Siun työterveys Oy:n tietosuojan ja tietoturvallisuuden omavalvontasuunnitelma

1. Johdanto

Sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetun lain 19 h §:n mukaan sosiaalihuollon ja terveydenhuollon palvelujen antajan on laadittava tietoturvaan ja tietosuojaan sekä tietojärjestelmien käyttöön liittyvä omavalvontasuunnitelma. Omavalvontasuunnitelman tarkoituksena on varmistaa, että palvelujen antajan henkilökunta hallitsee käytössään olevien tietojärjestelmien käytön ja osaa ottaa huomioon asiakas- ja potilastietojen salassapitoon ja tietoturvaan liittyvät vaatimukset. Lisäksi omavalvontasuunnitelmassa huomioidaan tietojärjestelmien käyttöympäristöön, ylläpitoon ja päivitykseen liittyvät asiat.

Viime kädessä vastuu omavalvontasuunnitelman noudattamisesta on toimintayksikön vastaavalla johtajalla, mutta jokaisen on huolehdittava osaltaan tietosuojan ja tietoturvan toteuttamisesta.

2. Suunnitelman kohde

Tämän omavalvontasuunnitelman piiriin kuuluvat kaikki Siun työterveys Oy:n terveyspalveluja tuottavat yksiköt sekä yhtiön lukuun toimivat yksityiset palveluntuottajat. Pääasiallinen potilas- ja asiakastietojärjestelmä on Mediatri. Siun työterveys Oy aloittaa toimintansa 1.1.2019.

Pohjois-Karjalan Tietotekniikkakeskus Oy (jatkossa PTTK Oy) tuottaa ICT-palvelut (mm. tietoliikenne-, työasema-, tietojärjestelmä-, tietoturva- ja tukipalvelut) Siun työterveys Oy:lle.

3. Yleiset tietoturvakäytännöt

Siun työterveys Oy:lle on valmistumassa **tietoturvapolitiikka**, jossa tietoturvan vastuutus, organisointi, seuranta ja valvonta on kuvattu. Lisäksi Siun työterveys Oy:lle laaditaan käyttäjiä varten potilasrekisterin tietosuojaohjeet.

Siun työterveydelle on valmistumassa **tietosuojan seuranta- ja valvontasuunnitelma**, jossa määritellään tietosuojan valvonnan organisointi, periaatteet ja toteutus sekä seuraamukset väärinkäyttötapauksissa.

Vastuu tietoturvan ja tietosuojan käytänteistä on yhtiön toimitusjohtajalla. Toimitusjohtajan alaisuudessa toimii tietosuojavastaava. Tietoturvan ja tietosuojan toteuttaminen kuuluu jokaiselle yhtiön työntekijälle.

Tietosuojan ohjausryhmänä toimii johtoryhmä.

4. Henkilöstön koulutus, ohjeistus ja käyttökokemus sekä niiden seuranta

Tietoturva ja tietosuoja

Tietoturva ja tietosuoja-asiat käydään läpi työntekijän perehdytyksessä. Riittävästä perehdytyksestä vastaa lähiesimies. Tietoturvaan ja tietosuojaan liittyvä ohjeistus löytyy yhtiön intrasta. Tietosuoja-asiantuntijat järjestävät tietoturvaan ja -suojaan liittyvää koulutusta esimiehen pyynnöstä toimintayksiköiden henkilöstölle. Työntekijät suorittavat verkossa Kanta-palvelun tietosuojakoulutuksen. Lisäksi on käytössä organisaation sisäinen web-pohjainen tietosuojakoulutus.

Tietojärjestelmät

Lähiesimiehellä on ensisijainen vastuu järjestää työntekijöille riittävä koulutus ja perehdytys tietojärjestelmien käyttöön. Koulutuksen toteuttamisesta vastaavat järjestelmien pääkäyttäjät. He myös antavat pyydettäessä lisäohjausta tietojärjestelmien käyttöön.

5. Käyttöympäristön ja useiden järjestelmien yhteiset tietoturvakäytännöt

Järjestelmien asennus ja ylläpito sekä tietoliikenne

Tietojärjestelmien asennuksesta ja ylläpidosta sekä tietoliikenteen suojauksesta vastaa PTTK Oy. Suojauksen periaatteet on kerrottu Siun työterveys Oy:n tietoturvasuunnitelmassa. Palvelimet ja konesalit ovat PTTK Oy:n hallinnassa. PTTK Oy tekee erilliset sopimukset etäyhteyksistä järjestelmätoimittajien kanssa. Sopimuksissa noudatetaan organisaation tietoturva- ja tietosuojaohjeistuksia.

