Tiedonvälittäjät
Tieto ja tiedonhallinnan ohjaus

Luonnos 16.10.2023

MÄÄRÄYS TIETOTURVASUUNNITELMAAN SISÄLLYTETTÄVISTÄ SELVITYKSISTÄ JA VAATIMUKSISTA

Valtuutussäännökset

Laki sosiaali- ja terveydenhuollon asiakastietojen käsittelystä (703/2023) 77 § 3 momentti

Kohderyhmät

Sosiaali- ja terveydenhuollon palvelunantajat
Apteekit
Välittäjät
Kansaneläkelaitos (Kela)

Voimaantulo

Tämä määräys tulee voimaan 16. päivänä tammikuuta 2024 ja on voimassa toistaiseksi.

Tämä määräys korvaa aiemman Terveyden ja hyvinvoinnin laitoksen (THL) määräyksen THL 3/2021 Tietoturvasuunnitelmaan sisällytettävistä selvityksistä ja vaatimuksista. Laki sosiaali- ja terveydenhuollon asiakastietojen käsittelystä (703/2023) kumoaa aiemman määräyksen antamiseen valtuuttaneen lain sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (784/2021), jonka nojalla annetut alemman asteiset säädökset kumoutuvat.

Sisällys

1 Määräyksen soveltamisala

Tämä määräys perustuu sosiaali- ja terveydenhuollon asiakastietojen käsittelystä annetun lain (703/2023, jäljempänä asiakastietolaki) 77 ja 78 §:ään.

THL:lle on annettu asiakastietolain 77 §:n 3 momentissa valtuus antaa tarkempia määräyksiä 1 ja 2 momentissa tarkoitetuista tietoturvasuunnitelmaan sisällytettävistä selvityksistä ja vaatimuksista sekä tietoturvallisuuden todentamisesta.

Määräys tietoturvasuunnitelmaan sisällytettävistä selvityksistä ja vaatimuksista koskee sosiaali- ja terveydenhuollon palvelunantajia, apteekkeja, välittäjiä ja Kelaa, joiden on laadittava tietoturvaan ja tietosuojaan sekä tietojärjestelmien käyttöön liittyvä tietoturvasuunnitelma.

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

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

Tietoturvasuunnitelman avulla vahvistetaan sosiaali- ja terveydenhuollon toimijoiden tietoturvallisuuskäytäntöjä. Palvelunantajien, apteekkien, välittäjien ja Kelan laatimissa tietoturvasuunnitelmissa on oltava selvitykset siitä, miten asiakastietojen käsittelyyn ja tietojärjestelmiin liittyvät vaatimukset varmistetaan asiakastietolain 77 §:n 1 momentin kohtien 1–9 mukaisesti.

Tietoturvallisuuden omavalvonnan kohteen velvollisuutena on toimia tietoturvasuunnitelman mukaisesti, säännöllisesti ylläpitää suunnitelmaa ja seurata aktiivisesti sen toteutumista. Kyse on jatkuvasta ja säännöllisestä riskien hallinnasta, asianmukaisten tietoturvallisuuden ja asiakastietojen käytäntöjen varmistamisesta sekä niiden toteuttamisesta.

2 Määritelmät

Tämän määräyksen keskeiset käsitteet ja niiden määritelmät ovat seuraavat:

- Asiakastieto (asiakastietolaki 3 § 1 mom. 6 kohta):
    - potilastieto ja sosiaalihuollon asiakastieto.
- Palvelunantaja (asiakastietolaki 3 § 1 mom. 11 kohta[1]):
    - viranomainen, julkisoikeudellinen yhteisö ja yksityinen elinkeinonharjoittaja, joka järjestää tai toteuttaa sosiaalipalveluja tai terveyspalveluja. Palvelunantaja tarkoittaa myös työterveyshuoltolain (1383/2001) 7 §:n 1 momentin 2 kohdassa tarkoitettua työnantajaa.
- Apteekki (asiakastietolaki 3 § 1 mom. 12 kohta):
    - lääkelain (395/1987) 38 §:n 1 kohdassa tarkoitettu apteekki.
- Hyvinvointisovellus (asiakastietolaki 3 § 1 mom. 18 kohta):
    - sovellus, joka liittyy omatietovarantoon ja jolla käsitellään hyvinvointitietoa, sekä sovellus, johon henkilö voi saada asiakastietonsa valtakunnallisesta asiakastietovarannosta, reseptikeskuksesta tai tiedonhallintapalvelusta.
- Tietojärjestelmä (asiakastietolaki 3 § 1 mom. 19 kohta):
    - ohjelmisto, järjestelmä tai osajärjestelmä, jota valmistajan suunnittelemien ominaisuuksien mukaisesti on tarkoitettu käytettäväksi asiakasasiakirjojen sähköiseen käsittelyyn, asiakirjojen tallentamiseen valtakunnallisiin tietojärjestelmäpalveluihin tai valtakunnallisiin tietojärjestelmäpalveluihin liittämiseen tai jolla sosiaali- ja terveydenhuollon ammattihenkilö voi hyödyntää hyvinvointitietoja.
- Tietojärjestelmäpalvelun tuottaja (asiakastietolaki 3 § 1 mom. 20 kohta):
    - taho, joka tarjoaa tai toteuttaa palvelunantajalle asiakastietolain 3 §:n 1 momentin kohdassa 19 tarkoitettua tietojärjestelmää ja joka vastaa tietojärjestelmän valmistajana, valmistajan lukuun tai yhden tai useamman valmistajan puolesta tietojärjestelmälle asetetuista vaatimuksista.
- Tietojärjestelmä valmistaja (asiakastietolaki 3 § 1 mom. 21 kohta):
    - taho, joka on vastuussa sosiaali- ja terveydenhuollon tietojärjestelmän suunnittelusta ja valmistuksesta.

[1] Asiakastietolain muutos on valmistelussa STM:ssä. Muutos koskee tätä määritelmää, josta tällä hetkellä puuttuvat muutkin yksityiset sosiaali- ja terveyspalvelujen järjestäjät ja tuottajat kuin elinkeinoharjoittajat.

- Välittäjä (asiakastietolaki 3 § 1 mom. 22 kohta):
    - palvelunantajan tietojärjestelmäpalvelujen tuottamisessa, tietojärjestelmien teknisen tai fyysisen käyttöympäristön toteuttamisessa tai valtakunnallisiin tietojärjestelmäpalveluihin liittymisessä käyttämä palveluntarjoaja, jolla on tässä roolissa mahdollisuus nähdä ylläpitotoimien yhteydessä tai muutoin salaamattomia asiakastietoja.
- Sertifiointi (asiakastietolaki 3 § 1 mom. 23 kohta):
    - menettely, jolla todennetaan tietojärjestelmän täyttävän sitä koskevat tuotantokäyttöä varten vaadittavat olennaiset vaatimukset. Luokkaan A kuuluvien järjestelmien vaatimusten todentaminen tehdään tietoturvallisuuden arvioinnin ja tarvittaessa yhteistestauksen kautta. Järjestelmälle hyväksytysti tehdystä sertifioinnista tehdään merkinnät valvontaviranomaisen rekisteriin (THL:n määräyksen 4/2024 mukaisesti).
- Valvontaviranomainen (asiakastietolaki 97 § 3 mom.):
    - tietosuojavaltuutettu, Lääkealan turvallisuus- ja kehittämiskeskus (Fimea), Sosiaali- ja terveysalan lupa- ja valvontavirasto (Valvira) sekä aluehallintovirasto (AVI), jotka toimialueellaan ohjaavat ja valvovat niille säädetyn toimivallan mukaisesti osaltaan tämän lain noudattamista.
- Kanta-palvelut:
    - sosiaali- ja terveydenhuollon valtakunnalliset tietojärjestelmäpalvelut, joita ovat asiakastietolain 65 §:n 1 mom. mukaiset palvelut.
- Tietojärjestelmän käyttöympäristö:
    - tekninen, organisatorinen ja fyysinen ympäristö, 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.

