Tietoturvapolitiikka

Hallitus 12.6.2018 § 63

VARSINAIS-SUOMEN SAIRAANHOITOPIIRIN TIETOTURVAPOLITIIKKA

1. JOHDANTO

Tietoturvapolitiikka määrittää ne periaatteet, toimintatavat, vastuut, valvonnan ja seuraamusjärjestelmän, joita noudatetaan Varsinais-Suomen sairaanhoitopiirin kuntayhtymän tietoturvan toteuttamisessa ja kehittämisessä.

Sairaanhoitopiirin palveluiden perustana ovat potilaidemme tarpeet. Palveluiden tuottaminen perustuu tietoon ja sen käsittelyyn sairaanhoitopiirin ja sen konsernin toimintaympäristöissä. Sairaanhoitopiirin palvelutuotanto on riippuvainen ICT-teknologiasta ja -palveluiden keskeytyksettömästä ja turvallisesta toiminnasta.

Tietoturvallisuus ja tietosuoja on huomioitava kaikessa toiminnassa jo suunnitteluvaiheessa. Sairaanhoitopiirin hallitus tietoturva- ja tietosuojatoiminnan omistajana määrittelee tässä politiikassa johtamiseen, palveluihin ja toimintoihin liittyvät tietoturvaperiaatteet, vastuut ja tavoitteet. Politiikka toimii perustana sairaanhoitopiirin tietoturvasuunnitelmalle ja muille tietoturvaa koskeville toimintaohjeille, joiden tehtävänä on tarkentaa politiikassa annettuja määräyksiä ja ohjeistaa niiden soveltamista käytäntöön.

Tietosuojatoiminnan periaatteet on määritelty sairaanhoitopiirin tietosuojapolitiikassa.

Sairaanhoitopiirin hallituksen vahvistama tietoturvapolitiikka kattaa konsernin kaikkeen toimintaan liittyvät tietojen käsittelyn tehtävät. Jokaisen sairaanhoitopiirin kuntayhtymän viranhaltijan, työntekijän ja luottamushenkilön sekä sairaanhoitopiirin tietojen ja tietojärjestelmien käyttäjän on tunnettava tämä tietoturvapolitiikka ja noudatettava sen perusteella annettuja ohjeita ja määräyksiä. Sairaanhoitopiirin ulkopuolisten terveydenhuollon toimijoiden, toimittajien ja muiden ulkopuolisten tahojen tulee myös sitoutua noudattamaan tätä tietoturvapolitiikkaa, kansallisia säädöksiä sekä ohjeita ehtona tehtäviensä mukaiselle pääsylle sairaanhoitopiirin tietojärjestelmiin ja niiden sisältämiin tietoihin.

2. TIETOTURVAN MÄÄRITELMÄ

Tietoturvallisuus koostuu tietoturvaan ja tietosuojaan liittyvistä vastuista ja käytännöistä, joilla pyritään varmistamaan tietojen, tietojärjestelmien ja palvelujen turvaaminen siten, että niiden luottamuksellisuus, eheys ja saatavuus voidaan taata ja osoittaa toteutuneen.

- Luottamuksellisuus: Tieto on vain siihen oikeutettujen saatavilla.
- Eheys: Tieto on oikeaa ja eheää, eikä muuttunut tahallisen tai tahattoman teknisen tai inhimillisen toiminnan seurauksena.
- Saatavuus: Tieto on saatavilla aina sitä tarvittaessa.
- Kiistämättömyys: Tietoon tehdyt muutokset sen käsittelyn eri vaiheissa pystytään tarvittaessa todentamaan.

Tietoturvatyö on tietoturvan saavuttamiseksi tehtävien toimenpiteiden suunnittelua ja toteuttamista. Tietoturvaan kuuluvat tietoturvaorganisaatio, tietojen turvaamisen menetelmät, välineet ja toimenpiteet, työhön osoitetut resurssit sekä välineistön ja tilojen tietoturvaominaisuudet.

