[MÄÄRÄYS 2/2015, LIITE 1, DNRO. THL/1305/4.09.00/2014]
[OMAVALVONTASUUNNITELMAN MALLIPOHJA]

[Omavalvonnan kohteen nimi]

OMAVALVONTASUUNNITELMA

[Päiväys ja mahdolliset versiotiedot]
[Laatijat]
[Mahdolliset hyväksymismerkinnät]

Sisältö

[Tämä määräyksen liite on dokumenttipohja, joka on tarkoitettu omavalvontasuunnitelman tuottamisen tueksi omavalvonnan kohteille. Mallipohjadokumentin rakenne tai sisällön yksityiskohdat eivät ole sitovia vaan dokumentti on informatiivinen. Varsinaisessa suunnitelmassa on kuvattava kaikki määräyksen mukaiset seikat, jotka ovat relevantteja omavalvonnan kohteen kannalta. Määräys sisältää tarkempia vaatimuksia useisiin dokumenttipohjan kohtiin.

Suunnitelman lopullinen rakenne ja sisältö on muodostettava suunnitelman käyttäjille tarkoituksenmukaisesti, ja esimerkiksi ne määräyksen seikat jotka eivät ole sovellettavissa omavalvonnan kohteen toiminnassa voidaan todeta suunnitelman liitteessä. Suunnitelmaan on mahdollista täydentää myös muita kohteen kannalta olennaisia seikkoja.

Suunnitelman sisällön tai siinä viitattujen muiden dokumenttien pohjalta on tarvittaessa pystyttävä todentamaan]

1 Johdanto

Sosiaali- ja terveydenhuollon palvelun antajien, apteekkien ja itsenäisten ammatinharjoittajien, Kansaneläkelaitoksen sekä Kanta-välityspalveluiden tuottajien tulee tehdä omavalvontasuunnitelma. (Määräys 2/2015,THL/1305/4.09.00/2014). Suunnitelman avulla ylläpidetään ja kehitetään organisaation tietoturvaa ja tietosuojaa.

[Terveydenhuollon palvelun antajat, jotka ovat jo liittyneet Kanta-palveluihin, ovat tehneet ennen liittymistään tietoturvan itseauditoinnin. Omavalvontasuunnitelma on jatkoa itseauditoinnille ja tulee korvaamaan sen.]

[Kuvataan tarvittaessa ennen omavalvontasuunnitelman tekemistä tehdyt auditoinnit ja tehdyt tarkastukset]

[Omavalvontasuunnitelmassa viitataan aina kuin mahdollista olemassa oleviin erikseen ylläpidettäviin ohjeisiin ja dokumentteihin. Olennaista on, että suunnitelman linkkien tai tietojen avulla on selvää, mistä dokumentaatio on löydettävissä tai vaatimuksen täyttyminen on todennettavissa. Mikäli muuta valmista dokumentaatiota ei ole olemassa tai saatavissa, on mahdollista kuvata vaadittavat asiakokonaisuudet ja toimintatavat suoraan omavalvontasuunnitelmaan.]

2 Suunnitelman kohde

Tämän omavalvontasuunnitelman piiriin kuuluvat:
[Kappaleessa selvitetään se taho tai ne tahot, jota tämä omavalvontasuunnitelma koskee (sosiaali- ja/ tai terveydenhuollon palvelun antajat, apteekit ja itsenäiset ammatinharjoittajat, Kansaneläkelaitos sekä Kanta-välityspalveluiden tuottajat).]

[Kuvaus suunnitelman hyödyntämisestä tietojärjestelmien käytössä, käytön valvonnassa, hankinnoissa ja kehitystyössä ja tähän mahdollisesti liittyvistä päätöksistä]

[Omavalvontasuunnitelman toteutumisen seurannan menettelyt]

3 Yleiset tietoturvakäytännöt

[Ajantasaiset kuvaukset seuraavista tai viittaukset ajantasaisiin kuvauksiin:]

[Viittaus mahdollisesti noudatettava erillinen tietoturvapolitiikka sekä tiedot sen tarkastamisen ja kehittämisen käytännöistä