3 Vastuut tietoturvan sekä asiakastietojen asianmukaisen käsittelyn varmistamisessa

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

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

Jos tietoturvasuunnitelmaan kuuluvia vastuita on jonkun muun kuin tietoturvallisuuden 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.

Tietoturvallisuuden omavalvonnan kohteella on oltava sopimus asiakastietojen käsittelystä ja tietoturvallisuuden varmistamisesta muiden sen asiakas- tai potilastietojärjestelmiä käyttävien palvelunantajien ja mahdollisten ulkopuolisten ammatinharjoittajien keskinäisten vastuiden osalta. 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 säädetystä poikkeavasti.

Tietoturvasuunnitelman varsinaisen sisällön tai siinä viitatuissa dokumenteissa esitetyn sisällön pohjalta on tarvittaessa pystyttävä todentamaan tietoturvallisuuden omavalvontaan liittyvät asiat:

- tietoturvasuunnitelma on laadittu,
- tietoturvasuunnitelma sisältää suunnitelmalta edellytettävät asiat tämän määräyksen mukaisesti,
- tietoturvasuunnitelmassa on kuvattu, miten suunnitelmaa säännöllisesti päivitetään ja
- miten sen toteutumista seurataan.

Tietoturvallisuuden omavalvonnan kohteen 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.

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

Tämän THL:n määräyksen 3/2024 lisäksi tietoturvasuunnitelman laatimisessa tulee soveltaa THL:n määräystä 5/2024 (ks. erityisesti luku 9) sosiaali- ja terveydenhuollon tietojärjestelmien olennaisista toiminnallisista ja tietoturvavaatimuksista kohdistuen asiakastietojen käsittelyyn tarkoitettuihin tietojärjestelmiin. Palvelunantajan ja apteekin käyttämien tietojärjestelmien on vastattava käyttötarkoitukseltaan niiden toimintaa. Lisäksi palvelunantajan ja apteekin on täytettävä toimintaan liittyvät olennaiset vaatimukset (asiakastietolaki 84 §). Olennaiset vaatimukset voidaan täyttää yhden tai useamman tietojärjestelmän muodostaman kokonaisuuden kautta.

THL:n määräyksen 4/2024 sosiaali- ja terveydenhuollon tietojärjestelmien luokittelusta ja sertifioinnista liitteessä 1 on kuvattu tietojärjestelmien luokittelua käytännön esimerkkeineen.

Tietoturvasuunnitelman laatimisessa suositellaan käytettäväksi tietoturvallisuuden suunnitteluun tarkoitettuja standardeja ja viitekehyksiä, esimerkiksi ISO 27000-sarjan standardeja tai Digi- ja väestötietoviraston julkaisemaa Digitaalisen turvallisuuden arkkitehtuuri -viitekehystä.

Tämän määräyksen kohdealueena ei ole sosiaali- ja terveystietojen toissijaisesta käytöstä annetun lain (552/2019, toisiolaki), mukaiset käyttötarkoitukset. Palvelunantajan on kuitenkin mahdollista huomioida myös toisiolakiin liittyviä tiedonkäsittelyn vaatimuksia tietoturvasuunnitelmassaan. Joillakin tietojärjestelmillä voi olla sekä asiakastietolain että toisiolain mukaisia käyttötarkoituksia.

Tämän määräyksen kohdealueena eivät ole lääkinnällisten laitteiden säädökset. Jos tietojärjestelmä täyttää lääkinnällisen laitteen määritelmän, on otettava huomioon sekä asiakastietolaki että lääkinnällisiä laitteita koskeva säädökset, kuten Euroopan parlamentin ja neuvoston asetus (EU) 2017/745[2].

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. asiakastietolaissa) ei toisin säädetä.

[2] 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.

5 Yleistä tietoturvasuunnitelmasta

Asiakastietolain 77 §:n mukaisesti palvelunantajan, apteekin, välittäjän ja Kelan on laadittava tietoturvaan ja tietosuojaan sekä tietojärjestelmien käyttöön liittyvä tietoturvasuunnitelma.

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, julkisuuslaki) salassapitoa koskevat säännökset (24 § 1 mom. 7 kohta).

Tietoturvasuunnitelmassa varmistetaan, että palvelunantajan ja apteekin henkilökunta hallitsee tietojärjestelmien käytön ja ottaa huomioon asiakastietojen salassapitoon ja tietoturvaan liittyvät vaatimukset sekä ymmärtää väärinkäyttöön liittyvät seuraamukset. Tietoturvasuunnitelman vaatimusten tarkoituksena on varmistaa, että tietojärjestelmiä asentaa, ylläpitää ja päivittää vain henkilö, jolla on siihen tarvittava ammattitaito ja asiantuntemus (ks. luku 6.6).

Henkilön luotettavuus tulee varmistaa tiedonhallintalain 12 §:ssä tarkoitetulla tavalla, jos henkilö tehtävissään pääsee käsittelemään asiakastietoja tai jos henkilö muuten tehtävissään voi vaarantaa sosiaali- ja terveydenhuollon jatkuvuuden kannalta kriittisten tietojärjestelmien toimintaa (ks. luku 6.6).

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.

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

Asiakastietolain 78 §:n mukaisesti sosiaali- ja terveydenhuollon palvelunantajan vastaavan johtajan ja apteekkarin on huolehdittava, että 77 §:ssä tarkoitettu tietoturvasuunnitelma laaditaan, sitä säännöllisesti ylläpidetään ja sitä noudatetaan. Osana suunnitelmaa on kuvattava, kuinka suunnitelma toteutetaan ja tietoturvallisuuden omavalvonta käytännössä järjestetään.

Kelan ylläpitämien valtakunnallisten tietojärjestelmäpalvelujen käytön osalta tietoturvasuunnitelmassa on selvitettävä myös tietosuojan ja tietoturvan erityiskysymykset. Palvelunantajan on tietoturvasuunnitelmassa selvitettävä, miten tietoturvallisen käytön ja tietosuojan edellyttämät vaatimukset on varmistettu ja miten tietosuojan ja tietoturvan erityiskysymykset on järjestetty ennen liittymistään Kanta-palvelujen käyttäjäksi (ks. luku 6.12).

