Tiedonvälittäjät

Tieto ja tiedonhallinnan ohjaus 20.2.2024

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 22. päivänä helmikuuta 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 tarkoitus ja soveltamisala 3
2 Määritelmät 4
3 Vastuut tietoturvan sekä asiakastietojen asianmukaisen käsittelyn varmistamisessa 6
4 Suhde THL:n muihin määräyksiin, yleisiin viitekehyksiin sekä eräisiin muihin säädöksiin 7
5 Yleistä tietoturvasuunnitelmasta 8
6 Tietoturvasuunnitelmaan sisällytettävät selvitykset ja vaatimukset 9
6.1 Yleiset tietoturvakäytännöt 9
6.2 Menettelyt virhe- ja ongelmatilanteissa sekä jatkuvuudenhallinta 10
6.3 Henkilökunnan koulutus sekä osaamisen ylläpito ja kehittäminen 11
6.4 Tietojärjestelmien käyttöohjeet ja ohjeiden mukainen käyttö 12
6.5 Tietojärjestelmien perustiedot, kuvaukset ja olennaisten vaatimusten täyttyminen 13
6.6 Tietojärjestelmien asennus, ylläpito ja päivitys 15
6.7 Käyttövaltuuksien hallinnan ja tunnistautumisen käytännöt 16
6.8 Asiakas- ja potilastietojärjestelmien pääsynhallinnan ja käytön seurannan käytännöt 17
6.9 Fyysinen turvallisuus osana tietojärjestelmien käyttöympäristön turvallisuutta 18
6.10 Työasemien, mobiililaitteiden ja käyttöympäristön tukipalveluiden hallinta 19
6.11 Alusta- ja verkkopalvelujen tietoturvallinen käyttö tietosuojan ja varautumisen kannalta 19
6.12 Kanta-palvelujen liittymisen ja käytön tietoturvakäytännöt 21
7 Ohjaus ja neuvonta 22
8 Voimaantulo 22
Tiedoksi 23

Liite Tietoturvasuunnitelman mallipohja

1 Määräyksen tarkoitus ja soveltamisala

THL:n määräys 3/2024 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 tarkentaa sosiaali- ja terveydenhuollon digitaalista tai ei-digitaalista asiakastietojen turvallista käsittelyä.

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

Tietoturvasuunnitelman avulla kootaan 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.

Tietoturvasuunnitelman laatimiseen velvoitetuista tahoista eli tämän määräyksen kohderyhmistä käytetään tässä määräyksessä ja määräyksen liitteessä yleisnimeä *tietoturvallisuuden omavalvonnan kohde*.

Määräyksen tarkoituksena ei ole tarkasti määrätä vaatimus vaatimukselta kaikista yksityiskohtaisista tietoturvallisuuskäytännöistä. Sosiaali- ja terveydenhuollon organisaatioita on hyvin erilaisia yhden henkilön yrityksistä useiden tuhansien henkilöiden yksityisiin ja julkisiin organisaatioihin. Oleellista on varmistua siitä, miten asiakastietojen käsittelyyn ja tietojärjestelmiin liittyvät vaatimukset käytännössä varmistetaan asiakastietolain 77 §:n 1 momentin kohtien 1–9 ja tämän THL:n määräyksen 3/2024 mukaisesti tietoturvallisuuden omavalvonnan kohteessa.

Tietoturvallisuuden omavalvonnan kohteen velvollisuutena on toimia laatimansa tietoturvasuunnitelman mukaisesti, säännöllisesti ylläpitää ja katselmoida suunnitelmaansa sekä seurata aktiivisesti sen toteutumista. Kyse on jatkuvasta ja säännöllisestä riskienhallinnasta, asianmukaisten tietoturvallisuuden ja asiakastietojen käyttöön liittyvien käytäntöjen varmistamisesta sekä niiden toteuttamisesta.

Määräyksen liitteenä on tietoturvasuunnitelman mallipohja, joka on tietoturvallisuuden omavalvonnan kohteiden tietoturvasuunnitelman laatimisen tueksi tarkoitettu esimerkinomainen dokumenttipohja. Mallipohjadokumentin rakenne on informatiivinen, suuntaa antava eli suunnitelman tekemistä helpottava ja ohjaava.

2 Määritelmät

Tämän määräyksen keskeiset käsitteet ja niiden määritelmät ovat seuraavat:

- **Asiakastieto** (asiakastietolaki 3 § 1 mom. 6 kohta):
    - potilastieto ja sosiaalihuollon asiakastieto.
- **Tietoturvallisuuden omavalvonnan kohde**
    - Tietoturvasuunnitelman laatimiseen velvoitetuista tahoista eli sosiaali- ja terveydenhuollon palvelunantajista, apteekeista, välittäjistä ja Kansaneläkelaitoksesta (Kela), käytetään tässä määräyksessä ja määräyksen liitteessä yleisnimeä tietoturvallisuuden omavalvonnan kohde.
- **Henkilökunta**
    - Asiakastietoja käsittelevät tai asiakastietojen käsittelyyn osallistuvat henkilöt tietoturvallisuuden omavalvonnan kohteen organisaatiossa mukaan lukien vuokratyöntekijät.
- **Palvelunantaja** (asiakastietolaki 3 § 1 mom. 11 kohta[1])
- **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.

[1] https://www.finlex.fi/fi/laki/alkup/2023/20230703

- **Tietojärjestelmän valmistaja** (asiakastietolaki 3 § 1 mom. 21 kohta):
    - taho, joka on vastuussa sosiaali- ja terveydenhuollon tietojärjestelmän suunnittelusta ja valmistuksesta.
- **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 ja hyvinvointisovelluksen 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 asiakastietolain noudattamista.
- **Kanta-palvelut** (asiakastietolaki 65 § 1 mom.):
    - Kansaneläkelaitoksen järjestämät ja ylläpitämät sosiaali- ja terveydenhuollon valtakunnalliset tietojärjestelmäpalvelut.
- **Tietojärjestelmän käyttöympäristö**:
    - tekninen, organisatorinen ja fyysinen ympäristö, jossa yksi tai useampi palvelunantaja tai apteekki käyttää tietojärjestelmää tai osajärjestelmää sosiaali- ja terveydenhuollon palvelujen tuottamisessa, järjestämisessä ja asiakastietojen käsittelyssä. Käyttöympäristö sisältää mm. päätelaitteet, palvelimet, työasemat, käyttöjärjestelmä- ja varusohjelmistot, viestintäverkot sekä hallinta- ja tietoturvakäytännöt, jotka eivät ole osa tietojärjestelmää.

3 Vastuut tietoturvan sekä asiakastietojen asianmukaisen käsittelyn varmistamisessa

Tietoturvallisuuden omavalvonnan kohteen tulee varmistaa, että tietoturvasuunnitelmaan sisällytettävät vaatimukset toteutuvat kaikissa sen omissa palveluyksiköissä ja kaikessa muiden sen lukuun palveluiden tuottamiseen tai toteuttamiseen osallistuvien palvelunantajien toiminnassa mukaan lukien mahdollisten alihankintapalveluntuottajien toiminnassa. Tietoturvasuunnitelmassa olevista selvityksistä tulee näkyä kaikkien edellä kuvattujen yksiköiden ja alihankintapalveluntuottajien vastuut.

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 sopimus- ja hankintajärjestelyjen (esimerkiksi palveluhankinta, sovellusvuokraus tai alihankinta) kautta.

