



Etelä-Pohjanmaan sairaanhoitopiirin tietoturva- ja tietosuojapolitiikka

Tämä tietoturva- ja tietosuojapolitiikka on hyväksytty Etelä-Pohjanmaan sairaanhoitopiirin yhtymähallituksessa 21.2.2011 - Etelä-Pohjanmaan sairaanhoitopiirin kuntayhtymän (myöhemmin sairaanhoitopiiri) yleiseksi tietoturva- ja tietosuojapolitiikaksi.

1 Johdanto

Tietojenkäsittely tukee sairaanhoitopiirin palvelujen tuottamista. Tietoaineistot sisältävät potilaisiin, työntekijöihin ja toimintaan liittyvää tietoa, joka on lainsäädännön perusteella suojattava. Tietojenkäsittelyn on oltava mahdollisimman tehokasta, virheetöntä ja varmaa. Tietojenkäsittelyyn liittyy aina inhimillisenä toimintana riskejä, joita minimoidaan mm. ohjeistuksilla, teknisillä ratkaisulla ja koulutuksella. Vain pieni osa tietoturvariskeistä pystytään välttämään teknisillä ratkaisulla. Tärkeintä on jokaisen meistä päivittäin tietoja käsitellessämme tekemät ratkaisut ja toimenpiteet.

Tietoturva- ja tietosuojapolitiikka määrittelee ne periaatteet, vastuut, toimintatavat sekä seurannan ja valvonnan, joita sairaanhoitopiirissä noudatetaan tietoturvan toteuttamisessa ja kehittämisessä. Tietoturva- ja tietosuojapolitiikkaa täydentävät hallinnollinen tietoturvasuunnitelma ja koko henkilökunnalle annetut ohjeet.

Sairaanhoitopiirin henkilökunnan ja sen luottamushenkilöiden sekä ulkopuolisten terveydenhuollon toimijoiden, toimittajien ja muiden ulkopuolisten tahojen tulee sitoutua noudattamaan tätä tietoturva- ja tietosuojapolitiikkaa, kansallisia normeja sekä ohjeita. Tämä ehto koskee osapuolia, joiden tehtävät edellyttävät pääsyä sairaanhoitopiirin tietojärjestelmiin ja tietoaineistoihin.

2 Tietoturva

Tietoturva tarkoittaa tietojen käsittelyn ja arkistoinnin turvaamista. Tietoturva rakentuu tiedon luottamuksellisuudesta, eheydestä, saatavuudesta, käytettävyydestä ja kiistämättömyydestä sekä tietojen käsittelyn valvonnasta. Tietoturvan hallintaan liittyvät tietoturvaorganisaatio, tietojen käsittelijöiden toimintatavat, tietojen turvaamisen menetelmät, välineet ja toimenpiteet, työhön osoitetut resurssit sekä välineistön ja tilojen tietoturvaominaisuudet.

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

Tietoturvatyö on tietoturvan saavuttamiseksi tehtävien toimenpiteiden suunnittelua ja toteuttamista. 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 ongelmat. Normaaliajan toiminnan tietojenkäsittelyn turvaamisen lisäksi varaudutaan toiminnan keskeyttävään uhkatilanteisiin ja niistä toipumiseen.

3 Tietosuoja

Tietosuoja on oleellinen osa tietoturvaluottisuutta. Tietosuojalla tarkoitetaan henkilötietojen ja muiden henkilön luottamuksellisten tai arkaluonteisten tietojen suojaamista.

Lainsäädäntö suojaa henkilötietoja usein tarkemmin kuin organisaation käytössä olevia muita luottamuksellisia tietoja. Tietosuojalainsäädäntö edellyttää, että henkilötietojen käsittely on turvattava ja henkilötiedot on suojattava asiattomalta käsittelyltä. Henkilötietojen oikeellisuus on varmistettava, ne on pidettävä salassa ulkopuolisilta, niitä ei saa tuhota tai käsitellä asiattomasti ja niiden on oltava tarpeen mukaan käytettävissä. Tietosuojalainsäädännössä säädetään lisäksi monista oikeuksista, joita henkilöllä on omiin tietoihinsa. Terveystenhuollon ammattihenkilökunnan toimintaa ohjaavat lain- ja määräysten mukaiset velvollisuudet ja oikeudet sekä näiden lisäksi ammattietiikka, johon sisältyy vastuu hyvästä toimintatavasta ja velvollisuus tietojen salassapidosta ja vaitiolosta.