Tietoturvasuunnitelma on käytännön työväline, jolla hahmotetaan tietoturvallisuuden kokonaiskuvaa ja toteutetaan asiakastietojen käsittely hyvien käytäntöjen mukaisesti. Tietoturvasuunnitelman mukaiset selvitykset ja käytännöt voidaan yhdistää muihin palvelunantajan tietosuojaa ja tietoturvallisuutta ohjaaviin menettelyohjeisiin, laatukäsikirjoihin tai tietoturvapolitiikkoihin.

Kuvaukset voivat tarvittaessa olla tietojärjestelmäkohtaisia tai yhteisiä useille saman suunnitelman piirissä toimiville tahoille. Kaikkien kuvausten ei tarvitse sisältyä tietoturvasuunnitelmaan, vaan suunnitelmassa voidaan viitata erillisiin saatavilla oleviin kuvauksiin, esimerkiksi tietoturvallisuuden omavalvonnan kohteen tietoturvaohjeisiin tai tietojärjestelmäsalkun kuvauksiin.

Tietoturvasuunnitelma on tietoturvallisuuden omavalvonnan kohteen dokumentti, jolla rekisterinpitäjä voi täydentää EU:n yleisen tietosuoja-asetuksen[3] mukaista osoitusvelvollisuuttaan (5 artikla 2 kohta). Rekisterinpitäjän osoitusvelvollisuutta voidaan toteuttaa esimerkiksi dokumentoimalla tehtyjä toimenpiteitä, laatimalla vaikutustenarviointi, tietotilinpäätös ja seloste käsittelytoimista. Osoitusvelvollisuutta voidaan toteuttaa myös muilla vastaavilla menettelyillä, joilla osoitetaan rekisterinpitäjän ja henkilötietojen käsittelijän toiminnan säädöstenmukaisuus.

Tietoturvasuunnitelman on katettava kaikki tietoturvallisuuden omavalvonnan kohteen käyttämät asiakastietojen käsittelyyn tarkoitetut tietojärjestelmät. Tietoturvallisuuden omavalvonnan kohteen on varmistettava tietojärjestelmiin liittyvien olennaisten vaatimusten toteutuminen tietojärjestelmiä hankkiessaan, kehittäessään ja käyttäessään. Valviran tietojärjestelmärekisterissä olevia tietoja voi hyödyntää olennaisten vaatimusten toteutumisen varmistamisessa. Tietojärjestelmäpalvelun tuottaja tai tietojärjestelmän valmistaja vastaa olennaisten vaatimusten toteuttamisesta tietojärjestelmään ja tietojärjestelmien luokittelusta ja sertifioinnista.

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

[3] 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).

6 Tietoturvasuunnitelmaan sisällytettävät selvitykset ja vaatimukset

Asiakastietolain 77 §:n 1 momentin kohtien 1–9 ja 77 §:n 2 momentin mukaisesti tietoturvasuunnitelmassa on oltava selvitykset siitä, miten asiakastietojen käsittelyyn ja tietojärjestelmiin liittyvät vaatimukset varmistetaan.

Tietoturvasuunnitelmassa on kuvattava tämän luvun 6 mukaiset alakohdat 6.1–6.12 tietoturvallisuuden omavalvonnan kohteen omaan toimintaan ja käytössä oleviin tietojärjestelmäratkaisuihin liittyen.

Tietoturvasuunnitelmaan on mahdollista täydentää asiakastietolain 77 §:n vaatimusten lisäksi myös muita tietoturvallisuuden omavalvonnan kohteen kannalta olennaisia asioita.

Tietoturvasuunnitelmassa voidaan viitata olemassa oleviin erikseen ylläpidettäviin ohjeisiin ja dokumentteihin. Olennaista on, että suunnitelmasta selviää, mistä dokumentaatio on löydettävissä tai miten vaatimuksen täyttyminen on todennettavissa. Vaadittavat asiakokonaisuudet ja toimintatavat on mahdollista kuvata suoraan tietoturvasuunnitelmaan, jos muuta valmista dokumentaatiota ei ole olemassa tai saatavissa.

6.1 Yleiset tietoturvakäytännöt

Asiakastietolain 77 §:n 1 momentin kohdan 5 mukaan tietojärjestelmän käyttöympäristön on sovelluttava tietojärjestelmien asianmukaiseen ja tietoturvan sekä tietosuojan varmistavaan käyttöön. Käyttöympäristöön ja tietojärjestelmiin kohdistuvien riskien hallinnasta on huolehdittava.

Tietoturvasuunnitelmaan tulee kuvata tietoturvallisuuden 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 säännöllisesti tarkistetaan ja kehitetään, miten tietoturvallisuustyössä on jaettu ja organisoitu vastuut toiminnan tavoitteiden saavuttamiseksi sekä riskien hallitsemiseksi.

Asiakastietolain 78 §:n 4 momentin mukaan tietosuojavastaavan nimittämisestä sekä tietosuojavastaavan asemasta ja tehtävistä säädetään yleisen tietosuoja-asetuksen 37–39 artiklassa. Tietoturvallisuuden omavalvonnan kohteella on siten oltava nimitettynä yksi tai useampi tietosuojavastaava. Tietosuojavastaavalla tulisi olla selkeä ja dokumentoitu tehtäväkuva, jossa otetaan huomioon asiakastietojen käsittelyyn liittyvät velvoitteet. Tietosuojavastaavalla tulisi olla tehtävään soveltuva osaaminen ja riittävät resurssit hoitaa tehtävää tietoturvallisuuden omavalvonnan kohteessa ottaen huomioon rekisterinpitoon ja henkilötietojen käsittelyyn liittyvät vastuut ja velvoitteet, organisaation koko ja toiminnan laajuus.

Tietoturvasuunnitelmaan tulee myös kuvata etä- ja hybridityöohjeistukset liittyen henkilöstön työskentelyyn etänä (esimerkiksi kotitoimistossa) ja erilaisissa liikkuvissa potilas- ja asiakastyötehtävissä.

Tietoturvasuunnitelman tavoitteena on varmistaa, että tietoja käyttävät ja tuottavat asiakastietojen käsittelijät ymmärtävät asiakastietojen käsittelyyn liittyvät vastuut ja osaavat kulloinkin toimia siten, että asiakastietojen eheys, luottamuksellisuus, saatavuus, kiistämättömyys ja autenttisuus toteutuvat. Tietoturvasuunnitelmassa voidaan erottaa eri työtehtävissä toimivan henkilöstön tarvitsemia tietosisältöjä toisistaan. Esimerkiksi tietohallinnon asiantuntijoiden ja kehitys- ja hankintatoimen henkilöstölle suunnattu sisältö tulisi vastata juuri heidän työtehtäviinsä liittyviä tarpeellisia tietoja.