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

Tietoturvasuunnitelman sisältö tulee suhteuttaa tietoturvallisuuden omavalvonnan kohteen oman toiminnan laajuuteen ja organisaation toimintaympäristössä tarvittaviin asianmukaisiin tietoturva- ja tietosuojakäytäntöihin. Toimintaan liittyvät mahdolliset riskit ja käytettävissä olevat toiminnan ylläpidon ja turvaamisen resurssit (omat tai ulkoistetut) tulee ennalta arvioida, sopia ja järjestää siten, että kaikenlaisissa tilanteissa kyetään tarvittaessa nopeasti reagoimaan ja siten oikein kohdistamaan relevantit asiakastietojen turvaamistoimenpiteet.

Riippumatta tietoturvallisuuden omavalvonnan kohteen organisaation koosta sillä tulee olla käytössä asianmukaiset käytännöt arkaluonteisten asiakastietojen suojaamiseksi digitaalisissa ja ei-digitaalisissa ympäristöissä. Näitä tietoturvallisuuden omavalvonnan kohteen omia käytäntöjä on myös noudatettava käsiteltäessä kyseisessä organisaatiossa asiakas- tai potilastietoja.

Tietoturvallisuuden omavalvonnan kohteella on oltava sopimus asiakastietojen käsittelystä ja tietoturvallisuuden varmistamisesta muiden sen asiakas- tai potilastietojärjestelmiä käyttävien palvelunantajien keskinäisten vastuiden osalta. Tietoturvallisuuden omavalvonnan kohde vastaa tietoturvasuunnitelmasta myös tilanteissa, joissa se hankkii käyttöympäristön tai tietotekniikkapalveluita esimerkiksi ostopalveluina muilta palvelunantajilta tai asiakastietolain mukaisilta tai muilta tietojärjestelmäpalvelujen tuottajilta.

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

Tietoturvasuunnitelman varsinaisen sisällön tai siitä viitatuissa liitteissä esitetyn sisällön pohjalta on tarvittaessa pystyttävä todentamaan seuraavat tietoturvallisuuden omavalvontaan liittyvät asiat:

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

Tietoturvallisuuden omavalvonnan kohteen on pystyttävä osoittamaan tietoturvasuunnitelman olemassaolo, asianmukaisuus ja toteuttaminen esimerkiksi valvontaviranomaisille myös niissä tilanteissa, joissa se ei itse tuota palveluita. Tämä koskee sekä sosiaali- että terveyspalvelujen että tietojärjestelmä- tai teknisten tukipalvelujen tuottamista. 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 tulee käyttää tietojärjestelmiä, joiden käyttötarkoitukset vastaavat palvelunantajan ja apteekin omaa toimintaa. Lisäksi palvelunantajan ja apteekin on täytettävä toimintaan liittyvät olennaiset vaatimukset (asiakastietolaki 84 §). Olennaiset vaatimukset voidaan täyttää yhden tai useamman tietojärjestelmän muodostaman kokonaisuuden kautta. Sosiaali- ja terveydenhuollon tietojärjestelmien luokittelusta ja sertifioinnista annetun THL:n määräyksen 4/2024 liitteessä 1 on kuvattu tietojärjestelmien luokittelua käytännön esimerkkeineen. Tietoturvasuunnitelmaa katselmoitaessa ja ylläpidettäessä tulee noudattaa myös muita tietoturvallisuuteen liittyviä voimassa olevia säädöksiä.

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

Tässä määräyksessä ei säädetä siitä, millaiset häiriöt tietojärjestelmien käyttöympäristöissä ja operatiivisissa verkkoympäristöissä ovat merkittäviä tai kuinka häiriöitä koskevat ilmoitukset on tehtävä (asiakastietolaki 90 §). Tietoverkkoihin ja käyttöympäristöihin liittyvästä poikkeamien hallinnasta tullaan mahdollisesti säätämään sosiaali- ja terveydenhuollossa NIS 2-säädösten perusteella valmisteilla olevassa laissa kyberturvallisuuden riskienhallinnasta[2].

Tämän määräyksen kohdealueena eivät 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 (vrt. luku 6.2 Menettelyt virhe- ja ongelmatilanteissa sekä jatkuvuudenhallinta vs. palvelunantajan ilmoittamisvelvollisuudet).

Laki julkisen hallinnon tiedonhallinnasta (906/2019, tiedonhallintalaki) on yleislaki, jota sovelletaan tiedonhallintaan ja tietojärjestelmien käyttöön, kun viranomaiset käsittelevät tietoaineistoja. Tiedonhallintalain 13 §:ssä säädetään tiedonhallintayksiköiden velvollisuuksista tietoturvallisuuden varmistamiseen niiden toiminnassa. Asiakastietolain 77 §:ssä säädetty tietoturvasuunnitelma velvoittaa kaikkia sosiaali- ja terveydenhuollon palvelunantajia; tietoturvasuunnitelmalla varmistetaan yhdenmukaiset menettelyt asiakastietojen käsittelyssä koskien sekä julkisia että yksityisiä palvelunantajia, välittäjiä sekä Kansaneläkelaitosta. Etenkin tiedonhallintalain luvuissa 2 (Tiedonhallinnan järjestäminen) ja 4 (Tietoturvallisuus) on viranomaisia velvoittavia ja yksityisille toimijoille informatiivisia kohtia, joita tulee tai, joita on hyvä hyödyntää tietoturvallisuuden omavalvonnan kohteen tietoturvasuunnitelmassa.

---

[2] Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555 toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi kaikkialla unionissa, asetuksen (EU) N:o 910/2014 ja direktiivin (EU) 2018/1972 muuttamisesta sekä direktiivin (EU) 2016/1148 kumoamisesta.

NIS2-direktiivi saatetaan osaksi kansallista lainsäädäntöä 17.10.2024 mennessä ja täytäntöönpanoa koskevien säännösten soveltaminen alkaa 18.10.2024. Hallituksen esityksessä eduskunnalle kyberturvallisuusdirektiivin täytäntöönpanemiseksi ehdotetaan säädettävän uusi laki kyberturvallisuuden riskienhallinnasta. Lakiehdotuksessa esitetään säädettävän tietoverkkoihin ja käyttöympäristöihin liittyvästä riskienhallinnasta.

5 Yleistä tietoturvasuunnitelmasta

Tietoturvasuunnitelma on käytännön työväline, jolla hahmotetaan tietoturvallisuuden kokonaiskuvaa ja toteutetaan asiakastietojen käsittely hyvien käytäntöjen mukaisesti. Tietoturvasuunnitelmassa kuvatut selvitykset ja käytännöt voidaan yhdistää muihin tietoturvallisuuden omavalvonnan kohteen 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 suunnitelmasta voidaan viitata erillisiin saatavilla oleviin kuvauksiin, esimerkiksi tietoturvallisuuden omavalvonnan kohteen tietoturvaohjeisiin tai tietojärjestelmäsalkun kuvauksiin.

Tämän määräyksen mukaista tietoturvasuunnitelmaa ei tule sisällyttää tai yhdistää julkaistaviin tai julkisesti saatavilla oleviin omavalvontasuunnitelmiin. Tietoturvasuunnitelmaa ja siitä viitattuja liitteitä tulee käsitellä ja säilyttää tietoturvallisesti. Ne tulee suojata sivullisilta, ja tarvittaessa niihin tulee merkitä salassa pidettävä -tieto. Palvelunantajan, joka toimii viranomaisena, tulee huomioida viranomaisten toiminnan julkisuudesta annetun lain (621/1999, julkisuuslaki) salassapitoa koskevat säännökset (24 § 1 mom. 7 kohta).