Tietosuojalla tarkoitetaan yksilön oikeutta henkilötietojen suojaan. Tietosuojatyön tavoitteena on lainsäädännön vaatimusten täyttäminen, asianmukaisuuden ja käyttötarkoitussidonnaisuuden takaaminen henkilötietojen käsittelyssä sekä rekisteröityjen oikeuksien tehokas toteutuminen kaikessa sairaanhoitopiirin toiminnassa.

3. TIETOTURVAN TAVOITTEET JA PERIAATTEET

Sairaanhoitopiirin tietoturvatyön päämäärä on turvata sairaanhoitopiirin toiminnalle tärkeiden tietojärjestelmien ja tietoverkkojen keskeytymätön toiminta, estää tietojen ja tietojärjestelmien joutuminen ulkopuolisille sekä estää niiden valtuudeton käyttö, tahaton tai tahallinen tiedon tuhoutuminen tai vääristyminen sekä minimoida aiheutuvat vahingot.

Normaaliajan toiminnan tietojenkäsittelyn turvaamisen lisäksi varaudutaan toiminnan keskeyttäviin uhkatilanteisiin ja niistä toipumiseen. Sairaanhoitopiirin toiminta kriisitilanteissa perustuu lakisääteiseen valmiussuunnitteluun. Suunnittelussa ja ohjaamisessa tulee varautua niin pieneen, keskisuureen, kuin suureen toimintahäiriöön sekä soveltuvin osin poikkeusoloihin.

Hyväksytyn tietoturvapolitiikan mukainen tietoturva tulee sisällyttää luonnollisena osana kaikkeen toimintaan. Tietoturvan kehittäminen ja ylläpito ovat osa sairaanhoitopiirin yleistä turvallisuustoimintaa, riskien hallintaa ja sisäistä valvontaa.

4. TIETOTURVAN ORGANISOINTI JA VASTUUT

Tietoturvaa johtaa ja valvoo sairaanhoitopiirin hallitus. Sairaanhoitopiirin johtaja päättää sairaanhoitopiirin kokonaisturvallisuuden eri osa-alueiden kehittämistoiminnan tavoitteista, organisoinnista, resursseista ja toimintavaltuuksista sekä nimeää tietoturvavastaavan. Potilastietoturvan osa-alueesta vastaa johtajaylilääkäri.

Tietoturvan kehittämisestä, toteutuksen valvonnasta, tietoturvatietouden edistämisestä ja tietoturvallisesta toimintatavasta sairaanhoitopiirissä ja sen ostamissa palveluissa sekä raportoinnista vastaa sairaanhoitopiirin johdolta saamiensa resurssien ja toimintavaltuuksien puitteissa tietoturvavastaava. Hän vastaa myös tietoturva-asioista tiedottamisesta sairaanhoitopiirin ulkopuolelle ja sairaanhoitopiirin sisällä yleisellä tasolla.

Tietoturvan kehittämisen suunnittelua ja toimeenpanon valmistelua varten sairaanhoitopiirissä toimii tietoturvaryhmä. Tietoturvaryhmään kuuluvat vähintään tietoturvavastaava, tietosuojavastaava, tietohallintojohtaja, teknillinen johtaja ja 2M-IT Oy:n tietoturvapäällikkö. Sairaanhoitopiirin johtaja nimeää tietoturvaryhmän muut jäsenet. Ryhmän jäsenten tehtävät kuvataan tarkemmin tietoturvasuunnitelmassa.

Jokaisella tietojärjestelmällä on omistajayksikkö ja vastuuhenkilö (omistaja). Tietojärjestelmän omistajan velvollisuuksiin kuuluu tietojärjestelmän toimintaan ja turvallisuuteen asetettavien vaatimusten kuten kriittisyyden, jatkuvuussuunnittelun ja varmuuskopiointimenettelyn määrittely sekä käyttöoikeuksien määrittely, myöntäminen ja valvonta.

Tietoturva-asioiden ohjeistamisesta, tiedottamisesta ja valvonnasta omassa yksikössään vastaa yksikön esimies.