6.2 Menettelyt virhe- ja ongelmatilanteissa sekä jatkuvuudenhallinta

Tietoturvallisuuden omavalvonnan kohteen on varauduttava virhe- ja ongelmatilanteisiin, tietoturvapoikkeamiin, tietoturvaloukkauksiin sekä muihin häiriöihin, jotta asiakastietojen käsittelyn jatkuvuus voidaan erilaisissa olosuhteissa hallita ja turvata. Tietoturvallisuuden omavalvonnan kohteella tulee olla virhe- ja ongelmatilanteiden varalle ennalta määritellyt ja selkeät toimintatavat, toimintaohjeet ja vastuut kyseisten tilanteiden ennalta havainnointiin, tiedottamiseen, korjaamiseen ja tilanteista toipumiseen (tietoturvapoikkeaman hallinta - incident management).

Tietojärjestelmät on mahdollista luokitella kriittisyyden perusteella. Tämä voi vaikuttaa varautumisen toteuttamisen käytäntöihin. Nämä asiat voivat olla kuvattuna suoraan tietoturvasuunnitelmaan tai tietoturvasuunnitelmasta viitattaviin erillisiin jatkuvuus-, toipumis- ja varautumissuunnitelmiin, joiden mukaisia menettelyitä noudatetaan virhe- ja ongelmatilanteissa.

Tietoturvallisuuden omavalvonnan kohteen tulee suunnitella tietojärjestelmähäiriöistä toipumisen edellyttämät toimenpiteet, niihin liittyvät ohjeet ja hankinnat. Normaalista poikkeavien tilanteiden ja poikkeusolojen varalle suunniteltuja menettelytapoja tulee säännöllisesti läpikäydä, testata ja tarkistaa, jotta tarpeellisten ohjeiden saatavuus on todella turvattu käytännön erityistilanteissa. Suunniteltuja käytäntöjä olisi suositeltavaa harjoitella esimerkiksi kerran vuodessa. Pelkästään kirjallinen läpikäynti erityistilanteiden varalle ei ole riittävää.

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 tietoturvallisuuden omavalvonnan kohteen on mahdollista saada käyttöönsä häiriötilanteesta yksityiskohtaista seurantatietoa, esimerkiksi tapahtumalokeja aikaleimoineen tilanteen ja tapahtuneen selvittämiseen.

Tietoturvallisuuden omavalvonnan kohteen on määriteltävä tärkeimpien tietojärjestelmien ja niiden komponenttien kriittisyys potilas- ja asiakasturvallisuuden näkökulmasta. Olennaista olisi 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.

Lisäksi on tärkeää suunnitella tietojärjestelmien, laitteiden ja verkkojen huolto, päivitykset ja tarvittaessa niiden uusiminen. Näin varmistetaan, että tarvittavat komponentti- ja ohjelmistopäivitykset hoidetaan hyvissä ajoin ennen mahdollisia vikaantumisia. Komponenttien kriittisyyttä tulee tarkastella erityisesti asiakas- ja potilasturvallisuuden näkökulmasta. Turvallisuutta uhanneista tapahtumista tulisi kerätä kaikki oleelliset tiedot, jotta toimintaa voidaan kehittää edelleen.

Palvelunantajan tai apteekin tulee ilmoittaa tietojärjestelmäpalvelun tuottajalle tietojärjestelmän ja hyvinvointisovelluksen olennaisten vaatimusten merkittävistä poikkeamista (asiakastietolaki 90 § 1 momentti). Merkittäviä poikkeamia on kuvattu THL:n määräyksen 5/2024 luvussa 10.4.

Palvelunantajan, apteekin, tietojärjestelmäpalvelun tuottajan tai tietojärjestelmän valmistajan, hyvinvointisovelluksen valmistajan, Kelan tai THL:n tulee ilmoittaa Valviralle tietojärjestelmien ja hyvinvointisovellusten merkittävistä poikkeamista erityisesti tilanteissa, joissa poikkeama voi aiheuttaa merkittävän riskin asiakas- tai potilasturvallisuudelle tai tietoturvalle. Merkittävien poikkeamien korjaamiseksi on ryhdyttävä välittömiin korjaaviin toimenpiteisiin. (Asiakastietolaki 90 § 1 momentti.)

Palvelunantajan tai muun tahon on ilmoitettava havaituista olennaisten vaatimusten tietosuojapoikkeamista tietosuojavaltuutetulle. Henkilötietojen tietoturvaloukkauksesta ilmoittamisesta säädetään EU:n yleisen tietosuoja-asetuksen 33 artiklassa. (Asiakastietolaki 90 § 1momentti.) Henkilötietojen tietoturvaloukkausten hallinta tulee olla dokumentoitu joko suoraan tietoturvasuunnitelmaan tai muihin asiakirjoihin tietoturvallisuuden omavalvonnan kohteessa.

Palvelunantajan, apteekin, Kelan ja tietojärjestelmäpalvelun tuottajan tai tietojärjestelmän valmistajan tai välittäjän on ilmoitettava viipymättä Valviralle sellaisesta sen käyttämiin käyttöympäristöihin ja tietoverkkoihin kohdistuvasta merkittävästä tietoturvallisuuteen liittyvästä häiriöstä, jonka seurauksena tietojärjestelmien käyttö ja sosiaali- ja terveyspalveluiden toteuttaminen voi merkittävästi vaarantua. THL voi antaa tarkempia määräyksiä siitä, milloin häiriö on merkittävä, sekä ilmoituksen sisällöstä, muodosta ja toimittamisesta. (Asiakastietolaki 90 § 2 momentti.)

6.3 Henkilöstön koulutus sekä osaamisen ylläpito ja kehittäminen

Tietoturvasuunnitelmassa on kuvattava, 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.

Tietoturvallisuuden 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 todistuksilla, merkinnöillä koulutuksiin osallistumisesta tai mulla organisaatiossa sovitulla tavalla.

Tietoturvasuunnitelmassa on kuvattava, kuinka henkilöstölle koulutetaan ja informoidaan asiakastietojen käsittelyn perusteet. Näitä ovat esimerkiksi asiakastietojen kirjaamisen, käytön ja suojaamisen merkitys, tietojen käsittelijän vastuu ja tietojen käsittelyyn liittyvän tietoturvallisuuden omavalvonnan ja viranomaisvalvonnan olemassaolo ja merkitys.

Tietojen luovutusperusteista säädetään laeissa. Tietoja luovutettaessa tulee selvittää laillinen peruste, jonka nojalla asiakastieto voidaan luovuttaa vastaanottajalle. Lisäksi tulee selvittää, että tiedon vastaanottaja saa asiakastiedon ainoastaan niiltä osin kuin hänellä on lain mukaan oikeus se saada. Asiakastietoja luovuttavien henkilöiden ja käytössä olevissa tietojärjestelmissä on varmistettava, että tietojen luovutuksista syntyy luovutusilmoitus tai luovutusloki. Näihin liittyvä käytännön osaaminen tulee 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 ja/tai tietojärjestelmän valmistajan antaman ohjeistuksen mukaisesti.