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.

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

Tietoturvasuunnitelmassa kuvatuilla menettelyillä ja keinoilla myös varmistetaan, että tietojärjestelmiin liitetyt muut kuin asiakastietojen käsittelyyn tarkoitetut tietojärjestelmät tai sovellukset eivät vaaranna tietojärjestelmien suorituskykyä eivätkä niiden tietoturva- tai tietosuojaominaisuuksia.

Kelan ylläpitämien valtakunnallisten tietojärjestelmäpalvelujen käytön osalta tietoturvasuunnitelmassa on selvitettävä myös tietosuojaan ja tietoturvallisuuteen liittyvät asiat. Palvelunantajan ja apteekin on tietoturvasuunnitelmassa selvitettävä, miten tietoturvallisen käytön ja tietosuojan edellyttämät vaatimukset on varmistettu ja miten tietosuojan ja tietoturvan käytännöt on järjestetty ennen liittymistään Kanta-palvelujen käyttäjäksi (ks. luku 6.12 Kanta-palvelujen liittymisen ja käytön tietoturvakäytännöt).

Tietoturvasuunnitelma on tietoturvallisuuden omavalvonnan kohteen dokumentti, jolla rekisterinpitäjä voi täydentää EU:n yleisen tietosuoja-asetuksen[3] mukaista osoitusvelvollisuuttaan (5 artikla 2 kohta). Rekisterinpitäjän eli tietoturvallisuuden omavalvonnan kohteen 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.

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 (EU:n 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 sisällyttää asiakastietolain 77 §:n vaatimusten lisäksi myös muita tietoturvallisuuden omavalvonnan kohteen kannalta olennaisia kokonaisturvallisuuteen liittyviä asioita.

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.

Tietoturvasuunnitelmasta voidaan viitata olemassa oleviin erikseen ylläpidettäviin ohjeisiin ja liitedokumentteihin (vrt. luku 5). 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[4].

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. ISO/IEC 27000 -sarjan standardien mukainen tietoturvallisuuden hallintajärjestelmä on suositeltava esimerkki hyvästä käytännöstä etenkin isoille organisaatioille. Pienemmille palvelunantajille suositeltava menettely on esimerkiksi Traficomin Kyberturvallisuuskeskuksen Kybermittarilla[5] tehtävä itsearviointi.

Tietoturvasuunnitelmaan tulee kuvata tietoturvallisuuden omavalvonnan kohteen yleiset tietoturvakäytännöt ja/tai voimassa olevat digiturvallisuuteen liittyvät politiikat, mikäli tällaisia on laadittu[6]. 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 sekä miten vastuut tietoturvallisuustyössä on jaettu ja organisoitu toiminnan tavoitteiden saavuttamiseksi ja riskien hallitsemiseksi.

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

---

[4] Huom. Tässä luvussa 6 olevat sanamuodot ”tietoturvasuunnitelmassa tulee kuvata” tai muut vastaavat pelkkään tietoturvasuunnitelmaan liittyvät kuvausvaatimukset voidaan aina myös tulkita ”tietoturvasuunnitelmassa tai siitä viitattavissa litteissä tulee kuvata” -muodossa.

[5] https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen/kybermittari

[6] Digiturvallisuuteen liittyviä politiikkoja ovat esimerkiksi tietoturva- ja tietosuojapolitiikat.

Tietoturvasuunnitelmaan tai siitä viitattuihin liitteisiin tulee kuvata etä- ja hybridityöohjeistukset liittyen henkilökunnan työskentelyyn etänä (esimerkiksi kotona tai muussa etätyöpisteessä) ja erilaisissa liikkuvissa potilas- ja asiakastyötehtävissä, jos omavalvonnan kohteen toiminnassa on etänä tapahtuvaa asiakastietojen käyttöä.

Tietoturvasuunnitelmaan tulee kuvata erilaisissa työtehtävissä toimivan henkilökunnan tarvitsemia asiakastietosisältöjä. Esimerkiksi tietohallinnon asiantuntijoiden ja kehitys- ja hankintatoimen henkilökunnan työssään mahdollisesti käyttämät asiakastiedot tulisi vastata juuri heidän työtehtäviinsä liittyviä tarpeellisia tietoja (vrt. luku 6.7).

6.2 Menettelyt virhe- ja ongelmatilanteissa sekä jatkuvuudenhallinta

Tietoturvallisuuden omavalvonnan kohteen on varauduttava virhe- ja ongelmatilanteisiin, tietoturvapoikkeamiin[7], 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 ja tietoturvapoikkeamien ennalta havainnointiin, tiedottamiseen, korjaamiseen ja tilanteista toipumiseen. Vastaavasti tiedonhallintalain 13 a §:ssä säädetään, että tiedonhallintayksikön on seurattava toimintaympäristönsä tietoturvallisuuden tilaa ja varmistettava tietoaineistojen ja tietojärjestelmien tietoturvallisuus koko niiden elinkaaren ajan. Lisäksi tiedonhallintayksikön on selvitettävä olennaiset tietojenkäsittelyyn kohdistuvat riskit ja mitoitettava tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti.

Käytössä olevat tietojärjestelmät tulee luokitella kriittisyyden perusteella. Kriittisyysluokittelu tulee tehdä oman toiminnan ja siihen liittyvien riskien ja tavoitteiden näkökulmasta. Tämä voi vaikuttaa varautumisen toteuttamisen käytäntöihin. Nämä asiat on kuvattava suoraan tietoturvasuunnitelmaan tai tietoturvasuunnitelmasta viitattaviin erillisiin jatkuvuus-, toipumis- ja varautumissuunnitelmiin, joiden mukaisia menettelyitä tietoturvallisuuden omavalvonnan kohde noudattaa virhe- ja ongelmatilanteissa.

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.

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 turvattu käytännön erityistilanteissa. Suunniteltuja käytäntöjä olisi suositeltavaa harjoitella esimerkiksi kerran vuodessa.

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.

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.

---

[7] Kyberturvallisuuden sanasto, Turvallisuuskomitea 2018: ”tietoturvahäiriö, *tietoturvapoikkeama*: ”yksi tai useampi toisiinsa liittyvä odottamaton tai ei-toivottu tietoturvatapahtuma, joka vaarantaa tietojen ja palvelujen tietoturvan ja vaikuttaa organisaation toimintaan epäsuotuisasti”.

Turvallisuutta uhanneista tapahtumista olisi suositeltavaa kerätä kaikki oleelliset tiedot tietoturvapoikkeaman selvittämisen varalta. Lisäksi olisi suositeltavaa selvittää tietoturvatapahtuman juurisyy(t), jotta voitaisiin havaita mahdolliset tietoturvallisuutta uhkaavat haavoittuvuudet ja se, että oliko tapahtuma tahallinen vai tahaton, ulkoisen vai sisäisen toimijan aiheuttama jne.

Tietoturvallisuuden omavalvonnan kohteiden olisi suositeltavaa toteuttaa yksi tai useampia raportointikanava, joiden kautta organisaation sisäinen tai ulkopuolinen henkilö voisi raportoida epäillyistä tietoturvapoikkeamista.

