LAPIN SAIRAANHOITOPIIRI
LAPPI BUOHCCEDIKŠUNBIIRE

TIETOTURVALLISUUSPOLITIIKKA

Yhtymähallitus hyväksynyt 14.6.2017

Sairaanhoitopiirin johtaja hyväksynyt 22.2.2022 muokkaukset liitteessä

Sisällys

1 Johdanto

Tietoturvallisuuspolitiikka pitää sisällään tietojen suojaamista teknisin ja fyysisin keinoin (tietoturva) sekä henkilötietojen asianmukaisen käsittelyn (tietosuoja). Tietoturvallisuuspolitiikan avulla vaikutetaan osaltaan siihen, että Lapin sairaanhoitopiirin strategiassa määritelty visio, toiminta-ajatus, arvot ja palvelut toteutetaan laadukkaasti ja turvallisesti. Erikoissairaanhoitoa koskevat EU:n yleinen tietosuoja-asetus, EU-tasoinen ja kansallinen lainsäädäntö ohjaavat, tarkentavat ja täydentävät tietoturvallisuuspolitiikkaa ja tietoturvallisuuden osa-alueita.

Tietoturvallisuuspolitiikassa ja sen liitteissä määritellään sairaanhoitopiirin tietoturvallisuuden tavoitteet, resurssit, vastuut ja toteutuskeinot. Tietoturvallisuuspolitiikka on koko organisaatiota sitova ja sitä tarkennetaan tietosuojakäsikirjalla sekä muilla erillisohjeilla ja määräyksillä. Koko henkilökunnan, luottamushenkilöiden sekä yhteistyö- ja sopimuskumppaneiden edellytetään noudattavan sairaanhoitopiirin tietoturvallisuusmääräyksiä.

Tietoturvallisuuspolitiikka noudattaa lainsäädännön velvoitteita. Järjestelmät ja laitteet luokitellaan kriittisyyden mukaisesti. Kriittisiksi luokitellut järjestelmät ja laitteet pitää olla käytettävissä päivystävän sairaalan tarpeiden mukaisesti. Organisaatiossa laaditaan suunnitelmat kriisien hallintaan ja poikkeustilanteiden varalta. Tietoturvallisuuden riskienarviointi päivitetään vuosittain ja arvioinnin tulokset kirjataan toimenpiteiden suunnittelun pohjaksi tietotilinpäätökseen. Tietovirrat kuvataan ja ylläpidetään osana kokonaisarkkitehtuuria.

Tietoturvaloukkauksista ilmoitetaan valvontaviranomaisille ja rekisteröidyille EU:n tietosuoja-asetuksen edellyttämällä tavalla. Organisaatio laatii toimintatavan ja osoittaa tarvittavat resurssit tietoturvaloukkausten käsittelylle.

Tietoturvallisuuteen liittyvä viestintä, viestintäkäytännöt ja vastuut saatetaan koko henkilöstön tietoon.

2 Tietoturvallisuustyö

Tietoturvallisuustyö on jatkuvaa toimintaa päivittäisessä työssä ja tietoturvallisuus on tärkeä osa sairaanhoitopiirin toiminnan ja palveluiden laatua. Kaikkien sairaanhoitopiirin henkilökuntaan kuuluvien, luottamushenkilöiden ja sopimuskumppaneiden on velvollisuus noudattaa tietoturvallisuudesta annettuja määräyksiä. Heillä on myös velvollisuus raportoida havaitsemistaan ongelmista ja tietoturvaloukkauksista esimiehelleen ja organisaatiossa käytössä olevan sähköisen järjestelmän kautta.