Tietoturvasuunnitelmassa on kuvattava, miten varmistetaan, että tietojärjestelmien käyttäjien saatavilla on tarpeelliset ja ajantasaiset organisaation toimintaohjeet (toimintamallit) ja tietojärjestelmien käyttöohjeet. Nämä ohjeet tulee olla vähintään sillä kielellä, jonka osaaminen on vähimmäisvaatimus kyseisessä työtehtävässä toimimiselle. Ohjeiden tulee olla helposti henkilöstön saatavilla ja niiden sijainti on oltava kaikkien tiedossa.

Asiakastietojen käsittelystä tulee olla annettu kirjalliset ohjeet kaikille asiakastietoja käsitteleville työntekijöille. Käyttöohjeiden ja muiden tarvittavien ohjeiden on oltava ymmärrettäviä ja vastattava organisaatiossa käytössä olevien tietojärjestelmien versioita. Ohjeistuksissa tulee pyrkiä yksiselitteisyyteen ja ottaa huomioon erilaiset työtehtävät ja roolit.

Tietoturvasuunnitelmasta tulee käydä ilmi, mistä eri jakelukanavista löytyvät tietojärjestelmäpalvelun tuottajan antamat ohjeistukset ja koulutusmateriaalit. Suunnitelmassa on kuvattava organisaation omat menettelytavat, joilla seurataan tietojärjestelmäpalvelun tuottajan antamien ohjeistusten noudattamista. 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 ja apteekin tulee asiakastietolain 77 §:n 1 momentin 8 kohdan mukaisesti varmistaa, että 79 §:ssä tarkoitetut tietojärjestelmät täyttävät käyttötarkoituksensa mukaiset olennaiset vaatimukset 84 §:n 2 momentin mukaisesti. Palvelunantajan ja apteekkien käyttämien tietojärjestelmien on vastattava käyttötarkoitukseltaan niiden toimintaa ja täytettävä toimintaan liittyvät olennaiset vaatimukset.

Olennaiset vaatimukset voidaan täyttää yhden tai useamman tietojärjestelmän muodostaman kokonaisuuden kautta. Palvelunantajan ja apteekin on osaltaan huolehdittava, että olennaiset vaatimukset täyttyvät hankinnoissa, sopimuksissa ja tietojärjestelmien ylläpidossa. Tietoturvallisuuden omavalvonnan kohde vastaa omassa toiminnassaan olennaisten vaatimusten täyttymisestä. Niiden varmistamiseen liittyvät menettelyt on kuvattava tietoturvasuunnitelmaan.

Tietojärjestelmäpalvelun tuottajan, tietojärjestelmän valmistajan ja hyvinvointisovelluksen valmistajan on toteutettava olennaiset vaatimukset tietojärjestelmiin, joita käytetään palvelunantajan ja apteekin toiminnassa (vrt. THL:n määräys 5/2024). Palvelunantajan ja apteekin tulee sisällyttää tietoturvasuunnitelmaansa tai sen liitteisiin perustiedot ja tarkemmat kuvaukset kaikista sen käytössä olevista, asiakastietolain mukaisista tietojärjestelmistä ja hyvinvointisovelluksista, jotka on tarkoitettu:

- käytettäväksi asiakastietojen sähköiseen käsittelyyn,
- asiakasasiakirjojen tallentamiseen ja ylläpitoon,
- valtakunnallisiin tietojärjestelmäpalveluihin liittämiseen,
- palvelunantajan toiminnassa käytettäviin kansalaissovelluksiin (hyvinvointisovellukset tai digitaaliset asiointipalvelut) tai
- hyvinvointitietojen hyödyntämiseen sosiaali- ja terveydenhuollon ammattihenkilöiden työssä.

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

Tietoturvallisuuden omavalvonnan kohteen on kuvattava tietoturvasuunnitelmaan tai siinä viitatuissa dokumenteissa, mistä löytyy tieto seuraavan tyyppisistä tietojärjestelmistä ja niiden versioista sekä statuksesta, joita tietoturvallisuuden omavalvonnan kohteen toiminnassa käytetään (vrt. THL:n määräys 4/2024):

- 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 (luokittelemattomat), 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 kuvattava tietoturvasuunnitelmassaan, miten varmistetaan, että tietojärjestelmien suorituskyky ja niiden tietoturva- tai tietosuojaominaisuudet eivät vaarannu. Kuvaus koskee Kanta-palveluihin liittyviä tietojärjestelmiä tai niiden käyttöympäristössä hyödynnettäviä muita sovelluksia tai tietojärjestelmiä, joilla tarkoitetaan esimerkiksi tietokoneohjelmia, jotka eivät käsittele asiakastietoja eivätkä siten ole asiakastietolain 79 §:n mukaisia A tai B luokan mukaisia tietojärjestelmiä.

Määräyksen 5/2024 mukaisesti palvelunantajan ja apteekin on huomioitava omassa toiminnassaan ja tietojärjestelmien käyttöönotossa, tuotantokäytössä sekä tietoturvasuunnitelman mukaisessa toiminnassa ne olennaisiin vaatimuksiin kohdistuvat ja sertifioinnissa esiin nousseet havainnot ja edellytykset, jotka vaikuttavat olennaisten vaatimusten toteutumiseen palvelunantajan ja apteekin käyttämissä tietojärjestelmissä. Erityisesti tulee huomioida Valviran tietojärjestelmärekisterin kautta julkaistavat tarkennukset ja muutokset järjestelmien vaatimustenmukaisuudesta (esimerkiksi merkittävät poikkeamat). Jos palvelunantajan toiminnassa käytetään hyvinvointisovelluksia, vastaavat varmistukset on tehtävä myös niiden osalta.

Tietoturvasuunnitelmaan voi sisällyttää myös sellaisia tietoturvallisuuden omavalvonnan kohteessa käytettäviä sovellusohjelmistoja tai tietojärjestelmiä, joissa ei käsitellä asiakastietoja.

6.6 Tietojärjestelmien asennus, ylläpito ja päivitys

Asiakastietolain 81 §:n 1 momentin mukaan 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 4/2024).

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

Tietoturvasuunnitelmassa on kuvattava tietojärjestelmien asennus, ylläpito ja päivitys tietojärjestelmäpalvelun tuottajan ohjeiden mukaisesti. Tietojärjestelmäpalvelun tuottajien kanssa tehtävissä sopimuksissa tulee kuvata tietoturvallisuuden omavalvonnan kohteen käyttöympäristön kannalta olennaiset asiat.

Tietoturvasuunnitelmasta on selvittävä tarvittava ammattitaito ja asiantuntemus, joka vaaditaan tietojärjestelmiä asentavalta, ylläpitävältä ja päivittävältä henkilöstöltä. Myös näiden henkilöiden roolit ja vastuut on määriteltävä suhteessa tietoturvallisuuden omavalvonnan kohteeseen sekä tietojärjestelmäpalvelun tuottajaan.