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

Tietoturvallisuuden omavalvonnan kohteen tulee ilmoittaa Valviralle tietojärjestelmien ja hyvinvointisovellusten merkittävistä olennaisten vaatimusten täyttymisen poikkeamista erityisesti tilanteissa, joissa tällainen poikkeama voi aiheuttaa merkittävän riskin asiakas- tai potilasturvallisuudelle tai tietoturvalle (asiakastietolaki 90 § 1 momentti). Myös muu taho voi ilmoittaa Valviralle havaitsemistaan riskeistä. Merkittävien poikkeamien korjaamiseksi on ryhdyttävä välittömiin korjaaviin toimenpiteisiin.

Rekisterinpitäjän on ilmoitettava havaituista henkilötietojen tietoturvaloukkauksista tietosuojavaltuutetulle. Henkilötietojen tietoturvaloukkauksesta ilmoittamisesta säädetään EU:n yleisen tietosuoja-asetuksen 33 artiklassa (asiakastietolaki 90 § 1 momentti). 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 (asiakastietolaki 90 § 2 momentti).

Jos tietojärjestelmä tai hyvinvointisovellus täyttää lääkinnällisen laitteen määritelmän, on palvelunantajan ilmoitettava lääkinnällisistä laitteista annetun lain (719/2021) 33 §:n mukaisesti Fimealle, kun kyseessä on säännöksessä tarkoitettu lääkinnällisiin laitteisiin liittyvä vaaratilanne, esimerkiksi lääkinnälliseksi laitteeksi kuuluvan tietojärjestelmän suorituskyvyn poikkeama tai häiriö.

6.3 Henkilökunnan koulutus sekä osaamisen ylläpito ja kehittäminen

Tietoturvasuunnitelman avulla varmistetaan, että tietoturvallisuuden omavalvonnan kohteen henkilökunta hallitsee tietojärjestelmien käytön ja ottaa huomioon asiakastietojen salassapitoon ja tietoturvaan liittyvät vaatimukset sekä ymmärtää väärinkäyttöön liittyvät seuraamukset.

Tietoturvasuunnitelmassa on kuvattava, kuinka koulutukset on järjestetty tietojärjestelmiä käyttäville henkilöille eli kuinka käytännössä varmistetaan järjestelmien käytön vaatima koulutus ja osaaminen. Tietojärjestelmiä käyttävillä henkilöillä on oltava koulutusta sekä asiakastietojen käsittelyyn että tietosuoja- ja tietoturva-asioihin.

Henkilökunnalle tarjolla olevan koulutuksen määrän ja sisällön tulisi olla riittävää ja tarkoituksenmukaista henkilön tai henkilöstöryhmän työ- ja tietojenkäsittelytehtävien kannalta. Koulutusta tulisi tarjota säännöllisesti sekä olemassa olevien taitojen ylläpitämiseksi, uusien tehtävien tai tilanteiden hoitamiseksi, että uusien työntekijöiden varalta. Vastaavasti tiedonhallintalain 4 §:n 2 momentin kohdassa 3 säädetään, että tiedonhallintayksikön johdon on huolehdittava siitä, että tiedonhallintayksikössä on tarjolla koulutusta, jolla varmistetaan, että henkilöstöllä ja tiedonhallintayksikön lukuun toimivilla on riittävä tuntemus voimassa olevista tiedonhallintaa, tietojenkäsittelyä sekä asiakirjojen julkisuutta ja salassapitoa koskevista säädöksistä, määräyksistä ja tiedonhallintayksikön ohjeista.

Tietoturvallisuuden omavalvonnan kohteella on oltava koulutussuunnitelma tai vastaava dokumentti, jossa kuvataan toimintamalli henkilökunnan 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 muulla organisaatiossa sovitulla tavalla.

Tietoturvasuunnitelmassa on kuvattava, kuinka henkilökunnalle koulutetaan ja informoidaan asiakastietojen käsittelyn perusteet. Näitä ovat esimerkiksi asiakastietojen kirjaamisen merkitys, 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 asiakastietoja luovuttavien henkilöiden selvittää laillinen peruste, jonka nojalla asiakastieto voidaan luovuttaa vastaanottajalle. Lisäksi asiakastietoja luovuttavien henkilöiden tulee huolehtia, että tiedon vastaanottaja saa asiakastiedon ainoastaan niiltä osin kuin hänellä on lain mukaan oikeus se saada. Edellä kuvattuun liittyvä käytännön osaaminen tulee olla osa henkilökunnan koulutusta ja perehdytystä. Asiakastietoja luovuttavien henkilöiden ja käytössä olevissa tietojärjestelmissä on varmistettava, että tietojen luovutuksista syntyy luovutusilmoitus tai luovutusloki.

6.4 Tietojärjestelmien käyttöohjeet ja ohjeiden mukainen käyttö

Tietoturvallisuuden omavalvonnan kohteen omien ohjeiden ja toimintatapojen tulee ohjata asiakastietojen käsittelijöitä omissa työtehtävissään ja rooleissaan oikeisiin toimintatapoihin ja asianmukaiseen asiakastietojen käsittelyyn.

Tietoturvasuunnitelmassa on kuvattava, miten tietojärjestelmän asianmukainen ja tietoturvallinen käyttö varmistetaan tietoturvallisuuden omavalvonnan kohteen toiminnassa ja käyttöympäristössä tietojärjestelmäpalvelun tuottajan ja/tai tietojärjestelmän valmistajan antaman ohjeistuksen mukaisesti. Vastaavasti tiedonhallintalain 4 §:n 2 momentin kohdassa 2 säädetään, että tiedonhallintayksikön johdon on huolehdittava siitä, että tiedonhallintayksikössä on ajantasaiset ohjeet tietoaineistojen käsittelystä, tietojärjestelmien käytöstä, tietojenkäsittelyoikeuksista, tiedonhallinnan vastuiden toteuttamisesta, tiedonsaantioikeuksien toteuttamisesta, tietoturvallisuustoimenpiteistä sekä poikkeusoloihin varautumisesta.

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 henkilökunnan 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, muiden tietojärjestelmien ja ohjelmistojen versiopäivitysten sekä muiden muutosten yhteydessä.

6.5 Tietojärjestelmien perustiedot, kuvaukset ja olennaisten vaatimusten täyttyminen

Tietoturvallisuuden omavalvonnan kohteen on kuvattava tietoturvasuunnitelmassa perustiedot ja tarkemmat kuvaukset kaikista sen käytössä olevista, asiakastietolain mukaisista tietojärjestelmistä ja hyvinvointisovelluksista[8], jotka on tarkoitettu:

- käytettäväksi asiakastietojen sähköiseen käsittelyyn,
- asiakasasiakirjojen tallentamiseen ja ylläpitoon,
- valtakunnallisiin tietojärjestelmäpalveluihin liittämiseen,
- palvelunantajan toiminnassa käytettäviin hyvinvointisovelluksiin tai digitaaliset asiointipalveluihin tai
- hyvinvointitietojen hyödyntämiseen sosiaali- ja terveydenhuollon ammattihenkilöiden työssä.

Tietoturvallisuuden omavalvonnan kohteen on kuvattava tietoturvasuunnitelmassa, mistä löytyy tieto luokitelluista ja luokittelemattomista tietojärjestelmistä, 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 sekä
- muut tietojärjestelmät (luokittelemattomat), joilla on vaikutusta ja jotka on otettava huomioon tietoturvasuunnitelman mukaisissa asennuksissa, ylläpidossa ja päivityksissä arkaluonteisten asiakastietojen suojaamisen kannalta.