Tietoturvallisuustyöllä tarkoitetaan tietoturvallisuuden saavuttamiseksi tehtävien toimenpiteiden suunnittelua ja toteuttamista. Tämä kattaa tietojen turvaamisen menetelmät, välineet, toimenpiteet, määräykset, ohjeistuksen, koulutuksen, viestinnän, varautumisen erilaisiin uhkatilanteisiin sekä sovittujen toimintatapojen noudattamisen. Tietosuojalla tarkoitetaan ihmisten yksityiselämän suojaa ja muita sitä turvaavia oikeuksia henkilötietoja käsiteltäessä. Sairaanhoitopiiri osoittaa tarvittavat resurssit tietoturvatyöhön.

Tietoturvallisuustyön päämääränä on:

- turvata sairaanhoitopiirin asiakkaiden ja henkilöstön yksityisyyden suoja
- turvata henkilötietojen asianmukainen käsittely
- turvata sairaanhoitopiirin toiminnalle tärkeiden tietojen ja palveluiden saatavuus
- turvata manuaalisten ja sähköisten tietojärjestelmien että tietoverkkojen keskeytymätön toiminta
- varautua toiminnan keskeyttäviin uhkatilanteisiin, kriiseihin ja niistä toipumiseen
- estää tietojen ja tietojärjestelmien oikeudeton käyttö
- estää tiedon tahaton tuhoutuminen

- estää tiedon tahallinen tuhoaminen
- estää tiedon vääristyminen
- minimoida aiheutuvat vahingot

3 Tietoturvallisuuden osa-alueet ja periaatteet

Tietoturvallisuus kattaa kaikki sairaanhoitopiirin tietojenkäsittelytehtävät sisältäen myös asiakirjahallinnon ja arkistoinnin. Tietoturvallisuustyö huomioi tiedon suojaamisen erilaiset kriteerit käyttötarpeen mukaan. Tietoturvallisuustoimet koskevat sähköisessä, puhutussa ja kirjallisessa muodossa olevan tiedon käsittelyä, luovutusta, säilyttämistä ja siirtämistä.

Sairaanhoitopiirin tiedot sekä tietojenkäsittelyjärjestelmät ja -palvelut on suojattu asianmukaisesti sekä normaalioloissa että poikkeusoloissa hallinnollisten, teknisten, rakenteellisten ja muiden toimenpiteiden avulla.

3.1 Tietoturvallisuuden osa-alueet

Tietoturvallisuuden osa-alueita ovat:

- hallinnollinen tietoturva
- henkilöstöturvallisuus
- fyysinen turvallisuus
- tietoliikenneturvallisuus
- ohjelmistoturvallisuus
- tietoaineistoturvallisuus
- käyttöturvallisuus
- laitteistoturvallisuus

Hallinnollisella tietoturvalla tarkoitetaan tietoturvallisuustoiminnan järjestelyjen, henkilöstön tehtävien ja vastuiden sekä ohjeistuksen, koulutuksen ja valvonnan muodostamaa kokonaisuutta.

Henkilöstöturvallisuudella tarkoitetaan henkilöstön luotettavuuteen ja soveltuvuuteen, oikeuksien hallintaan, sijaisuusjärjestelyihin, henkilöstön suojaamiseen ja työsuhteen järjestelyihin liittyvien turvallisuustekijöiden hoitamista.

Fyysisellä turvallisuudella tarkoitetaan niitä turvallisuustoimenpiteitä, joilla luodaan ja ylläpidetään tietotekniikan vaatiman käyttöympäristön toimintaolosuhteet. Fyysisin turvallisuustoimenpitein myös suojataan ja valvotaan kiinteistö, sen erikoistilat kuten muun muassa laite- ja arkistointitilat luvattomia tai rikollisia toimia vastaan, onnettomuuksilta ja luonnontuhoilta sekä varmistetaan teknisten järjestelmien toiminta.

Tietoliikenneturvallisuudella tarkoitetaan tiedonsiirtoyhteyksien käytettävyyteen, tiedonsiirron suojaamiseen ja salaamiseen, käyttäjän tunnistamiseen ja verkon varmistamiseen liittyviä turvallisuustoimenpiteitä.

