen ja riittävän tilava paloturvallinen fyysinen toimintaympäristö. Asiakastietoja sisältävien tulosteiden hävittämiskäytäntö tulee suunnitella, toteuttaa ja kouluttaa kaikille asiakastietojen tulosteita käsitteleville työntekijöille. Turvallisuusluokiteltujen ja salassa pidettävien paperitulosteiden hävittäminen tulee olla henkilökunnalle ohjeistettu ja käytännössä mahdollistettu riittävillä määrillä lukittavia säilytysastioita ja/tai käyttötarkoitukseen sopivia, riittävän turvaluokan ominaisuuksilla varustettuja niin kutsuttuja ristiin leikkaavia paperisilppureita.

6.10 Työasemien, mobiililaitteiden ja käyttöympäristön tukipalveluiden hallinta

Tietoturvasuunnitelmassa on kuvattava, miten tietojärjestelmien käyttöympäristössä huolehditaan asiakas- ja potilastietojärjestelmien käytössä olevien työasemien ja mobiililaitteiden hallinnasta tietoturvallisuuden näkökulmasta. Tietoturvasuunnitelmassa tai siihen liittyvissä dokumenteissa on myös kuvattava, miten laitteiden ja palvelujen virusturva- ja haittaohjelmien suojaamisen ohjelmistojen toimivuus ja päivitykset on käytännössä varmistettu, ja miten muut suojauskäytännöt on järjestetty, kuten esimerkiksi laitteiden käyttäjätunnukset, salasanat, PIN-koodit, SIM-korttien hallinta sekä kadonneiden mobiililaitteiden etälukitseminen ja/tai tyhjentäminen.

Lisäksi tietoturvasuunnitelmassa tulee kuvata, kuinka huolehditaan yleisistä käyttöympäristön tukipalveluista, kuten esimerkiksi käyttöjärjestelmän päivityksistä ja varusohjelmistojen (esimerkiksi MS Office) päivityksistä. Kokonaisuuteen liittyy mahdolliset niin kutsutut koventamiset sekä käyttöjärjestelmä- että varusohjelmistojen yhteentoimivuuden varmistaminen ja toimivuuden seuranta sosiaali- ja terveydenhuollon tietojärjestelmien kanssa.

Keskeistä on kuvata tietoturvasuunnitelmaan ja/tai sen liitteisiin ainakin edellä mainittujen asioiden osalta käyttöympäristön kokonaisuus ja se, mitkä seikat ovat palvelunantajan omaa toimintaa ja mitkä

sopimuskumppanien vastuulla. Myös mahdolliset alihankkijat tulee kuvata. Asiat tulee ilmaista toimijoiden välisissä sopimuksissa riittävän tarkasti ja käytännönläheisesti, jotta muun muassa vastuu- ja työnjakokysymykset eri tilanteissa ovat sopimuskumppaneiden välillä selkeitä omavalvonnan kohteen tietoturvallisen ja sujuvan toiminnan varmistamiseksi.

6.11 Alusta- ja verkkopalvelujen tietoturvallinen käyttö tietosuojan ja varautumisen kannalta

Sosiaali- ja terveydenhuollon toimijoiden tulee olla tietoisia kaikista käytössään olevista alusta- ja verkkopalveluista. Verkon kautta käytettävien palvelujen osalta on oltava selvää, mistä palveluista vastaa palvelunantaja itse, mistä palveluista vastaa tietojärjestelmäpalvelun tuottaja ja mistä kolmas osapuoli.

Sosiaali- ja terveydenhuollon toimijoiden tulee varmistaa tietosuojasäädösten, kuten EU:n yleisen tietosuoja-asetuksen mukaan toimiminen. Henkilötietojen siirto ja säilytys EU/ETA-alueella on pääsääntöisesti sallittua vastaavilla suojatoimenpiteillä kuin Suomessa.

Tietoturvasuunnitelmassa tulee kuvata sekä palvelimien että niiden edellyttämien käyttöympäristöjen tietoturvallisuustoimenpiteet, joita ovat esimerkiksi tietoverkon suojaaminen sekä tietojen kahdennus-, ylläpito- ja huoltotoimenpiteet.