Potilastietojärjestelmästä saa hakea työtehtävien hoitamiseksi hoidettavan potilaan tietoja ainoastaan tarvittavassa laajuudessa. Potilaalta ei tarvitse erikseen pyytää suostumusta toisessa Etelä-Pohjanmaan sairaanhoitopiiriin julkisen terveydenhuollon toimintayksikössä laadittujen potilasasiakirjojen käyttöön. Potilas voi halutessaan kieltää yksiköiden välisen tietojen luovutuksen osittain tai kokonaan.

Yksityisiltä tai Etelä-Pohjanmaan sairaanhoitopiiriin alueen ulkopuoliselta julkiselta toimintayksiköltä pyydettyihin ja annettuihin potilastietoihin tarvitaan potilaan kirjallinen suostumus.

Potilaan tajuttomuustila vaikeassa loukkaantumisessa, potilaan vajaakykyisyys päättää itse asiasta, oikeusviranomaisen määräämä pakkokeino tai hallinnollinen peruste terveydenhuollon yksikön sisällä oikeuttaa terveydenhuollon yksikön käsittelemään potilaan tietoja.

Potilasta koskevien tietojen käytön asianmukaisuuden varmistamiseksi suoritetaan lain vaatimaa valvontaa.

4 Organisaatiot ja vastuut

Tietoturvaluottisuus on koko sairaanhoitopiiriin yhteinen asia. Tietoturvaluottudesta vastaa sairaanhoitopiiriin hallitus ja sitä johtaa **sairaanhoitopiiriin johtaja**. Sairaanhoitopiiriin hallitus päättää sairaanhoitopiiriin kokonaisturvaluottisuuden eri osa-alueiden kehittämistoiminnan tavoitteista, organisoinnista, resursseista ja toimintavaltuuksista sekä nimeää tietoturvaluottavastaavan ja tietosuojavastaavan. Potilastietojen tietoturvaluottavasta vastaa **johtajaylilääkäri**.

Tietoturvaluottava vastaa osaltaan sairaanhoitopiiriin tietoturvaluottotyön kokonaisuudesta johdolta saamiensa resurssien ja toimintavaltuuksien puitteissa.



Tietoturvavastaava vastaa sairaanhoitopiirin tietoturvaluustason määrittämisestä, arvioinnista ja raportoinnista sekä muusta hallinnollisesta tietoturvasta. Hän vastaa hallinnollisen tietoturvasuunnitelman tekemisestä, toteutuksen valvonnasta, tietoturvatietouden edistämisestä.

Sairaanhoitopiirin potilastietoja sisältävien henkilörekistereiden suojaamisesta ja valvonnasta vastaa osaltaan **tietosuojavastaava**. Tietosuojavastaava osallistuu suunnittelutoimintaan, ohjeiden valmistelun ja ylläpitoon sekä tietosuojakoulutuksiin. Tietosuojavastaava tukee henkilökuntaa ja rekisteröityjä tietosuoja-asioissa sekä seuraa ja valvoo henkilötietojen käsittelyä sekä suojausmenettelyä.

Tietoturva- ja tietosuojavastaavilla on velvollisuus ryhtyä toimenpiteisiin havaittujen tietoturvan heikkouksien korjaamiseksi. Tietoturva- ja tietosuojavastaava raportoivat sairaanhoitopiirin hallitukselle kerran vuodessa tietoturva- ja tietosuojaryhmää kuultuaan.

Tietoturva- ja tietosuojavastaavien toiminnan tukena on **tietoturva- ja tietosuojaryhmä**, jonka asettaa sairaanhoitopiirin johtoryhmä. Tietoturva- ja tietosuojaryhmä käsittelee tietoturvan linjaukset ja ohjeet ennen kuin ne esitellään johdolle hyväksyttäväksi. Ryhmään kuuluvat ainakin tietoturvavastaava, tietosuojavastaava, tietohallintojohtaja, henkilöstöjohtaja, arkistopäällikkö, turvallisuuspäällikkö, lääketieteellinen toiminta-aluejohtaja ja ylihoitaja.