Jokainen sairaanhoitopiirin työntekijä, tietoja käsittelevä, tietojärjestelmien tai tietoverkkojen ylläpitäjä ja käyttäjä on omalta osaltaan vastuussa tietoturvan toteuttamisesta sekä tietoturvaohjeiden noudattamisesta. Jokainen henkilö on velvollinen tietoturvaan liittyvien uhkien ja poikkeamien raportoimisesta esimiehelleen tai tietoturvavastaavalle.

5. TIETOTURVAN TOTEUTTAMINEN

Sairaanhoitopiirin tietoturva perustuu tietoturvaa, tietosuojaa, hyvää tiedonhallintatapaa ja tiedon laatua ohjaaviin ja velvoittaviin kansallisiin ja kansainvälisiin säädöksiin, velvoitteisiin, määräyksiin ja ohjeisiin. Lainsäädännön ja ohjeistuksen muutokset otetaan huomioon sairaanhoitopiirin tietoturvan kehittämisessä.

Tietoturvan toteuttaminen ja ylläpito kuvataan yksityiskohtaisesti tietoturvasuunnitelmassa. Tietoturvan toteutuksen tulee perustua niihin vaatimuksiin, joita toiminta ja palvelut sekä kunkin tiedon ja tietojärjestelmän turvallisuus- ja kriittisyysluokitus asettavat tietojenkäsittelyn varmuudelle, käytettävyydelle, salassapidolle, laadulle ja toiminnan jatkuvuudelle sekä toimintaan kohdistuvien riskien arvioinnille. Vaatimusten selvittäminen, riskien arvioiminen ja niiden perusteella turvallisuustoimenpiteiden määritteleminen tapahtuu säännöllisesti suoritettavilla turvallisuusanalyyseillä.

Tietoturvan tavoitteiden saavuttaminen on jatkuva prosessi, joka tapahtuu hallinnollisten ja teknisten ratkaisujen avulla. Ne kuvataan tietoturvasuunnitelmassa ja tarvittaessa käyttöympäristöille ja yksiköille laadituissa erillisissä tietoturvan kehittämissuunnitelmissa. Keskeiset kehittämistoimet toteutetaan hankkeina, joista tehdään hankesuunnitelma.

Käyttäjien toimintaa ohjataan tietoturvasuunnitelmaan sisältyvillä käyttösäännöillä sekä vahvistetuilla ja saatavilla olevilla toimintaohjeilla sekä tietoturva- ja tietosuojakoulutuksella. Jokainen käyttäjä allekirjoittaa käyttäjän tietosuojaohjeen ja sitoumuksen saadessaan oikeuden tehtäviensä mukaiseen tietojärjestelmien käyttöön.

Sairaanhoitopiirin solmimissa sopimuksissa tulee huomioida tietoturvaan ja tietosuojaan liittyvät vastuut ja velvoitteet.

6. TOIMINTA TIETOTURVA- JA TIETOSUOJAPOIKKEAMATILANTEISSA SEKÄ ILMOITUSVELVOLLISUUS

Sairaanhoitopiirissä on määritetty toimintaprosessi tietoturva- ja tietosuojapoikkeamatilanteisiin. Tietoturvapoikkeamat ilmoitetaan, käsitellään ja rekisteröidään toimintaohjeen mukaisesti. Tietoturvapoikkeamat ilmoitetaan tarvittaessa valvontaviranomaiselle voimassaolevan kansallisen lainsäädännön ja ohjeistuksen mukaisesti. Henkilötietoihin kohdistuvien tietoturvapoikkeamien käsittely on kuvattu tietosuojapolitiikassa.

7. RIKKOMUKSET JA SEURAAMUKSET

Jokainen sairaanhoitopiirin tietojärjestelmien käyttäjä on sitoutunut noudattamaan organisaation tietosuoja- ja tietoturvaperiaatteita allekirjoittamalla tietosuojasitoumuksen, ja periaatteiden noudattamista seurataan. Tietosuojasitoumuksen ja toimintaohjeiden sekä lainsäädännön vastainen toiminta käsitellään tapauskohtaisesti. Tietoturvarikkomusten mahdollisiin seuraamuksiin sovelletaan toimintaohjetta ja tietoturvarikkomukset raportoidaan sairaanhoitopiirin johdolle ja tietoturvavastaavalle.