[8] Tietojärjestelmien lisäksi myös hyvinvointisovellukset ja muut asiakkaille tarkoitetut digitaaliset asiointipalvelut, joita käytetään tietoturvallisuuden omavalvonnan kohteen toiminnassa, on kuvattava tietoturvasuunnitelmassa. THL:n määräyksessä 4/2024 luvussa 2 Määritelmät on määritelty hyvinvointisovellukset ja digitaaliset asiointipalvelut, jotka yhdessä muodostavat digitaalisen palvelun eli digipalvelun.

Digitaalinen palvelu, digipalvelu: yleistermiä digipalvelu käytetään määräyksissä 4/2024 ja 5/2024 viitaten sekä hyvinvointisovelluksiin että digitaalisiin asiointipalveluihin. Termi kattaa sekä tietojärjestelmät että hyvinvointisovellukset, joissa on suoraan kansalaisen käytettäväksi tarkoitettuja ominaisuuksia. Digipalveluihin voi kuulua sekä digitaalisia asiointipalveluja että Kanta-palveluihin kuten omatietovarantoon liittyviä hyvinvointisovelluksia. On mahdollista myös, että yksi digipalvelu täyttää sekä hyvinvointisovelluksen että tietojärjestelmän määritelmän asiakastietolaissa.

Tietoturvasuunnitelmassa on käytössä olevista tietojärjestelmistä ja hyvinvointisovelluksista kuvattava vähintään seuraavat asiat:

- perustiedot: nimi, versio (tai vastaava statustieto), toimittaja, yhteystiedot, tiedot Kelan yhteistestauksesta (luokat A2 ja A3), tiedot tietoturvallisuuden arviointia koskevasta todistuksesta (luokat A1, A2 ja A3) ja sen vastaavuus Valviran tietojärjestelmärekisterin tietoihin (luokat B, A1, A2 ja A3) sekä myös tiedot omaan toimintaan liittyvistä digitaalisista asiointipalveluista,
- tietojärjestelmän tai hyvinvointisovelluksen käyttötarkoitus,
- käyttäjäryhmät sekä
- tietojärjestelmä- ja hyvinvointisovelluskohtaiset käytännöt ja menettelyt, jotka on kuvattu tässä määräyksessä.

Tietoturvasuunnitelman on katettava kaikki tietoturvallisuuden omavalvonnan kohteen käyttämät tietojärjestelmät ja hyvinvointisovellukset. Tietoturvasuunnitelmassa on oltava tiedot myös sellaisista digitaalisista asiointipalveluista (tietojärjestelmistä), jotka liittyvät omaan toimintaan.

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 apteekin tulee käyttää tietojärjestelmiä [9], joiden käyttötarkoitukset vastaavat palvelunantajan ja apteekin omaa toimintaa. Tietojärjestelmien on täytettävä toimintaan liittyvät olennaiset vaatimukset.

Palvelunantaja ja apteekki vastaavat omassa toiminnassaan olennaisten vaatimusten täyttymisestä. Olennaiset vaatimukset voidaan täyttää yhden tai useamman tietojärjestelmän muodostaman kokonaisuuden kautta. Niiden varmistamiseen liittyvät menettelyt on kuvattava tietoturvasuunnitelmaan.

Määräyksen 5/2024 mukaisesti palvelunantajan ja apteekin on huomioitava omassa toiminnassaan ja tietojärjestelmien käyttöönotossa, tuotantokäytössä sekä tietoturvasuunnitelman mukaisessa toiminnassa olennaiset vaatimukset. Lisäksi on varmistettava tietojärjestelmiin ja hyvinvointisovelluksiin liittyvien olennaisten vaatimusten toteutuminen tietojärjestelmien hankinnoissa, sopimuksissa, kehittämisessä ja ylläpidossa. Palvelunantaja ja apteekki voivat hyödyntää olennaisten vaatimusten toteutumisen varmistamisessa Valviran tietojärjestelmärekisterissä olevia tietoja.

Valvira ylläpitää julkista rekisteriä asiakastietojen käsittelyyn tarkoitetuista tietojärjestelmistä (asiakastietolaki 80 § 2 momentti). Valviran tietojärjestelmärekisterin tiedot perustuvat 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 tietojärjestelmärekisteristä löytyvää tietoa siitä, mitä THL:n määräyksen 5/2024 mukaisia vähimmäisvaatimusten profiileja omassa toiminnassa käytettävät tietojärjestelmät täyttävät.

Tietoturvallisuuden omavalvonnan kohteen on huomioitava ja seurattava Valviran tietojärjestelmärekisterissä mahdollisesti julkaistavia tarkennuksia tietojärjestelmien ja hyvinvointisovellusten vaatimustenmukaisuuden toteuttamiseksi. Samalla tulisi tunnistaa, minkä profiilien mukaisia käyttötarkoituksia omassa toiminnassa käytettävissä tietojärjestelmissä tulisi olla toteutettuna.

[9] Tietojärjestelmäpalvelun tuottajan, tietojärjestelmän valmistajan ja hyvinvointisovelluksen valmistajan on toteutettava olennaiset vaatimukset tietojärjestelmiin, joita käytetään palvelunantajan ja apteekin toiminnassa.

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 muita tietojärjestelmiä, joilla tarkoitetaan esimerkiksi tietokoneohjelmia, jotka eivät käsittele asiakastietoja eivätkä siten ole asiakastietolain 79 §:n mukaisia A tai B luokan mukaisia tietojärjestelmiä.

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

6.6 Tietojärjestelmien asennus, ylläpito ja päivitys

Asiakastietolain 81 §:n 2 momentin mukaan asiakastietojen käsittelyyn tarkoitettua tietojärjestelmää tai hyvinvointisovellusta ei saa ottaa tuotantokäyttöön, ellei siitä ole voimassa olevia tietoja Valviran tietojärjestelmärekisterissä tai luokkaan A kuuluvan tietojärjestelmän tai hyvinvointisovelluksen tietoturvallisuuden arviointia koskeva todistus on vanhentunut. Asia on yksityiskohtaisesti kuvattu THL:n määräyksen 4/2024 luvussa 9 Tietojärjestelmän tai hyvinvointisovelluksen käyttöönoton edellytykset.

Tietoturvasuunnitelmaan on kuvattava tietoturvallisuuden omavalvonnan kohteeseen liittyvien tietojärjestelmien asennusten, ylläpidon ja päivitysten menettelytavat sekä niihin liittyvä tietoturvallisuuden varmistaminen. Kuvauksiin kuuluu myös henkilökunnan 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. Samalla tulee huomioida kiireelliset, mahdollisesti laajasti hyväksikäytettyihin haavoittuvuuksiin liittyvien päivitysten asentaminen ja muut korjaus- ja vahinkojen rajoitustoimenpiteet, jotka saattavat olla ristiriidassa normaalitilanteissa käytössä olevien tietojärjestelmien testaus- ja hyväksymismenettelyiden kanssa.

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 henkilökunnalta. Myös näiden henkilöiden roolit ja vastuut on määriteltävä suhteessa tietoturvallisuuden omavalvonnan kohteeseen sekä tietojärjestelmäpalvelun tuottajaan.