Ohjelmistoturvallisuudella tarkoitetaan käyttöjärjestelmien, varus- ja työkaluohjelmistojen sekä muiden ohjelmistojen ja sovellusten suojausominaisuuksia, valvonta- ja lokimenettelyjä sekä ohjelmistojen määrittelyyn, suunnitteluun, kehittämiseen ja hankintaan sekä ylläpitoon ja päivitykseen liittyviä turvallisuustoimenpiteitä.

Tietoaineistoturvallisuudella tarkoitetaan tiedon ja tietoaineiston käytettävyyttä, oikeellisuutta, salassa pitämistä, turvallista käsittelyä ja säilyttämistä sekä tietojätteen hävittämistä.

Käyttöturvallisuudella luodaan ja ylläpidetään tietotekniikan turvallisen käytön vaatimat toiminta-olosuhteet huolehtimalla tekniikan toimivuuden valvonnasta, käyttöoikeuksista, käytön ja lokien valvonnasta, ohjelmistotukeen, ylläpito-, kehittämis- ja huoltotoimintoihin liittyvistä turvallisuustoimenpiteistä, varmuus- ja suojakopioinnista sekä häiriöraportoinnista.

Laitteistoturvallisuudella tarkoitetaan laitteiston käytettävyyteen, toimintaan, ylläpitoon sekä laitteiden ja tarvikkeiden saatavuuteen liittyviä toimenpiteitä. Turvatoimenpiteet kohdistuvat atk- ja tutkimuslaitteistojen ja tietoverkon rakenteeseen, varusohjelmiin, käyttöjärjestelmiin, laite- ja varusohjelmahuoltoon, keskitettyyn operointiin, varmistuksiin, atk- ja tutkimuslaitteisiin sekä pääsyn suojaukseen.

3.2 Tietoturvallisuuden periaatteet

Tietoturvallisuus rakentuu tietojen:

- käsittelyn lainmukaisuudesta, kohtuullisuudesta ja läpinäkyvyydestä
- käyttötarkoitussidonnaisuudesta
- minimoinnista
- täsmällisyydestä
- säilytyksen rajoittamisesta
- eheydestä ja luottamuksellisuudesta
- saatavuudesta
- käytettävyydestä
- kiistämättömyydestä
- pääsynvalvonnasta / todentamisesta
- käsittelyn toimintatavoista ja henkilöstön asenteesta

Rekisterinpitäjää koskevan EU-tietosuoja-asetuksen mukaisen **osoitusvelvollisuuden** mukaisesti rekisterinpitäjällä on oltava kyky osoittaa noudattavansa asetusta henkilötietoja käsitellessä ja toteuttavansa tietosuojaperiaatteita myös käytännössä. Osoitusvelvollisuus edellyttää käsittelyyn liittyvien prosessien sekä tietosuojaperiaatteiden käytännön toteuttamisen dokumentointia.

Käsittelyn lainmukaisuus, kohtuullisuus ja läpinäkyvyys perustuu rekisterinpitäjän lakisääteiseen velvoitteeseen käsitellä henkilötietoja. Henkilötietoja pitää käsitellä asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi.

Käyttötarkoitussidonnaisuus tarkoittaa, että tietoja on kerättävä tiettyä, nimenomaista ja laillista tarkoitusta varten, eikä niitä saa käsitellä myöhemmin näiden tarkoitusten kanssa yhteensopimattomalla tavalla.

Minimoinnilla tarkoitetaan sitä, että henkilötietojen on oltava asianmukaisia, olennaisia ja rajoitettuja siihen, mikä on tarpeellista suhteessa niihin tarkoituksiin, joita varten niitä käsitellään.

Henkilötietojen on oltava **täsmällisiä** ja tarvittaessa päivitettyjä. Rekisterinpitäjän on toteutettava kaikki mahdolliset kohtuulliset toimenpiteet sen varmistamiseksi, että käsittelyn tarkoituksiin nähden epätarkat ja virheelliset henkilötiedot poistetaan tai oikaistaan viipymättä.