Tietoturvasuunnitelmassa on kuvattava, kuinka huolehditaan tietoliikenneasioiden käytännön järjestelyistä, palveluiden saatavuudesta, verkkojen tietoturvallisuuskäytänteiden järjestämisestä, verkkolaitteiden ja niiden komponenttien, laiteohjelmistojen sekä langattomien verkkojen ja reitittimien päivityksistä ja tietoturvasta, etäyhteyksiin ja etätyöskentelyyn liittyvistä ohjeistuksista sekä etähallintaratkaisuista.

Tietoliikenteen ja viestinvälityksen tietosuojaa ja tietoturvaa koskevat vaatimukset ja vastuiden määrittely tulee olla osa palvelunantajan ja tietoliikenne- tai viestinvälitysoperaattorin välistä sopimusta.

Tietojärjestelmät ja niiden käyttöympäristöt tulee pitää kunnossa ja sosiaali- ja terveydenhuollon toimijoiden tulee varautua toimimaan poikkeustilanteissa ilman tietojärjestelmiä.

Alusta- ja verkkopalvelujen, kuten esimerkiksi pilvipohjaisten ratkaisujen, etähallintapalvelujen, palvelinvuokrauksen, palvelinhallinnan, varmistuspalveluiden ja konesalipalvelujen osalta on kuvattava, mitä ratkaisuja on käytössä, sekä kuinka niihin liittyvissä sopimuksissa ja käytännöissä on varmistettu seuraavat seikat:

- Tietojen siirron riskitaso on arvioitava (EU:n yleisen tietosuoja-asetuksen mukainen vaikutustenarviointi). Jos tietoja siirretään kolmansiin maihin, on noudatettava lainsäädännössä säädettyjä, hyväksyttyjä siirtoperusteita ja toteutettava tarvittavat organisatoriset, sopimuspohjaiset ja tekniset suojatoimet tapaus- ja maakohtaisesti.

- Arkaluonteisten ja salassa pidettävien sosiaalihuollon asiakastietojen tai potilastietojen laaja tietojoukko on suojattava siten, ettei sivullisilla ole pääsyä salaamattomiin asiakastietoihin. Mikäli tietoja välitetään tai siirretään kolmansien osapuolien palveluihin, asiakastietojen laajamittaisessa säilytyksessä salausavaimet pitää olla palvelunantajan ja/tai tietojärjestelmäpalvelun tuottajan hallussa. Alustapalvelun toimittajalla ja/tai siihen liittyvässä käyttöympäristössä ei saa olla mahdollista päästä käsiksi salausavaimiin.

- Erityisesti kriittisissä palveluissa kuten julkisen terveydenhuollon päivystysvastuulla olevat palvelut varaudutaan tietojen käsittelyyn normaalista poikkeavissa olosuhteissa. Varautumisessa on huomioitava

keskeisimmät riskiuhat mukaan lukien tiedon hallinnointi tilanteissa, joissa yhteiskunnan verkkoyhteydet on rajoitettu Suomen maantieteellisten rajojen sisäpuolelle.

- Käytössä olevia alusta- ja verkkopalveluja seurataan säännöllisesti muun muassa toimivuuden, tietoturvallisuusriskien, häiriötilanteiden ja käyttöehtomuutosten näkökulmasta. Tarvittaessa sopimusten ja käytäntöjen päivittäminen muuttunutta tilannetta vastaavaksi.

- Palvelunantajalla ja tälle palveluja tuottavilla toimijoilla on oltava tietojärjestelmien, osajärjestelmien, laitekomponenttien sekä verkkojen ja huolto-, päivitys- ja uusimissuunnitelma ja selkeä toimintamalli huoltotoimenpiteisiin liittyvään päätöksentekoon. Lisäksi tulee huolehtia näihin liittyvien päivitystarpeiden seurannasta.