Asiakastietolain 77 § 1 momentin kohdassa 7 säädetään, että tietojärjestelmiä asentaa, ylläpitää ja päivittää vain henkilö, jolla on siihen tarvittava ammattitaito ja asiantuntemus ja jonka luotettavuus on varmistettu julkisen hallinnon tiedonhallinnasta annetun lain (906/2019) 12 §:ssä tarkoitetulla tavalla, jos henkilö tehtävissään pääsee käsittelemään asiakastietoja tai jos hän muuten tehtävissään voi vaarantaa sosiaali- ja terveydenhuollon jatkuvuuden kannalta kriittisten tietojärjestelmien toimintaa. Tietoturvasuunnitelmassa on kuvattava, kuinka tämä asia varmistetaan ja kuinka tietojärjestelmäpalvelun tuottajan ja tietoturvallisuuden omavalvonnan kohteen välisissä sopimuksissa kuvataan muut 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 tai siitä viitattavissa liitteissä on kuvattava, kuinka asiakastietoihin kohdistuvien käyttöoikeuksien määrittely ja hallinnointi tapahtuu, kuten käyttövaltuuksien, tunnistautumisen, pääsynhallinnan ja käytön seurannan (ks. luku 6.8) käytännöt rajauksineen. Käytön seurannan tulee perustua yhtenäisiin ammattiryhmä- ja tehtäväkohtaisiin käyttövaltuuslinjauksiin ja käyttäjärooleihin. Tietojärjestelmien käyttäjät ja erilaiset käyttäjäryhmät, käyttäjäroolit ja rooleihin liittyvät käyttövaltuudet on kuvattava. Keskeistä on kuvata, kuinka käyttövaltuuksia hallinnoidaan ja käytännössä hallitaan asiakas- tai potilastietojärjestelmien tai ulkoisen tietojärjestelmän, esimerkiksi identiteetin ja pääsynhallinta (IAM) -järjestelmän avulla. Tällaisissa ulkoisissa järjestelmissä ylläpidettäviä käyttövaltuuksien, tunnistusratkaisujen tai roolien hallinnan yksityiskohtia ei ole tarpeen toistaa tietoturvasuunnitelmassa.

Tietoturvasuunnitelmassa on kuvattava se, kuinka asiakastietojen käyttövaltuuksissa hyväksytään ja dokumentoidaan sosiaali- ja terveydenhuollon työntekijöiden työtehtävien muutokset[10]. Tietoturvasuunnitelmassa on lisäksi kuvattava henkilöt tai roolit, joilla on oikeus käsitellä, hylätä ja 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 tietoturvasuunnitelmassa tai siitä viitattavissa liitteissä. Kuvauksiin on myös sisällyttävä oman vakituisen henkilökunnan lisäksi se, kuinka työtehtävien mukaiset käyttöoikeudet järjestetään välttämättömiin asiakastietoihin organisaation lyhytaikaisille sijaisille, organisaatiossa työskenteleville opiskelijoille (ottaen huomioon opiskelijoita koskevat rajoitukset ammatin harjoittamisessa) sekä ulkopuolisille palveluntuottajille (ostopalvelut)[11].

Vastaavasti tietoturvasuunnitelmassa tai siitä viitattavissa liitteissä on kuvattava, kuinka, milloin ja millä tavalla poistuneiden työntekijöiden käyttöoikeudet poistetaan. Erityisen tärkeää on kuvata yksittäisten tai useiden tunnusten pääsyoikeuksien nopea poistaminen. Asiakastietoon liittyvistä käyttöoikeuksista ja niihin tehdyistä muutoksista tulee pitää kirjaa ja lokia (ks. luku 6.8).

Tietoturvasuunnitelmassa tai siitä viitattavissa liitteissä tulee kuvata, kuinka omavalvonnan kohteessa hallinnoidaan tietojärjestelmän käyttäjien käyttöoikeuksia, jotka liittyvät Kanta-palveluiden osalta sähköiseen lääkemääräykseen, valtakunnalliseen potilastiedon arkistoon, sosiaalihuollon asiakastiedon arkistoon ja muuhun potilastietoon.

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. Myös näihin asioihin liittyvät käytännöt on kuvattava tietoturvasuunnitelmassa tai siitä viitattavissa liitteissä.

---

[10] Sosiaali- ja terveysministeriö on valmistelemassa asetusta sosiaali- ja terveydenhuollon asiakastietojen käsittelystä, jonka tarkoitus on täydentää käyttöoikeuksia koskevaa sääntelyä lisäämällä sääntelyyn mukaan myös käyttöoikeudet sosiaali- ja terveydenhuollon yhteisissä palveluissa ja sosiaali- ja terveydenhuollon välillä luovutettaviin tietoihin.

[11] Asiakastietolain 9 §:n 3 momentin 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.

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, hyvinvointisovelluksia, paikallisia tietovarantoja tai -altaita ja katselimia) käyttävien henkilöiden tunnistautumistavat ja erilaisten tunnistautumisvälineiden hallinta (esimerkiksi toimikortit) sekä niiden voimassaolon hallinnointikäytännöt.

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[12].

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.

Kanta-palveluihin kirjautuminen edellyttää vahvaa sähköistä tunnistautumista. Sosiaali- ja terveydenhuollossa toimivien henkilöiden luotettava sähköinen tunnistaminen tapahtuu sosiaali- ja terveydenhuollon toimikorttien varmenteilla. Näihin liittyvät hallintakäytännöt on kuvattava tietoturvasuunnitelmaan.

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

Tietoturvasuunnitelmassa on kuvattava mahdollisten yhteiskäyttöisten tunnusten käyttäminen[13].

Tunnisteellisiin asiakastietoihin liittyviä usean käyttäjän näkymiä voidaan käyttää esimerkiksi osaston potilaspaikkojen koontinäytöissä tai vastaavissa käytännön työn kannalta välttämättömissä potilashallinnollisissa, ei-hoidollisissa tarkoituksissa. Tietoturvasuunnitelmassa tulee kuvata, kuinka tällaiset tiedot ja näkymät suojataan sivullisilta esimerkiksi tila- ja kulunhallintaratkaisuilla erilaisissa käytännön tilanteissa asiakastiedon käsittelyssä. Lisäksi tällaisia tietoja työssään hyödyntävät työntekijät on tarvittaessa kyettävä jälkikäteen todentamaan esimerkiksi työvuorojen hallinnan tai kulunhallintaratkaisujen kautta[14].

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 asiakastietolaissa tiedonhallintalakia tarkemmalla tasolla.

---

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

[13] 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.

[14] Tietosuojalaki 1050/2018 6 § 2 momentti 1 kohta: ”...toimenpiteet, joilla on jälkeenpäin mahdollista varmistaa ja todentaa kenen toimesta henkilötietoja on tallennettu, muutettu tai siirretty; ...".

Asiakastietojen käyttöön liittyvien lokitietojen luomisen ja käsittelyn prosessien tavoitteina tulee olla, että niissä syntyvät tarpeelliset lokit, jotka 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 ja muiden reseptikeskukseen tallennettujen lääkehoitoa koskevien merkintöjen käsittelystä[15].

Tietoturvallisuuden omavalvonnan kohteen 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 seuranta- ja valvontasuunnitelma, joka voi myös sisältyä tietoturvasuunnitelmaan. Kyse on seuranta- ja valvontasuunnitelmasta, jolla seurataan henkilötietojen ja tietojärjestelmien käyttöä. Seuranta- ja valvontasuunnitelmassa tulee ottaa kantaa vähintään siihen, miten tehdään säännöllistä henkilötietojen käytön seurantaa ja miten toimitaan tilanteissa, joissa väärinkäytöksiä ilmenee. Seuranta- ja valvontasuunnitelmaan on kuvattava toimintatavat, jos käyttölokitiedoista paljastuu virhetilanteita, epäiltyjä rikkomuksia tai epäasianmukaisia asiakastietojen käyttöjä. Seuranta- ja valvontasuunnitelmassa on myös kuvattava, kuinka rekisterinpitäjä ja Kela toimivat luovuttaessaan tietoja luovutuslokirekisteristä[16].