[Yleistiedot tietoturvan vastuutuksesta, organisoinnista, seurannasta ja valvonnasta sekä tietosuojavastaavista]

Koulutus, ohjeistus ja käyttökokemus ja niiden seuranta

[Mahdolliset viittaukset erillisiin koulutus- ja/tai osaamisen ja käyttökokemuksen seurannan suunnitelmiin]

[Miten varmistetaan, että henkilöstölle on annettu koulutus tietojärjestelmien käyttöön, potilas- ja asiakastietojen käsittelyyn sekä tietosuoja- ja tietoturva-asioihin. Lisäksi tulee kuvata miten seurataan ja ylläpidetään henkilöstön osaamista ja kokemusta.]

Toimintamallien koulutus ja perehdytys

[Miten huolehditaan toimintamallien perehdytykseen ja koulutukseen liittyvistä toimintatavoista ja koulutussuunnitelmista sekä miten koulutusten toteutumista ja oppimista seurataan (esim. todistukset tai ylläpidettävät tiedot koulutuksiin osallistumisista).]

Tietojärjestelmien käyttökoulutus

[Miten huolehditaan tietojärjestelmien käyttökoulutukseen liittyvistä toimintatavoista ja koulutussuunnitelmista sekä miten koulutusten toteutumista ja oppimista seurataan (esim. todistukset tai ylläpidettävät tiedot koulutuksiin osallistumisista).]

Riittävä kokemus

[Miten varmistetaan ja todennetaan käytössä olevien asiakas- ja / tai potilastietojärjestelmien käytön vaatima kokemus. Käytön vaatimaa kokemusta voidaan kartuttaa tarvittaessa myös koulutuksella tai perehdytyksellä, jos käyttäjä ei ole aiemmin järjestelmää käyttänyt tai käyttökokemus on vähäistä. Tarvittavan perehdytyksen osalta voidaan viitata kohdan ”Tietojärjestelmien käyttökoulutus” käytäntöihin. Miten on järjestetty käyttäjien ohjaus.]

Ohjeet ja koulutus potilastietojen käsittelystä

[Miten ohjeet potilastietojen käsittelystä ja palvelujen antajan henkilöstön koulutuksesta potilastietojen käsittelyyn sekä henkilöstön tietämyksen ylläpito on dokumentoitu ja todennettavissa]

4 Käyttöympäristön ja useiden järjestelmien yhteiset tietoturvakäytännöt

[Mistä saatavissa seuraavat tiedot, tai kuvaukset osana suunnitelmaa:]

Menettelyt virhe- ja ongelmatilanteissa

[Miten menetellään virhe- ja ongelmatilanteiden selvittämisessä, tarvittaessa erilaiset virhe- ja ongelmatilanteet erikseen (verkko- tai tietoliikenneongelmat, järjestelmien käyttöön liittyvät ongelmat, havaittujen tai toteutuneiden tietoturva- tai tietosuoja-uhkien tai ongelmien hallinta jne.). Vastuut virhe- ja poikkeustilanteissa]

[Luokan A tai luokan B järjestelmien olennaisten vaatimusten täyttymisessä havaittujen merkittävien poikkeamien ilmoittaminen tietojärjestelmän valmistajalle]

[Luokan A tai luokan B järjestelmien merkittävien poikkeamien ilmoittaminen Valviralle, jos poikkeama aiheuttaa merkittävän riskin potilasturvallisuudelle]

Järjestelmien käyttöohjeiden hallinnointi ja saatavuus

[Miten asiakas- ja / tai potilastietojärjestelmien käyttöohjeiden hallinnointi ja ohjeiden saatavuus sekä henkilöstön perehdyttäminen ohjeisiin on yleisesti dokumentoitu ja todennettavissa. Valmistajien ohjeiden hallintakäytännöt, päivittäminen ja jakelu.]

[Miten tietojärjestelmäpalvelun tuottajalta saadaan tai hankitaan ajantasaiset ja riittävät käyttöohjeet]

[Miten käyttöohjeiden päivittäminen ja jakelu toteutetaan ohjelmistojen ja niiden versiopäivitysten sekä muiden muutosten yhteydessä.]