Tilojen, työasemien, tallennusvälineiden ja tulosteiden turvallisuus

Tilojen fyysisen turvallisuuden suunnittelusta ja toteutuksesta on tarkemmat ohjeet Siun työterveyden tietoturvasuunnitelmassa.

Laitteet (mm. työasemat ja tulostimet) on sijoitettu niin, etteivät sivulliset pääse näkemään asiakastietoja. Ohjeet tietojenkäsittely- ja viestintävälineiden tietoturvalliseen käyttöön löytyvät yhtiön intrasta.

PTTK Oy vastaa virustorjunnasta sekä siihen liittyvästä käyttäjien ohjeistuksesta.

PTTK Oy vastaa asiakastietojärjestelmien tietoaineistojen varmuuskopioinnista.

Potilas- ja asiakastietoja sisältävät asiakirjat säilytetään lukituissa kaapeissa ja tietoja käsittelevien työntekijöiden huoneet ovat lukittuina huoneiden ollessa tyhjillään.

Tuhottavat paperidokumentit laitetaan niille erikseen varattuihin lukittuihin säiliöihin tai tietoturvallisiin paperisilppureihin. Säiliöiden tyhjentämisestä huolehtii palvelua tarjoava yhtiö.

Sähköiset tallennuslaitteet (muistitikut, CD-levyt ym.) kerätään tietosuojajätelaatikkoon tai lähetetään tuhottavaksi PTTK Oy:lle. PTTK Oy vastaa myös käytöstä poistettavien laitteiden kiintolevyjen tyhjentämisestä tietoturvallisesti.

Menettelyt virhe- ja ongelmatilanteissa

Järjestelmien ja tietoteknisten laitteiden ongelmien selvityspyynnöt välitetään ServiceDesk-järjestelmän kautta PTTK Oy:lle.

Tarkemmat ohjeet tietoturvatoimenpiteistä ja -menettelyistä poikkeamatilanteissa on Siun työterveys Oy:n tietoturvasuunnitelmassa.

6. Käyttövaltuuksien, pääsynhallinnan ja käytön seurannan yleiset käytännöt

Siun työterveydessä on yleisesti käytössä yksilölliset käyttäjätunnukset eri järjestelmiin. Potilastietojärjestelmään tunnistaudutaan henkilökohtaisella sähköisellä toimikortilla. Siun työterveys Oy:n asiakas- ja potilastietojen valvontasuunnitelmassa on kuvattu asiakas- ja potilastietojen käsittelyn seuranta ja valvonta.

Esimies myöntää työntekijälle järjestelmien käyttöoikeudet sekä voimassaoloajan työntekijän työtehtävien perusteella ja tilaa käyttäjätunnukset PTTK Oy:ltä tai järjestelmien pääkäyttäjiltä. Työntekijä allekirjoittaa salassapito- ja käyttäjäsitoumuksen.

Potilas- ja asiakastietojärjestelmät tuottavat käyttölokitietoja, jotka ovat vain tietosuojavastaavien käytössä. Tietosuojavastaavat suorittavat seuranta- ja valvontasuunnitelman mukaista lokivalvontaa.

7. Tietojärjestelmät

PTTK Oy vastaa tietojärjestelmäluetteloista sekä tietojärjestelmäselosteista ja -kuvauksista. Tietojärjestelmien kriittisyystasot on määritelty PTTK Oy:n kanssa yhteistyössä.

8. Raportointi

Toimitusjohtaja, johtava lääkäri ja tietosuojavastaavat laativat yhteistyössä EU:n tietosuoja-asetuksen mukaisen tietotilinpäätöksen Siun työterveys Oy:n johtoryhmälle kerran vuodessa.

9. Suunnitelman päivitys ja toteutumisen seuranta

Siun työterveys Oy:n tietosuojan ja tietoturvallisuuden omavalvontasuunnitelman hyväksyy Siun työterveyden toimitusjohtaja. Suunnitelmaa päivitetään tarpeen mukaan tai vähintään kerran kahdessa vuodessa. Vastuu päivittämisestä on tietosuojavastaavalla.