Tietoja on **säilytettävä** muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin on tarpeen tietojenkäsittelyn tarkoitusten toteuttamista varten. Henkilötietoja voidaan säilyttää pidempiä aikoja, jos henkilötietoja käsitellään ainoastaan yleisen edun mukaisia arkistointitarkoituksia taikka tieteellisiä tai historiallisia tutkimustarkoituksia tai tilastollisia tarkoituksia varten artikla 89 kohdan 1 mukaisesti edellyttäen, että tässä asetuksessa vaaditut asianmukaiset tekniset ja organisatoriset toimenpiteet on pantu täytäntöön rekisteröidyn oikeuksien ja vapauksien turvaamiseksi.

Eheys ja luottamuksellisuus tarkoittavat niitä toimenpiteitä, jolla varmistetaan henkilötietojen asianmukainen turvallisuus, mukaan lukien suojaaminen luvattomalta ja lainvastaiselta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta käyttäen asianmukaisia teknisiä tai organisatorisia toimia. Luottamukselliset tiedot (ei-julkiset ja salassa pidettävät) ovat vain niiden käyttöön oikeutettujen saatavissa sovituilla tavoilla ja sovittuun aikaan eikä niitä paljasteta tai muutoin saateta sivullisten tietoon. Niiden käsittelyssä noudatetaan voimassa olevaa lainsäädäntöä.

Saatavuus tarkoittaa, että tietojen tulee olla helposti ja viiveettä niiden käytössä, joille tieto kuuluu. Samalla on huolehdittava, että tiedot ovat teknisesti käytettävissä. Saatavuuden turvaamisessa on otettava huomioon asiakirjallisten tietojen käytettävyydelle määritetyt vaatimukset.

Käytettävyys tarkoittaa, että tiedot ja tietojenkäsittelyjärjestelmät ovat käytettävissä ja käyttökelpoisia valtuutetuille käyttäjille, toiminnan kannalta hyväksyttävän ajan kuluessa.

Kiistämättömyys tarkoittaa todisteiden luomista sen varmistamiseksi, ettei yksikään tietojen käsittelyn tai siirron osapuoli voi jälkikäteen kiistää osuuttaan siihen. Kiistämättömyys voidaan todentaa esim. lokitiedoilla ja niiden valvonnalla.

Pääsynvalvonta/todentaminen tarkoittaa, että tietoa tai tietojärjestelmää ei voi käyttää ilman lupaa ja ettei arkistotiloihin tai arkaluonteisia tietoja sisältäviin tietoihin pääse ilman valvontaa. Pääsy tietoihin on mahdollista vain tietojärjestelmiin henkilökohtaisesti tunnistautumalla. Tiloihin pääsyä, joissa arkaluonteista tietoa säilytetään, valvotaan kulunvalvonnan keinoin.

Asenteella tarkoitetaan sitä, että henkilöstö ymmärtää tietoturvan merkityksen ja on motivoinut noudattamaan tietoturvaohjeita ja tietoturvamääräyksiä.

4 Valtuudet ja vastuut

Kuntayhtymän hallitus käyttää ylintä päätäntävaltaa tietoturvallisuuden ohjeistamisessa hyväksymällä tietoturvallisuuspolitiikan ja osoittamalla riittävät resurssit tietoturvallisuuden kehittämiseen ja toimeenpanoon. Sairaanhoitopiirin johtaja vastaa kokonaisturvallisuudesta, valvonnasta ja tietoturvallisuustyön organisoinnista. Henkilörekistereistä vastaavat ja muut johtavat viranhaltijat sekä johtoryhmä sitoutuvat tietoturvallisuuden suunnitteluun, kehittämiseen, seurantaan ja arviointiin sekä vastaavat osaltaan tietoturvaloukkausten käsittelystä. Jokainen työntekijä, luottamushenkilö ja sopimuskumppani vastaavat osaltaan tietoturvallisuuden toteutumisesta voimassaolevan lainsäädännön ja annettujen ohjeiden mukaisesti.