Tietoturvasuunnitelman vaatimusten tarkoituksena on varmistaa, että tietojärjestelmiä asentaa, ylläpitää ja päivittää vain henkilö, jolla on siihen tarvittava ammattitaito ja asiantuntemus. Henkilön luotettavuus tulee varmistaa tiedonhallintalain 12 §:ssä tarkoitetulla tavalla (esimerkiksi turvallisuusselvitys), jos henkilö tehtävissään pääsee käsittelemään asiakastietoja tai jos henkilö muuten tehtävissään voi vaarantaa sosiaali- ja terveydenhuollon jatkuvuuden kannalta kriittisten tietojärjestelmien toimintaa. (Asiakastietolaki 77 § 1 momentti 7 kohta). Lisäksi tietojärjestelmäpalvelun tuottajan ja tietoturvallisuuden omavalvonnan kohteen välisissä sopimuksissa tulee kuvata edellä mainitut asiat.

Tietojärjestelmien asennukseen, ylläpitoon ja päivityksiin liittyvät asiat tulee sisällyttää joko tietoturvasuunnitelmaan tai erillisiin suunnitelmiin, jotka sisältävät kuvaukset päivitys-, muutoksenhallinta- ja korjausprosesseista. Suunnitelmissa on mahdollista esittää myös kuvaukset luvun 6.2 mukaisista virhe- ja poikkeustilanteisiin liittyvistä menettelytavoista. Päivitysprosessin kuvaamisessa on otettava huomioon etenkin versio- ja korjauspäivitykset ja muiden muutosten mahdollisesti vaatimat menettelyt. Muutoksenhallintaprosessiin liittyy esimerkiksi tietojärjestelmien muutosten ja uusien versioiden testaus- ja hyväksymismenettelyiden kuvaaminen. 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, kuinka käyttövaltuuksia hallinnoidaan asiakas- tai potilastietojärjestelmien tai ulkoisen tietojärjestelmän, esimerkiksi identiteetin ja pääsynhallinta (IAM) -järjestelmän avulla.

Asiakastietolain 9 §:n mukaan palvelunantajan ja apteekin on määriteltävä käyttöoikeudet sosiaali- ja terveydenhuollon asiakastietoihin kaikille niille työntekijöilleen, joiden työtehtävien hoitaminen edellyttää asiakastietojen käsittelyä. Käyttöoikeudet on määriteltävä siten, että kukin työntekijä pääsee vain niihin asiakastietoihin, jotka ovat työtehtävien tekemisessä välttämättömiä. Asiakastietojen käsittelyn perusteena on oltava tietoteknisesti varmistettu asiakas- tai hoitosuhde tai muu asiakkaan sosiaali- ja terveyspalvelun järjestämiseen ja toteuttamiseen liittyvä tehtävä. Sosiaali- ja terveysministeriön asetuksella säädetään, mitä tietoja sosiaali- ja terveydenhuollon ammattihenkilöt ja muut asiakastietoja käsittelevät henkilöt työtehtävänsä ja annettavan palvelun perusteella saavat enintään käyttää. Palvelunantajan ja apteekin arvioitava kunkin asiakastietoja käsittelevän henkilön kohdalla, mikä on juuri tämän työtehtävässä ja antamassaan palvelussa se tietojoukko, johon on välttämätöntä olla käyttöoikeus.

Tietoturvasuunnitelmassa on kuvattava se, kuinka asiakastietojen käyttövaltuuksissa hyväksytään ja dokumentoidaan sosiaali- ja terveydenhuollon työntekijöiden työtehtävien muutokset. Tietoturvasuunnitelmassa on lisäksi kuvattava henkilöt tai roolit, joilla on oikeus hyväksyä käyttöoikeuspyyntöjä. Käyttövaltuuksia tulee läpikäydä ja seurata säännöllisesti niiden ajantasaisuuden varmistamiseksi.

Käyttövaltuuksien hakemisen, myöntämisen, seurannan, tarkistamisen tai varmistamisen ja poistamisen käytännöt ja toimintamallit on kuvattava. Tietoturvallisuuden omavalvonnan kohteen tulee oman vakituisen henkilöstönsä lisäksi järjestää työtehtävien mukaiset käyttöoikeudet välttämättömiin asiakastietoihin myös organisaation lyhytaikaisille sijaisille, organisaatiossa työskenteleville opiskelijoille (ottaen huomioon opiskelijoita koskevat rajoitukset ammatin harjoittamisessa) sekä ulkopuolisille palveluntuottajille (ostopalvelut). Vastaavasti on kuvattava, kuinka, milloin ja millä tavalla poistuneiden työntekijöiden käyttöoikeudet poistetaan. Erityisen tärkeää on kuvata yksittäisten tai useiden tunnusten pääsyoikeuksien erityisen nopea poistaminen. Asiakastietoon liittyvistä käyttöoikeuksista ja niihin tehdyistä muutoksista tulee pitää kirjaa ja lokia (ks. luku 6.8).

Omavalvonnan kohteen tulee hallinnoida huolellisesti tietojärjestelmän käyttäjien käyttöoikeuksia, jotka liittyvät Kanta-palveluiden osalta sähköiseen lääkemääräykseen, valtakunnalliseen potilastiedon arkistoon, sosiaalihuollon asiakastiedon arkistoon ja muuhun potilastietoihin.

Kaikilla pääkäyttäjillä ja tietojärjestelmäasiantuntijoilla ei lähtökohtaisesti ole oikeutta asiakastietoihin riippumatta siitä, missä asiakastieto sijaitsee. Poikkeuksen tähän muodostaa paikallisiin rekistereihin liittyvät virhetilanteiden selvitykset, joissa pääkäyttäjillä ja tietojärjestelmäasiantuntijoilla on oikeus tarkastaa ja korjata oman organisaationsa tietoja tai sen organisaation tietoja, jonka lukuun he selvityksen aikana toimivat.

Asiakastietolain 8 §:n mukaan asiakastietojen käsittelyssä asiakas, palvelunantaja, apteekki, muu asiakastietojen käsittelyn osapuoli ja näiden edustajat sekä tietotekniset laitteet ja Kanta-palvelut on tunnistettava luotettavasti. Tietoturvasuunnitelmassa on kuvattava tietojärjestelmiä (esimerkiksi asiakas- tai potilastietojärjestelmiä, apteekkijärjestelmiä, paikallisia tietovarantoja tai -altaita ja katselimia) käyttävien henkilöiden tunnistautumistavat ja erilaisten tunnistautumisvälineiden hallinta (toimikortit) sekä voimassaolo.

Tietoturvasuunnitelmassa tulee kuvata työasemiin ja mobiililaitteisin liittyvät kirjautumis- ja tunnistautumiskäytännöt sekä mahdolliset kulunvalvontaan liittyvät pääsynhallinnan ratkaisut. Toimitilojen fyysisen turvallisuuden ratkaisut voidaan yhdistää tietoteknisiin turvakäytäntöihin.

Tietoturvasuunnitelmassa tulee 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.

Käyttäjätunnuksella ja salasanalla tunnistautumista voidaan käyttää ainoastaan paikallisesti tietoturvallisuuden 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.

Kanta-palveluihin kirjautuminen edellyttää vahvaa sähköistä tunnistautumista. Sosiaali- ja terveydenhuollossa toimivien henkilöiden luotettava sähköinen tunnistaminen tapahtuu sosiaali- ja terveydenhuollon toimikorttien varmenteilla.