- Tietojärjestelmät täyttävät niihin kohdistuvat olennaiset tietoturvavaatimukset myös siltä osin kuin niiden toteutus tai käyttö nojautuu kolmansien osapuolten alusta- tai kapasiteettipalveluihin.

Nämä edellä mainitut seikat tulee erityisesti huomioida ja varmistaa palvelunantajan ja tietojärjestelmäpalvelun tuottajan välisissä sopimuksissa.

6.12 Kanta-palvelujen liittymisen ja käytön tietoturvakäytännöt

Jos omavalvonnan kohde on liittynyt Kanta-palvelujen käyttäjäksi, on tietoturvasuunnitelmassa selvitettävä, miten valtakunnallisten tietojärjestelmäpalveluiden tietoturvallisen käytön edellyttämät vaatimukset varmistetaan. Vaatimusten toteuttamistapa on kuvattava tietoturvasuunnitelmassa ja se on oltava todennettavissa valvontaviranomaisen järjestämissä valvontatilanteissa.

Palvelunantajan on huolehdittava siitä, että henkilöstö hallitsee Kanta-palvelujen käyttöön liittyvät toimintamallit ja periaatteet sekä tietää väärinkäytösten seuraamukset. Tietoturvasuunnitelmassa on selvitettävä, miten asiakkaiden informointi Kanta-palveluista ja tietojen käytöstä tapahtuu ja on palvelunantajan todennettavissa.

Tietoturvasuunnitelmaan on kuvattava, miten Kanta-palvelujen käyttäminen on otettu huomioon henkilöstön koulutusmateriaaleissa, koulutuksissa ja ohjeistuksissa.

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

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

Ohjeistuksessa tulee muun muassa huolehtia siitä, kuinka varmistetaan asiakirjojen valmiiksi merkitseminen ja viivytyksetön arkistointi Kanta-palveluihin. Asiakirjojen arkistoimattomuus Kanta-palveluihin tai merkittävät viiveet aiheuttavat riskejä tiedon eheyden, asiakkaan lakisääteisten oikeuksien sekä sosiaali- ja terveydenhuollon ammattilaisten oikeusturvan näkökulmasta.

Häiriötilanteiden varalta omavalvonnan kohteella tulee olla selkeät menettelytavat ja vastuut Kanta-palvelujen ja niihin liittyvien järjestelmien virhetilanteiden tilanteiden havainnointiin, tiedottamiseen, korjaamiseen ja jälkihoitoon. Palvelunantajan ja tietojärjestelmäpalvelun tuottajan välisissä sopimuksissa tulee kuvata vastuut esimerkiksi kiireellisissä häiriötilanteissa tai tietoturvaloukkaustilanteissa (kuten esimerkiksi asiakas- ja viranomaisviestintä ja tarvittavien tapahtumalokitietojen käsittely).

Vastuutahot häiriötilanteiden ilmoittamisesta Kanta-palvelujen tekniseen tukeen on oltava todennettavissa. Palvelunantajan on ilmoitettava Kelalle sen antamien ohjeiden mukaisesti muutoksista palvelunantajan käyttämissä tietojärjestelmissä (sisältäen versiotiedot tai muut tietojärjestelmän statusta kuvaavat tiedot).

Omavalvonnan kohteen on kuvattava, kuinka Kanta-palveluista haettujen asiakastietojen käyttöä seurataan. Tämä koskee erityisesti niin sanotun hätähaun käytön seurannan järjestämistä, erityissuojattavien tietojen hakua ja käyttöä sekä ilman teknistä hoitosuhteen varmistusta (ns. erityinen syy) tehtyjä hakuja. Henkilöstön on oltava tietoisia seurannasta ja väärinkäytön seuraamuksista.