Viranomaisten toiminnan julkisuudesta annetun lain (621/1999) mukaan viranomaisten asiakirjat ovat julkisia, jollei tässä tai muussa laissa erikseen toisin säädetä. Terveydenhuollon ammattihenkilöiden salassapitovelvollisuudesta on säädetty terveydenhuollon ammattihenkilöistä annetussa laissa (1994/559). Laissa potilaan asemasta ja oikeuksista (785/1992) säädetään, että terveydenhuollon ammattihenkilö tai muu terveydenhuollon toimintayksikössä työskentelevä taikka sen tehtäviä suorittava henkilö ei saa ilman potilaan kirjallista suostumusta antaa sivulliselle potilasasiakirjoihin sisältyviä tietoja. Terveyden- ja sairaanhoidossa sivullisella tarkoitetaan muita kuin asianomaisessa toimintayksikössä tai sen toimeksiannosta potilaan hoitoon tai siihen liittyviin tehtäviin osallistuvia henkilöitä. Vaitiolovelvollisia ovat myös siviilipalvelumiehet ja sairaalassa toimivat harjoittelijat. Salassapitovelvollisuus säilyy ammatinharjoittamisen päättymisen jälkeen.

Henkilötietolaki (523/1999) ja EU-tietosuoja-asetus (679/2016) edellyttävät, että henkilötietojen käsittely tulee olla asiallista ja käsittely perustuu terveydenhuollossa lakisääteisten velvoitteiden noudattamiseen.

Organisaation tietoturvallisuustehtävät, vastuut ja organisointi on kuvattu liitteessä 1.

Sairaanhoitopiirin yhtymähallitus hyväksyy tietoturvallisuuspolitiikan. Johtoryhmä käsittelee ja sairaanhoitopiirin johtaja hyväksyy liitteisiin tehdyt muutokset sekä tietoturvallisuuspolitiikan päivitykset, jollei politiikka olennaisesti muutu.

5 Soveltaminen

Lapin sairaanhoitopiirin yhtymähallituksen hyväksymä kirjallinen tietoturvallisuuspolitiikka annetaan tiedoksi jokaiselle työntekijälle, luottamushenkilölle sekä yhteistyö- ja sopimuskumppanille.

Tietoturvallisuuspolitiikka on voimassa toistaiseksi ja voimassaolo jatkuu, ellei sitä nimenomaisesti kumota.

Liite 1: Tietoturvallisuustehtävät, tietoturvallisuustyön organisointi ja vastuut

Sairaanhoitopiirin yhtymähallitus hyväksyy tietoturvallisuuspolitiikan. Johtoryhmä käsittelee ja sairaanhoitopiirin johtaja hyväksyy liitteisiin tehdyt muutokset sekä tietoturvallisuuspolitiikan päivitykset, jollei politiikka olennaisesti muutu. Kaikille rekistereille on nimetty vastuuhenkilö.

Tietoturvallisuudesta vastaaminen on osa organisaation strategista ja operatiivista johtamista. Vastuu tietoturvallisuudesta kuuluu jokaiseen tehtävään. Jokainen työntekijä vastaa osaltaan tietoturvallisuuden toteutumisesta voimassaolevan lainsäädännön ja annettujen ohjeiden mukaisesti.

Tietoturvallisuusorganisaation toiminta on osa sisäistä valvontaa ja riskien hallintaa.

Yleiset vastuut

Tietoturvallisuuden edistäminen ja toteuttaminen sekä tietoturvaloukkauksista ilmoittaminen on sairaanhoitopiirin jokaisen työntekijän ja luottamushenkilön velvollisuus.