Tietoturvavastaava toimii tietoturva- ja tietosuojaryhmän puheenjohtajana ja tietosuojavastaava varapuheenjohtajana. Ryhmän jäsenet vastaavat oman vastualueensa tietoturvaprosessin asioiden valmistelusta. Hoidollisten palveluiden osa-alueiden edustajat tuovat eri käytännön työn näkemykset tietoturvatyöhön. Ryhmä ottaa tarvittaessa kantaa valmisteltaviin asioihin.

Jokaisella tietojärjestelmällä on **omistajayksikkö ja pääkäyttäjä**. Laajemmilla järjestelmillä voi olla myös erikseen **vastuukäyttäjä**.

Tietoturva- ja tietosuoja-asoiden toteutumisesta, tiedottamisesta ja valvonnasta omassa yksikössään vastaavat **yksiköiden esimiehet**.

Jokainen sairaanhoitopiirin **työntekijä**, tietoja käsittelevä, tietojärjestelmien tai tietoverkkojen ylläpitäjä ja käyttäjä on omalta osaltaan vastuussa tietoturvan toteuttamisesta sekä tietoturvaohjeiden noudattamisesta.

Jokaisella sairaanhoitopiirin työntekijällä on tietosuoja- ja tietoturva-asioihin liittyvä valvontavastuu.

Jokainen henkilö on velvollinen raportoimaan mahdolliset väärinkäytökset tai niiden uhat. Potilastietoihin liittyvät asiat raportoidaan johtajaylilääkärille ja/tai tietosuojavastaavalle, henkilöstötietoihin liittyvät asiat raportoidaan henkilöstöjohtajalle ja tietosuojavastaavalle. Tietoturvavastaavalle raportoidaan havaituista tietoturvan puutteista, tietoturvaan liittyvästä väärinkäytöksestä tai epäilemästä tietoturvarikkomuksesta.

5 Tietoturvan toteutus

Tietoturvan toteuttamisen perusta on tämä sairaanhoitopiirin hallituksen hyväksymä kirjallinen tietoturva- ja tietosuojapolitiikka, joka annetaan tiedoksi jokaiselle sairaanhoitopiirin työntekijälle, tietojärjestelmien käyttäjälle ja luottamusmiehelle.

Sairaanhoitopiirin tietoturvaperiaatteet perustuvat kansallisiin, yleisiin ja toimialakohtaisiin tietoturvaa, henkilörekistereitä, hyvää tiedonhallintatapaa ja tiedon laatua ohjaaviin ja velvoittaviin säädöksiin, ohjeisiin ja standardeihin.

Lainsäädännön ja ohjeistuksen muutokset otetaan huomioon sairaanhoitopiirin tietoturvan kehittämisessä.

Tietoturvan toteuttaminen ja ylläpito kuvataan tietoturvasuunnitelmassa. Tietoturvan toteutuksen tulee perustua niihin vaatimuksiin, joita toiminta ja palvelut sekä kunkin tiedon ja tietojärjestelmän turvallisuusluokka asettavat tietojenkäsittelyn varmuudelle, käytettävyydelle, salassapidolle, laadulle ja toiminnan jatkuvuudelle sekä toimintaan kohdistuvien riskien arvioinnille. Vaatimusten selvittäminen, riskien arvioiminen ja niiden perusteella turvallisuustoimenpiteiden määrittäminen tapahtuvat säännöllisesti suoritettavilla turvallisuusanalyseillä.

Tietoturvan tavoitteiden saavuttaminen on jatkuva prosessi, jota tuetaan 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 henkilökohtaisella ja riittävällä perehdytyksellä, saatavilla olevilla toimintaohjeilla sekä tietoturvakoulutuksella. Jokainen käyttäjä sitoutuu noudattamaan tietoturva- ja tietosuojaohteita saadessaan oikeuden tehtäviensä mukaiseen tietojärjestelmien ja tietoaainestojen käyttöön.

6 Tietoturvarikkomusten seuraukset

Kaikki tietoturvarikkomukset käsitellään asianmukaisesti. Tietoturvarikkomusta lieventää merkittävästi, mikäli rikkomuksen tehnyt henkilö on välittömästi rikkomuksen huomattuaan ottanut yhteyttä esimieheensä sekä tietoturva- tai tietosuojavastaavaan eikä käytä missään olosuhteissa väärin saamaansa tietoa. Tietoturvarikkomuksesta seuraa varoitus ja sen perusteella on mahdollista purkaa työ- tai virkasuhde.