[Miten varmistetaan ja todennetaan, että tietojärjestelmiä käytetään valmistajan antamien ohjeistusten mukaisesti tai niitä tarkoituksenmukaisesti soveltaen tai täydentäen.]

Järjestelmien asennus ja ylläpito yleisesti

[järjestelmäkohtaisille seikoille on paikka luvussa 8, jos ne poikkeavat tässä määritellyistä käytännöistä]

[Järjestelmien asennuksen, ylläpidon ja päivityksen roolit ja vastuut yleisesti]

[Ylläpitotehtävien vaatima ammattitaito ja asiantuntemus yleisesti]

[Järjestelmien muutoshallinnan, testauksen ja hyväksymisen menettelyt]

Tilojen, työasemien, tallennusvälineiden ja tulosteiden turvallisuus

[Suojattavat fyysiset tilat ja niiden suojauskäytännöt]

[Työasemien sijoittuminen, lukittuminen ja suojaaminen sivullisilta]

[Työasemien viruksilta ja haittaohjelmilta suojautuminen]

[Mobiililaitteiden ja –ympäristöjen suojauskäytännöt, PIN-koodien hallinta, SIM-korttien hallinta, ohjelmalliset suojaukset]

[Oheisohjelmistojen asentaminen työasemilla, palvelimilla ja mobiililaitteissa]

[Tulosteiden turvallisuus ja tulosteiden turvallisen käsittelyn käytännöt]

[Ulkoiset tallennuslaitteet ja tallennusvälineet]

Muut käyttöympäristön käytännöt.

[Yleiset käyttöympäristön tukipalvelut]

[Tietoliikenneoperaattorit ja tietoliikenteen tietoturvaan liittyvät vastuut ja sopimukset]

[Etäyhteydet ja niiden tietoturva]

[Langattomat verkot ja reitittimet ja niiden tietoturva]

5 Käyttövaltuuksien, pääsynhallinnan ja käytön seurannan yleiset käytännöt

[Ajantasaiset kuvaukset seuraavista tai viittaukset ajantasaisiin kuvauksiin:]

[järjestelmäkohtaisille seikoille on paikka luvussa 8, jos ne poikkeavat tässä määritellyistä käytännöistä]

Käyttäjäryhmät

[Mistä on saatavissa dokumentaatio niistä käyttäjäryhmistä, jotka käyttävät asiakas- ja/tai potilastietojärjestelmiä. Kanta-palveluihin liittyvien tahojen osalta tulee myös olla dokumentoituna käyttäjäryhmien Kanta-palveluiden käyttöoikeudet.]

Käyttövaltuushallinnan ja käytön seurannan käytännöt

[Käyttövaltuuksien hakemisen, myöntämisen, seurannan, muuttamisen, tarkistamisen / varmistamisen ja poistamisen käytännöt]

[Käyttäjien tunnistamisen ja todentamisen käytännöt]

[Lokien hallinnan ja käytön seurannan käytännöt]

[Toimintamalli havaittaessa lainvastaista asiakas- tai potilastietojen käsittelyä]

[Kelan lokitietojen saanti ja hankinta seurannan ja valvonnan toteuttamiseksi]

6 Kanta-palvelujen käytön tietoturvakäytännöt

[Ajantasaiset kuvaukset seuraavista tai viittaukset ajantasaisiin kuvauksiin:]

[Nämä seikat on mahdollista kuvata myös aiempien lukujen vastaavien kohtien yhteydessä tai järjestelmäkohtaisesti (luku 8)]

[Valtakunnallisten palvelujen tietoturvallisen käytön edellyttämien vaatimusten varmistaminen]

[Kanta-palveluiden edellyttämien tunnistamis- ja todentamisratkaisujen toteuttaminen]

[Kanta-palveluiden edellyttämien varmenneratkaisujen toteuttaminen (eri tyyppiset varmenteet)]

[Kanta-palveluiden edellyttämien käyttövaltuuksien hallinta ja kytkentä työntekijöiden työrooleihin]

[Kanta-palveluiden käytön seuranta]

[Kanta-palveluiden pääsynhallinnan toteuttaminen]

[Sosiaalihuollon ja terveydenhuollon dokumenttien ja eri rekisterien erottaminen]