Seuranta- ja valvontasuunnitelma voi olla esimerkiksi vuosikohtainen. Oleellista on säännöllisesti katselmoida ja tarvittaessa päivittää suunnitelmaa. Tietosuojan ja asiakastietojen käytön omavalvontaa toteutetaan käytännössä suunnitelman kautta. Asiakastietojen käytönvalvonnan raportoinnissa on suositeltavaa 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 säännöllistä yksityiskohtaista seurantaa, jonka lähtökohtana on organisaatiossa käsiteltyjen asiakastietojen ja siellä toimivien käyttäjien seuranta ja valvonta kokonaisuutena, mukaan lukien mahdollisten tietoturvapoikkeamien 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[17].

6.9 Fyysinen turvallisuus osana tietojärjestelmien käyttöympäristön turvallisuutta

Tietoturvallisuuden omavalvonnan kohteen on kuvattava tietoturvasuunnitelmassa, kuinka huomioidaan fyysinen käyttöympäristö, jossa asiakastietoja käsitellään. Tämä voi esimerkiksi tarkoittaa erilaisten ja erityyppisten toimitilojen tarkastelemista sekä niihin liittyviä tilaratkaisu-, sisustus-, äänieristys- tai muita vastaavia toimenpiteitä, joilla voidaan käytännössä vaikuttaa tietosuojaan ja tietoturvaan. Tietoturvasuunnitelmassa on kuvattava myös se, kuinka huolehditaan palvelinten käyttöympäristön fyysisestä turvallisuudesta.

---

[15] Asiakastietolaki 10 §, laki sähköisestä lääkemääräyksestä 61/2007 3 §

[16] Asiaan liittyvää vastuunjakoa on kuvattu Kanta-palvelujen asiakkuuden sitoumusliitteessä (1.1.2024): ”Kuvaus Kantapalveluihin liittyvien palvelujen yhteisrekisterinpitäjyydestä”.

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

Tietoturvasuunnitelmassa on kuvattava, kuinka näytöt, työasemat ja tulostimet on sijoitettu ja suojattu 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.

Tietoturvasuunnitelmassa on kuvattava, kuinka varmistetaan se, että arkistotoimella on tehtäviinsä nähden asianmukainen ja riittävän tilava paloturvallinen fyysinen toimintaympäristö. Tietoturvasuunnitelmassa on kuvattava, kuinka asiakastietoja sisältävien tulosteiden hävittämiskäytäntöön liittyvät toimintatavat on suunniteltu, toteutettu ja koulutettu kaikille asiakastietojen tulosteita käsitteleville työntekijöille. Tietoturvasuunnitelmassa on lisäksi kuvattava, kuinka ei-julkisten ja salassa pidettävien paperitulosteiden hävittäminen on 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 tietoturvallisesti asiakas- ja potilastietojärjestelmien käytössä olevien työasemien ja mobiililaitteiden hallinnasta. Lisäksi on kuvattava, kuinka toimitaan työsuhteiden päättymisten jälkeen työntekijöillä käytössä olleiden laitteiden tietojen poistamisessa. 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 käyttöjärjestelmien 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 alihankintapalveluntuottajat tulee kuvata. Asiat tulee ilmaista toimijoiden välisissä sopimuksissa riittävän tarkasti tietoturvallisen ja sujuvan toiminnan varmistamiseksi.

6.11 Alusta- ja verkkopalvelujen tietoturvallinen käyttö tietosuojan ja varautumisen kannalta

Tietoturvallisuuden omavalvonnan kohteen tulee olla tietoinen kaikista käytössään olevista alusta- ja verkkopalveluista, joiden osalta on oltava selvää, mistä palveluista vastaa tietoturvallisuuden omavalvonnan kohde itse, mistä palveluista vastaa tietoturvallisuuden omavalvonnan kohteen lukuun toimiva tietojärjestelmäpalvelun tuottaja ja mistä mahdollinen kolmas osapuoli.

Seuraavat alakohdat a–j velvoittavat tietoturvallisuuden omavalvonnan kohdetta siihen, että tietoturvasuunnitelmassa tai siitä viitattavissa liitteissä on kuvattava tai vähintään otettava kantaa siihen, kuinka alakohdassa kuvattu asia varmistetaan tietoturvallisuuden omavalvonnan kohteen käyttöympäristössä käytössä olevine alusta- ja verkkopalveluineen. Nämä asiat tulee erityisesti ottaa huomioon ja varmistaa tietoturvallisuuden omavalvonnan kohteen ja tietojärjestelmäpalvelun tuottajan välisissä sopimuksissa:

a) Kuinka varmistetaan tietosuojasäädösten, kuten yleisen tietosuoja-asetuksen mukaan toimiminen. Henkilötietojen siirto ja säilytys EU/ETA-alueella on pääsääntöisesti sallittua vastaavilla suojatoimenpiteillä kuin Suomessa. Tietojen siirron riskitaso on arvioitava (yleisen tietosuoja-asetuksen mukainen vaikutustenarviointi). Jos tietoja siirretään EU/ETA-alueen ulkopuolelle nk. kolmansiin maihin, on noudatettava lainsäädännössä säädettyjä, hyväksyttyjä henkilötietojen siirtoperusteita ja toteutettava tarvittavat organisatoriset, sopimuspohjaiset ja tekniset suojatoimet tapaus- ja maakohtaisesti. Ajantasainen lisätieto Tietosuojavaltuutetun toimiston sivuilta kohdasta Henkilötietojen siirrot Euroopan talousalueen ulkopuolelle[18].

b) Kuinka on järjestetty palvelimien ja niiden edellyttämien käyttöympäristöjen tietoturvallisuustoimenpiteet, joita ovat esimerkiksi tietoverkon suojaaminen sekä tietojen kahdennus-, ylläpito- ja huoltotoimenpiteet.

c) 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 tietoturvallisuuden omavalvonnan kohteen ja tietoliikenne- tai viestinvälitysoperaattorin välistä sopimusta.

d) Kuinka tietojärjestelmät ja niiden käyttöympäristöt pidetään kunnossa ja kuinka varaudutaan toimimaan poikkeustilanteissa ilman tietojärjestelmiä.

e) Kuinka hallitaan ja hallinnoidaan käytössä olevia ratkaisuja, sopimuksia ja käytäntöjä. Tällaisia ovat esimerkiksi pilvipohjaiset ratkaisut, etähallintapalvelut, palvelinvuokraukset, palvelinhallinnat, varmistuspalvelut ja konesalipalvelut.

f) Kuinka arkaluonteisten ja salassa pidettävien asiakastietojen laaja tietojoukko suojataan siten, ettei sivullisilla ole pääsyä salaamattomiin asiakastietoihin. Asiakastietojen laajamittaisessa säilytyksessä salausavaimet tulee 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.

g) Kuinka kriittisissä palveluissa varaudutaan tietojen käsittelyyn normaalista poikkeavissa olosuhteissa. Kriittisiä palveluita ovat esimerkiksi julkisen terveydenhuollon päivystysvastuulla olevat palvelut. Varautumisessa on huomioitava keskeisimmät riskit tilanteissa, joissa yhteiskunnan verkkoyhteydet on rajoitettu Suomen maantieteellisten rajojen sisäpuolelle (esimerkiksi tiedon hallinnointi näissä tilanteissa). Varautumisessa tulee lisäksi suunnitella kaikki soveltuvat tietotekniset ja ei-tietotekniset keinot (esimerkiksi mahdollisuus käyttää väliaikaisesti kuulakärkikyniä ja vihkoja potilastietojen kirjaamiseen) sekä käytännöt tietojen siirtämisessä tietojärjestelmiin olosuhteiden sen salliessa.