Palvelunantajan on varmistettava, että sen toimintaa varten hankittava tai päivitettävä tietojärjestelmä täyttää tietojärjestelmän käyttötarkoitusta vastaavat olennaiset vaatimukset THL:n määräyksen 5/2021 mukaisesti. Palvelunantajan on säännöllisesti seurattava, että THL:n määräyksen 4/2021 mukaisesti luokkaan A1, A2 tai A3 kuuluvilla tietojärjestelmillä ja välityspalveluilla on voimassa oleva todistus tietoturvallisuuden arvioinnista. Kanta-palveluihin liittyvien (erityisesti luokkaan A2 tai A3 kuuluvien) tietojärjestelmien osalta on varmistettava, että järjestelmissä on hyväksytysti yhteistestattu ne ominaisuudet, jotka vastaavat järjestelmän käyttötarkoitusta. Nämä tiedot ovat julkisesti saatavilla Valviran tietojärjestelmärekisteristä. Lisäksi palvelunantajan tulee osaltaan varmistaa, että myös muut kuin Kanta-palveluihin liittyvät sosiaalihuollon asiakastietojen ja potilastietojen käsittelyyn tarkoitetut tietojärjestelmät on ilmoitettu Valviralle ja että tiedot ovat ajan tasalla Valviran tietojärjestelmärekisterissä.

Palvelunantajan on myös määriteltävä menettelytavat käytännön toiminta- ja vastuukysymyksissä niihin tilanteisiin, että tietojärjestelmän tai välityspalvelun todistus tietoturvallisuuden arvioinnista peruutetaan määräajaksi tai kokonaan tai tietojärjestelmän käyttö kielletään tai sen käyttöä rajoitetaan. Tällaiset seikat tulee ottaa ennalta huomioon palvelunantajan, välittäjän ja tietojärjestelmäpalvelun tuottajan välisissä sopimuksissa (vrt. THL:n määräys 5/2021).

Tässä luvussa kuvatut seikat tulee olla tarvittaessa todennettavissa valvontaviranomaisen järjestämissä valvontatilanteissa.

7 Ohjaus ja neuvonta

Terveyden ja hyvinvoinnin laitos ohjaa ja neuvoo pyynnöstä tämän määräyksen soveltamisessa ja tarvittaessa ylläpitää tietoturvasuunnitelman mallipohjaa.

8 Voimaantulo

Tämä määräys tulee voimaan 20. päivänä joulukuuta 2021 ja on voimassa toistaiseksi. Palvelunantajien, välittäjien ja Kansaneläkelaitoksen on päivitettävä aiemmat tietosuojaan, tietoturvallisuuteen ja tietojärjestelmien käyttöön liittyvät omavalvontasuunnitelmansa tietoturvasuunnitelmaksi tämän määräyksen mukaisesti.

Pekka Rissanen
vt. Tiedonhallintajohtaja

Jarmo Kärki
Yksikönpäällikkö

Jakelu

Sosiaali- ja terveydenhuollon palvelunantajat
Apteekit
Välittäjät
Kansaneläkelaitos
Lääkealan turvallisuus- ja kehittämiskeskus Fimea
Sosiaali- ja terveydenhuollon asiakas- ja potilastietojärjestelmien valmistajat ja tietojärjestelmäpalvelujen tuottajat
Sosiaali- ja terveydenhuollon tietohallintopalvelujen ja ICT-palvelujen tuottajat
Sosiaalialan osaamiskeskukset
Sosiaali- ja terveysministeriö
Suomen Kuntaliitto ry
Sosiaali- ja terveysalan lupa- ja valvontavirasto Valvira
Traficom
Traficom/Kyberturvallisuuskeskus
Valtiovarainministeriö
Työ- ja elinkeinoministeriö
Digi- ja väestötietovirasto
Tietosuojavaltuutetun toimisto
Aluehallintovirastot

Tämä määräys on julkaistu viranomaisten määräyskokoelmissa

https://www.finlex.fi/fi/viranomaiset/normi/561001/ (FINLEX® - Viranomaisten määräyskokoelmat: Terveyden ja hyvinvoinnin laitos) ja saatavissa:

Terveyden ja hyvinvoinnin laitoksen kirjaamosta sekä

Internetosoitteesta https://thl.fi/fi/web/tiedonhallinta-sosiaalija-terveysalalla/maaraykset-ja-maarittelyt/maaraykset