[Vaatimustenmukaisuustodistuksen edellyttäminen Kanta-palveluihin liittyviltä tietojärjestelmiltä ja välityspalveluilta]

[Toiminta ja vastuut tilanteessa, jossa käytössä olevalta järjestelmältä peruutetaan vaatimustenmukaisuustodistus määräajaksi tai kokonaan jossa vaatimustenmukaisuustodistusta rajoitetaan, tai tilanteessa jossa tietojärjestelmän käyttö kielletään]

7 Tietojärjestelmät

[Esimerkiksi viittaus ylläpidettävään ja ajantasaiseen tietojärjestelmäsalkkuun tai tietojärjestelmäportfolioon, tai luettelo käytettävistä järjestelmistä]

Kanta-palveluihin liittyvät tietojärjestelmät (luokka A)
-järjestelmä, versio, toimittaja, yhteystiedot, vaatimustenmukaisuustodistus

-järjestelmä, versio, toimittaja, yhteystiedot, vaatimustenmukaisuustodistus

Muut asiakas- tai potilastietoja käsittelevät järjestelmät (luokka B)
-järjestelmä, versio, toimittaja, yhteystiedot
-järjestelmä, versio, toimittaja, yhteystiedot

Muut tietojärjestelmät, jotka on otettava huomioon arkaluonteisten asiakas- ja potilastietojen suojaamisen kannalta
-järjestelmä, versio, toimittaja, yhteystiedot

8 Tietojärjestelmäkohtaiset ohjeet ja suunnitelmat

[Viittaukset järjestelmäkohtaisiin kuvauksiin tai järjestelmäkohtaisia alaosioita tässä dokumentissa. Soveltuvin osin eri kohtiin voidaan käyttää samantyyppisiä kuvauksia kuin aiempien kappaleiden vastaavissa osissa. Vain järjestelmät, joilla vaikutusta asiakas- tai potilastietojen käsittelyyn, tietoturvaan ja tietosuojaan]

8.1 Järjestelmä X (luokkaan A kuuluva)

-järjestelmä, versio, toimittaja, yhteystiedot
-käyttötarkoitus
-käyttäjäryhmät
-käyttöohjeet
-ohjeiden päivittäminen ja jakelu
-menettelyt virhe- ja ongelmatilanteissa
-järjestelmäkohtaiset tukipalvelut
-asennus- ja ylläpitovastuut ja -vaatimukset
-menettelytavat ja vastuut virhe- ja poikkeustilanteissa
-käyttövaltuushallinta järjestelmässä
-tunnistautuminen järjestelmässä
-lokit
-järjestelmän lukittuminen
-Kantaan liittyvän järjestelmän vaatimustenmukaisuustodistuksen tietojen varmistaminen
-järjestelmän tiedot Valviran rekisterissä

8.2 Järjestelmä Y (luokkaan B kuuluva)

-järjestelmä, versio, toimittaja, yhteystiedot
-käyttötarkoitus
-käyttäjäryhmät

-käyttöohjeet
-ohjeiden päivittäminen ja jakelu
-menettelyt virhe- ja ongelmatilanteissa
-järjestelmäkohtaiset tukipalvelut
-asennus- ja ylläpitovastuut ja -vaatimukset

-menettelytavat ja vastuut virhe- ja poikkeustilanteissa
-käyttövaltuushallinta järjestelmässä
-tunnistautuminen järjestelmässä
-lokit
-järjestelmän lukittuminen
-järjestelmän tiedot Valviran rekisterissä

8.2 Järjestelmä Y (muu järjestelmä)

-järjestelmä, versio, toimittaja, yhteystiedot
-käyttötarkoitus
-käyttäjäryhmät

[tarvittavin ja soveltuvin osin]:
-käyttöohjeet
-ohjeiden päivittäminen ja jakelu
-menettelyt virhe- ja ongelmatilanteissa
-järjestelmäkohtaiset tukipalvelut
-asennus- ja ylläpitovastuut ja -vaatimukset
-menettelytavat ja vastuut virhe- ja poikkeustilanteissa
-käyttövaltuushallinta järjestelmässä
-tunnistautuminen järjestelmässä
-lokit
-järjestelmän lukittuminen