Työntekijät ja luottamushenkilöt

- Perehtyvät sairaanhoitopiirin tietoturvallisuus- ja tietosuojaohjeistukseen (tietoturvallisuuspolitiikka, tietosuojakäsikirja, atk-työskentelyn tietosuojaohjeet) sekä käyttämiensä tietojärjestelmien käyttöohjeisiin ja rekisteriselosteisiin.
- Suorittavat tietosuojan- ja tietoturvan verkkokoulutuksen vähintään kolmen (3) vuoden välein. Yhtymähallitus määrittelee, kuinka laajasti vaatimusta sovelletaan luottamushenkilöiden osalta ottaen huomioon luottamustoimessa käsiteltävien aineistojen luonteen ja sisällön.
- Noudattavat omassa työssään tietoturvallisuudesta annettuja ohjeita sekä voimassaolevaa lainsäädäntöä. Ohjeilla ja koulutuksilla annetaan henkilöstölle perustiedot henkilötietojen asianmukaisesta käsittelystä, tietoaineiston ja tietojärjestelmien käytöstä sekä niihin liittyvästä tietoturvallisuudesta.
- Toteuttavat hyvää tiedonhallintatapaa työssään.
- Osallistuvat tietoturvallisuuteen liittyvään täydennyskoulutukseen tehtäviensä edellyttämässä laajuudessa.
- Raportoivat välittömästi havaitsemistaan tahattomista tai tahallisista tietoturvaloukkauksista omalle esimiehelleen sekä sähköisen HaiPro-järjestelmän kautta.

Esimiehet

- Tukevat tietoturvan ja tietosuojan ylläpitämistä, jalkauttamista ja kehittämistä.
- Vastaavat siitä, että henkilökunta ja sopimuskumppanit ovat selvillä tietoturvallisuuden vaatimuksista ja säännöistä.
- Vastaavat, että tietojärjestelmiä ja laitteita käytetään ohjeistuksen mukaisesti.
- Vastaavat hyvän tiedonhallintatavan toteutumisesta yksikössään.
- Saattavat tiedoksi ja toimenpiteitä varten rekistereistä vastaaville sekä tietosuojavastaavalle kaikki omassa yksikössään tapahtuneet tietoturvaloukkaukset. Tietoturvaloukkaukset ilmoitetaan sähköisen järjestelmän (HaiPro) kautta, jolloin asia dokumentoituu jatkotoimenpiteitä varten.
- Osallistuvat yksikössään tapahtuneeseen tietoturvaloukkausten käsittelyyn ja jatkotoimenpiteiden suunnitteluun.
- Seuraavat henkilöstönsä tietoturva- ja tietosuojakoulutuksiin osallistumista

Organisaation johtavat viranhaltijat ja johtoryhmä

- Sitoutuvat tietoturvallisuuden suunnitteluun, kehittämiseen, seurantaan ja arviointiin.
- Varmistavat, että tietoturvallisuustavoitteet asetetaan ja tietoturvallisuuteen liittyvät suunnitelmat laaditaan.

- Viestivät henkilöstölle tietoturvallisuuden sekä siihen liittyvien lakisääteisten velvoitteiden noudattamisen tärkeydestä.
- Huolehtivat siitä, että tietoturvallisuuden kehittämiseen ja toteuttamiseen on käytettävissä riittävät resurssit.
- Vastaavat, että HaiPro tietoturvailmoitukset käsitellään viivytyksettä.
- Vastaavat, että tietoturvallisuuden riskienarviointi tehdään vuosittain osana riskienhallintapolitiikkaa.
- Vastaavat, että riskienarvioinnin perusteella nousseet kehittämistoimenpiteet suunnitellaan ja toteutetaan.
- Päättävät hyväksyttävistä riskitasoista.
- Vastaavat, että sopimuksissa ulkopuolisten palveluntarjoajien ja toimittajien kanssa sovitaan noudatettavan sairaanhoitopiirissä laadittuja tietoturvallisuusmääräyksiä.
- Suorittavat johdon katselmuksia omalla vastuualueellaan.
- Hyväksyvät tietoturvaloukkauksissa käytettävät sanktiot.
- Ryhtyvät tarvittaviin toimenpiteisiin tietoturvaloukkauksissa.
- Hyväksyvät oman vastuualueensa osalta laaditut tietovirtakaaviot
- Vastaavat osaltaan tietoturvallisuuteen liittyvästä tiedotuksesta

Sopimuskumppanit

- Velvoitetaan noudattamaan hyvää tiedonhallintatapaa sekä vastaavia tietoturvallisuusohjeita ja -käytäntöjä kuin sairaanhoitopiirin oma henkilöstö.
- Velvoitteet kirjataan sopimuskumppanien kanssa tehtäviin sopimuksiin.