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

h) Kuinka säännöllisesti seurataan alusta- ja verkkopalveluja muun muassa toimivuuden, tietoturvallisuusriskien, häiriötilanteiden ja käyttöehtomuutosten näkökulmasta. Tarvittaessa sopimuksia ja käytäntöjä on päivitettävä muuttunutta tilannetta vastaavaksi.

i) Kuinka on järjestetty tietojärjestelmien, osajärjestelmien, laitekomponenttien sekä verkkojen ja huolto-, päivitys- ja uusimissuunnitelma ja selkeä toimintamalli huoltotoimenpiteisiin liittyvään päätöksentekoon sekä kuinka seurataan näihin liittyviä päivitystarpeita.

j) Kuinka on huolehdittu siitä, että tietojärjestelmät täyttävät niihin kohdistuvat olennaiset tietoturvavaatimukset myös siltä osin kuin niiden toteutus tai käyttö nojautuu kolmansien osapuolten alusta- tai kapasiteettipalveluihin.

6.12 Kanta-palvelujen liittymisen ja käytön tietoturvakäytännöt

Tietoturvasuunnitelmassa on selvitettävä, miten valtakunnallisten tietojärjestelmäpalveluiden tietoturvallisen käytön edellyttämät vaatimukset varmistetaan, kun palvelunantaja tai apteekki on liittymässä Kanta-palvelujen käyttäjäksi. Kanta-palvelujen vaatimusten toteuttaminen on kuvattava tietoturvasuunnitelmassa tai siitä viitattavissa liitteissä ja niiden on oltava todennettavissa valvontaviranomaisen järjestämissä valvontatilanteissa.

Palvelunantajan ja apteekin on huolehdittava siitä, että henkilökunta 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 henkilökunnan koulutusmateriaaleissa, koulutuksissa ja ohjeistuksissa (asiakastietolaki 7 §).

Palvelunantajalla on oltava kuvaus toimintamallista, jonka mukaisesti se seuraa aktiivisesti Kanta-palvelujen käyttöä. Osana toimintamallia on muun muassa kuvattava, miten seurataan asiakirjojen asianmukaista[19] arkistointia ja Kanta-palvelujen lähettämiä virheilmoituksia.

Palvelunantajan on lisäksi varmistettava, että Kanta-palveluihin arkistoidaan ainoastaan sosiaali- ja terveydenhuollon rekistereihin kuuluvia potilas- ja asiakasasiakirjoja tai muita asiakastietoja sisältäviä asiakirjoja sekä sosiaali- ja terveydenhuollon järjestämiseen liittyviä asiakirjoja (asiakastietolaki 69 §).

Palvelunantajalla ja apteekilla tulee olla selkeät menettelytavat ja vastuut Kanta-palvelujen ja niihin liittyvien järjestelmien häiriö- ja virhetilanteiden havainnointiin, tiedottamiseen, korjaamiseen ja jälkihoitoon. Palvelunantajan ja tietojärjestelmäpalvelun tuottajan tai apteekin ja tietojärjestelmäpalvelun tuottajan välisissä sopimuksissa tulee kuvata vastuut toimintatavoista ja tehtävät lokitietojen käsittelyssä häiriö- tai tietoturvaloukkaustilanteissa. On sovittava esimerkiksi asiakas- ja viranomaisviestinnän käytännöistä ja tarvittavista menettelyistä tapahtumalokitietojen käsittelyssä.

Tietoturvasuunnitelmassa on kuvattava se, kuinka Kanta-palvelujen tekninen tuki saa tiedokseen palvelunantajan ja apteekin vastuutahot häiriötilanteissa. Muutokset palvelunantajan ja apteekin käyttämissä tietojärjestelmissä (sisältäen versiotiedot tai muut tietojärjestelmän statusta kuvaavat tiedot) on ilmoitettava Kelalle sen antamien ohjeiden mukaisesti. Kanta-palvelut toimii henkilötietojen käsittelijänä ja tukee rekisterinpitäjän teknistä selvittämistä häiriö-, virhe- ja loukkaustilanteiden selvittämiseksi.

---

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

Palvelunantajan ja apteekin on tietoturvasuunnitelmassa 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. Henkilökunnan on oltava tietoisia seurannasta ja väärinkäytön seuraamuksista.

Palvelunantajan ja apteekin on varmistettava, että sen toimintaa varten hankittava tai päivitettävä tietojärjestelmä täyttää tietojärjestelmän käyttötarkoitusta vastaavat olennaiset vaatimukset THL:n määräyksen 5/2024 mukaisesti. Palvelunantajan on ja apteekin säännöllisesti seurattava, että THL:n määräyksen 4/2024 mukaisesti luokkaan A1, A2 tai A3 kuuluvilla tietojärjestelmillä ja välityspalveluilla on voimassa oleva todistus tietoturvallisuuden arvioinnista. (Vrt. luku 6.5).

Kanta-palveluihin liittyvien (erityisesti luokkaan A2 tai A3 kuuluvien) tietojärjestelmien osalta on varmistettava, että järjestelmissä on hyväksytysti yhteistestattu ne ominaisuudet, jotka vastaavat järjestelmän käyttötarkoitusta (vrt. luku 6.5). Nämä tiedot ovat julkisesti saatavilla Valviran tietojärjestelmärekisteristä. Lisäksi palvelunantajan ja apteekin 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, apteekin, välittäjän ja tietojärjestelmäpalvelun tuottajan välisissä sopimuksissa (vrt. THL:n määräys 5/2024).

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 22. päivänä helmikuuta 2024 ja on voimassa toistaiseksi. Palvelunantajien, apteekkien, välittäjien ja Kansaneläkelaitoksen on päivitettävä aiemmat tietosuojaan, tietoturvallisuuteen ja tietojärjestelmien käyttöön liittyvät tietoturvasuunnitelmansa tämän määräyksen mukaisesti.

Sirpa Soini
Johtaja

Jarmo Kärki
Yksikönpäällikkö

Liite

Tietoturvasuunnitelman mallipohja

Tiedoksi

Sosiaali- ja terveydenhuollon palvelunantajat
Apteekit
Välittäjät
Kansaneläkelaitos

Tietosuojavaltuutetun toimisto
Lääkealan turvallisuus- ja kehittämiskeskus Fimea
Sosiaali- ja terveysalan lupa- ja valvontavirasto Valvira
Aluehallintovirastot

Sosiaali- ja terveysministeriö
Traficom/Kyberturvallisuuskeskus
Valtiovarainministeriö
Digi- ja väestötietovirasto

Sosiaalialan osaamiskeskukset
Hyvinvointialueyhtiö Hyvil Oy

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/aiheet/tiedonhallinta-sosiaali-ja-terveysalalla/maaraykset-ja-maarittelyt/maaraykset