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

Yhteiskäyttöisten tunnusten käyttö on sallittu tilanteissa, joissa tarkastellaan organisaation resurssien käyttöä tai muita prosesseihin liittyviä ei-tunnisteellisia, yksittäisiin henkilöihin liittymättömiä tietoja tai yhteenvetotietoja useista asiakkaista. Useat käyttäjät voivat tarkastella ja käsitellä näkymiä, joissa on tunnisteellisia asiakastietoja. Tällaisia ovat esimerkiksi osaston potilaspaikkojen koontinäkymät tai vastaavat käytännön työn kannalta välttämättömät potilashallinnolliset, ei-hoidolliset ratkaisut. 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

Asiakastietolain 10 §:n mukaan tietojärjestelmistä kerättävillä lokitiedoilla seurataan tietojen käyttöä ja luovutuksia sekä tiedonhallintalain 17 §:n mukaisesti selvitetään viranomaistoiminnassa tietojärjestelmän teknisiä virheitä. Tiedonhallintalain 17 §:ssä säädetään viranomaisten velvollisuudesta lokitietojen keräämiseen. Koska myös yksityiset palvelunantajat liittyvät valtakunnallisten tietojärjestelmäpalveluiden käyttäjäksi, säädetään asiakastietolaissa käytön ja luovutuksen seurannasta niin, että samat velvoitteet koskevat kaikkia sosiaali- ja terveydenhuollon palvelunantajia. Käytön ja luovutuksen seurannasta säädetään myös tiedonhallintalakia tarkemmalla tasolla.

Lokitietojen luomisen ja käsittelyn prosessin tulee taata riittävällä tasolla, että tarpeelliset lokit syntyvät ja pysyvät muuttumattomina ja todistusvoimaisina.

Palvelunantajan on kerättävä lokitiedot asiakasrekisterikohtaisesti kaikesta asiakastietojen käytöstä ja luovutuksesta seurantaa ja valvontaa varten (asiakastietolaki 10 §), jos tietojärjestelmän käyttö edellyttää tunnistautumista tai muuta kirjautumista. Apteekin on kerättävä käyttölokitiedot lääkemääräysten muiden lääkemääräyslain 3 §:n 1 momentin 4 kohdassa tarkoitettuun reseptikeskukseen tallennettujen lääkehoitoa koskevien merkintöjen käsittelystä. (Asiakastietolaki 10 §, lääkemääräyslaki 3 §.) Asiakaskohtaisten tietojen katselemisesta ja käsittelystä on jäätävä lokimerkinnät.

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

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 yhtenäisiin ammattiryhmä- ja tehtäväkohtaisiin käyttövaltuuslinjauksiin ja käyttäjärooleihin (ks. luku 6.7).

Tietoturvallisuuden omavalvonnan kohteella on oltava tietosuojaan ja asiakastietojen käsittelyn valvontaan sekä tietoturvasuunnitelman toteuttamiseen liittyvä erillinen seuranta- ja valvontasuunnitelma, joka voi myös sisältyä tietoturvasuunnitelmaan. Kyse on seuranta- ja valvontasuunnitelmasta, jolla itse seurataan henkilötietojen ja tietojärjestelmien käyttöä. Seuranta- ja valvontasuunnitelmassa tulisi ottaa kantaa vähintään siihen, miten tehdään säännöllistä henkilötietojen käytön seurantaa ja miten toimitaan tilanteissa, joissa väärinkäytöksiä ilmenee. Seuranta- ja valvontasuunnitelmaan on kuvattava yksityiskohtaiset toimintatavat, jos käyttölokitiedoista paljastuu virhetilanteita, epäiltyjä rikkomuksia tai epäasianmukaisia asiakastietojen käyttöjä. Seuranta- ja valvontasuunnitelmaan tulee kuvata myös toimintamalli, jonka mukaisesti rekisterinpitäjä ja Kela toimivat luovuttaessaan tietoja luovutusrekisteristä.

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.

Organisaation sisäisessä lokitietojen seurannassa ja raportoinnissa tulisi tehdä jatkuvaa ja toistuvaa yksityiskohtaista seurantaa, jonka lähtökohtana on organisaatiossa käsiteltyjen asiakastietojen ja siellä toimivien käyttäjien seuranta ja valvonta kokonaisuutena, mukaan lukien mahdollisten poikkeamien havaitseminen. Lokien hallinnan ja käytön seurannan yksityiskohtaiset toimintakäytännöt tulee kuvata joko tietoturvasuunnitelmaan tai erillisiin dokumentteihin. Tällaisia ovat esimerkiksi asiakkaiden ja viranomaisen tietopyyntöihin vastaaminen, lokiraporttien kokoaminen ja hallinta sekä valvontatoiminnassa mukana olevien henkilöiden roolit. Lisätietoja on saatavissa lokitietojen hallinnan kansallisista vaatimusmäärittelyistä kohdasta raportoinnin vaatimukset[4].

6.9 Fyysinen turvallisuus osana tietojärjestelmien käyttöympäristön turvallisuutta

Tietoturvallisuuden omavalvonnan kohteen on otettava huomioon fyysinen käyttöympäristö, joissa asiakastietoja käsitellään. Tietoturvallisuuden omavalvonnan kohteen tulee tarkastella toimitiloja ja niiden tilaratkaisu-, sisustus-, äänieristys- tai muita vastaavia toimenpiteitä, joilla voidaan käytännössä vaikuttaa tietosuojaan ja tietoturvaan. Lisäksi on huolehdittava palvelinten käyttöympäristön fyysisestä turvallisuudesta.

Näytöt, työasemat ja tulostimet tulee sijoittaa ja suojata sivullisilta tietoturvallisen käyttöympäristön varmistamiseksi. Kokonaisuuteen liittyy tekninen ja fyysinen kulunvalvonta ja mahdolliset fyysisen pääsyn rajoittamistoimenpiteet. Tietoturvasuunnitelmassa on yleisellä tasolla kuvattava, kuinka nämä asiat on otettu huomioon ja mistä on tarvittaessa saatavilla yksityiskohtaisempaa tietoa.

Tietoturvasuunnitelmassa on kuvattava, miten on huolehdittu ja todennettu mahdollisesti käytössä olevien liikuteltavien asiakastietoja sisältävien laitteiden tietosuojasta ja tietoturvasta omavalvonnan kohteessa.

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

Tietojärjestelmistä paperille tulostettavien asiakastietojen asianmukaisesta säilyttämisestä ja hävittämisestä tulee olla kuvattuna menettelytavat, joilla estetään omavalvonnan kohteen asiakastietojen päätyminen sivullisten haltuun. 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.

[4] Asiakas- ja potilastietojen käsittelyssä syntyvien lokitietojen hallinnan kansalliset vaatimusmäärittelyt v 1.2

6.10 Työasemien, mobiililaitteiden ja käyttöympäristön tukipalveluiden hallinta

Tietoturvasuunnitelmassa on kuvattava, miten tietojärjestelmien käyttöympäristössä huolehditaan tietoturvallisesti asiakas- ja potilastietojärjestelmien käytössä olevien työasemien ja mobiililaitteiden hallinnasta. Tietoturvasuunnitelmassa tai siihen liittyvissä dokumenteissa on kuvattava, miten laitteiden ja palvelujen virusturva- ja haittaohjelmien suojaamisen ohjelmistojen toimivuus ja päivitykset on käytännössä varmistettu, ja miten muut suojauskäytännöt on järjestetty, 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, 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. Kuvauksesta tulee selkeästi selvitä vastuu- ja työnjakokysymykset, toisin sanoen mitkä asiat ovat palvelunantajan oman toiminnan ja mitkä sopimuskumppanien vastuulla. Myös mahdolliset alihankkijat tulee kuvata. Asiat tulee ilmaista toimijoiden välisissä sopimuksissa riittävän tarkasti ja käytännönläheisesti tietoturvallisen ja sujuvan toiminnan varmistamiseksi.

6.11 Alusta- ja verkkopalvelujen tietoturvallinen käyttö tietosuojan ja varautumisen kannalta

Sosiaali- ja terveydenhuollon toimijoiden (palvelunantaja, apteekki, välittäjä, Kela) tulee olla tietoisia kaikista käytössään olevista alusta- ja verkkopalveluista, joiden 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 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 osalta on kuvattava käytössä olevat ratkaisut, sopimukset ja käytännöt. Näitä ovat esimerkiksi pilvipohjaiset ratkaisut, etähallintapalvelut, palvelinvuokraukset, palvelinhallinnat, varmistuspalvelut ja konesalipalvelut. Alla listatut asiat on varmistettava ja kuvattava:

- Tietojen siirron riskitaso on arvioitava (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. Ajantasainen lisätieto Tietosuojavaltuutetun toimiston sivuilta kohdasta Henkilötietojen siirrot Euroopan talousalueen ulkopuolelle[5].

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

- Erityisesti kriittisissä palveluissa on varauduttava tietojen käsittelyyn normaalista poikkeavissa olosuhteissa. Kriittisiä palveluita ovat esimerkiksi julkisen terveydenhuollon päivystysvastuulla olevat palvelut. Varautumisessa on huomioitava keskeisimmät riskiuhkat tilanteissa, joissa yhteiskunnan verkkoyhteydet on rajoitettu Suomen maantieteellisten rajojen sisäpuolelle (esimerkiksi tiedon hallinnointi näissä tilanteissa).

- Käytössä olevia alusta- ja verkkopalveluja on seurattava säännöllisesti muun muassa toimivuuden, tietoturvallisuusriskien, häiriötilanteiden ja käyttöehtomuutosten näkökulmasta. Tarvittaessa sopimuksia ja käytäntöjä on päivitettävä 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. Näihin liittyviä päivitystarpeita on seurattava.

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

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

[5] https://tietosuoja.fi/henkilotietojen-siirrot-etan-ulkopuolelle

6.12 Kanta-palvelujen liittymisen ja käytön tietoturvakäytännöt

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

Palvelunantajan ja apteekin on huolehdittava siitä, että henkilöstö hallitsee Kanta-palvelujen käyttöön liittyvät toimintamallit ja periaatteet sekä tietää väärinkäytösten seuraamukset. Tietoturvasuunnitelmassa on kuvattava, miten palvelunantaja ja apteekki todentavat asiakkaiden informoinnin Kanta-palveluista ja asiakastietojen käytöstä.

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

Tietoturvallisuuden 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.

Tietoturvallisuuden omavalvonnan kohteen on lisäksi varmistettava, että Kanta-palveluihin arkistoidaan ainoastaan sosiaali- ja terveydenhuollon rekistereihin kuuluvia potilas- ja asiakasasiakirjoja (asiakastietolaki 69 §).

Asiakastietolain mukaisesti asiakasasia kirja tulee laatia ja tallentaa Kanta-palveluihin viivytyksettä, kun asiakirja on valmistunut (asiakastietolaki 21 §, 65 §). Viiveet arkistoinnissa tai arkistoimattomuus voivat aiheuttaa merkittäviä riskejä tiedon eheydelle sekä asiakkaan ja sosiaali- ja terveydenhuollon ammattilaisen oikeusturvalle.

Tietoturvallisuuden omavalvonnan kohteella tulee olla selkeät menettelytavat ja vastuut Kanta-palvelujen ja niihin liittyvien järjestelmien häiriö- ja virhetilanteiden havainnointiin, tiedottamiseen, korjaamiseen ja jälkihoitoon. Palvelunantajan ja tietojärjestelmäpalvelun tuottajan välisissä sopimuksissa tulee kuvata vastuut toimintatavoista liittyen esimerkiksi kiireellisiin häiriö- tai tietoturvaloukkaustilanteisiin. On sovittava esimerkiksi asiakas- ja viranomaisviestinnän käytännöistä ja tarvittavista menettelyistä tapahtumalokitietojen käsittelyssä.

Kanta-palvelujen teknisen tuen tulee tietää tietoturvallisuuden omavalvonnan kohteen vastuutahot häiriötilanteissa. Muutokset palvelunantajan ja apteekin käyttämissä tietojärjestelmissä (sisältäen versiotiedot tai muut tietojärjestelmän statusta kuvaavat tiedot) on ilmoitettava Kelalle sen antamien ohjeiden mukaisesti.

Tietoturvallisuuden 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 5/2024 mukaisesti. Palvelunantajan on säännöllisesti seurattava, että THL:n määräyksen 4/2024 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. Jos palvelunantajan toiminnassa käytetään hyvinvointisovelluksia, vastaavat varmistukset on tehtävä myös niiden osalta.

Palvelunantajan ja apteekin on määriteltävä menettelytavat käytännön toiminta- ja vastuukysymyksissä niihin tilanteisiin, joissa tietojärjestelmän tai välityspalvelun todistus tietoturvallisuuden arvioinnista peruutetaan määräajaksi tai kokonaan tai tietojärjestelmän käyttö kielletään tai sen käyttöä rajoitetaan. Tällaiset asiat tulee ottaa ennalta huomioon palvelunantajan, välittäjän ja tietojärjestelmäpalvelun tuottajan välisissä sopimuksissa (vrt. THL:n määräys 5/2024).

Tässä luvussa kuvatut asiat 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 16. päivänä tammikuuta 2024 ja on voimassa toistaiseksi. Palvelunantajien, apteekkien, välittäjien ja Kansaneläkelaitoksen on päivitettävä aiemmat tietosuojaan, tietoturvallisuuteen ja tietojärjestelmien käyttöön liittyvät omavalvontasuunnitelmansa tietoturvasuunnitelmaksi tämän määräyksen mukaisesti.

Sirpa Soini
Johtaja

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 julkaistaan viranomaisten määräyskokoelmissa

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

ja on saatavissa:

- Terveyden ja hyvinvoinnin laitoksen kirjaamosta sekä
- Internet-osoitteesta https://thl.fi/fi/web/tiedonhallinta-sosiaali-ja-terveysalalla/maaraykset-ja-maarittelyt/maaraykset