Järjestelmien ja laitteiden omistajat

(tietojärjestelmäselosteeseen tai laiterekisteriin nimetty vastuutaho)

- Jokaiselle tietojärjestelmälle on nimettävä omistaja (yksikkö, jota varten tietojärjestelmä tai laite on hankittu), jota käytännössä edustaa yksikön johtaja

Omistajayksikön tehtävät:

- Huomioi järjestelmän tietoturva-, tietosuoja- ja muut tiedonhallinnan vaatimukset jo järjestelmän hankintavaiheessa
- Vastaa, että järjestelmät ja laitteet on kirjattu sovittuun hallintajärjestelmään.
- Vastaa, että kaikille järjestelmille ja laitteille on laadittu tietojärjestelmäseloste (ei käsitellä henkilötietoja) tai tietosuojaseloste (käsitellään henkilötietoja).
- Vastaa, että järjestelmille ja laitteille on olemassa ajantasainen ohjeistus.
- Vastaa, että kaikki lääkintälaitteet täyttävät lääkintälaitedirektiivin mukaiset vaatimukset.
- Vastaa, että järjestelmistä ja laitteista on olemassa tarvittavat tekniset asiakirjat
- Osallistuu tarvittaessa poikkeusolojen tilanteiden suunnitelman laadintaan.

Erikseen nimetyt vastuut

Arkistopäällikkö

- Vastaa asiakirjojen sekä niihin sisältyvien tietojen asianmukaisesta saatavuudesta, käytettävyydestä, suojaamisesta, eheydestä ja lainmukaisesta säilyttämisestä sekä arkistoinnista hyvän tiedonhallintatavan luomiseksi ja toteuttamiseksi.
- Vastaa asiakirjojen säilytysaikojen määrittelystä.
- Vastaa asiakirjahallinnon suunnittelua, ohjausta ja käytännön tehtävien hoitoa säätelevän toimintasäännön laatimisesta ja ylläpitämisestä.
- Ylläpitää ja päivittää arkistonmuodostussuunnitelmaa, mikä on asiakirjojen ja tietoaineistojen hakumahdollisuuksien, säilytystavan ja -muotojen suunnittelun työväline.
- Vastaa asiakirjoihin kohdistuvasta tietopalvelusta lainsäädäntöä ja erillisohjeita noudattaen.
- Vastaa tietosuojan varmistamisesta hävitettäessä määräajan säilytettäviä asiakirjoja.

- Varmistaa tiedonhallintaan liittyvien vaatimusten huomioimisesta tietojärjestelmien ja asiakirjahallinnon kehittämishankkeissa ja hankinnoissa.
- Vastaa asiakirjajulkisuuskuvauksen ylläpidosta.

Henkilöstöjohtaja

- Vastaa henkilöstöhallinnon tiedoista ja rekistereistä sekä niiden asianmukaisesta käsittelystä.
- Ohjeistaa ja valvoo henkilöstöhallinnon tietojen ja -järjestelmien käyttöä sekä tietojen luovuttamista.
- Päättää henkilöstöhallinnon järjestelmien roolikohtaisista käyttöoikeuksista.
- Vastaa henkilöstöhallinnon järjestelmien lokitietojen käytön valvonnasta.
- Käsittelee HaiPro-järjestelmässä olevat tietoturvailmoitukset ja muuta kautta esiin tulleet tietoturvaloukkaukset koskien henkilöstöhallinnon tietoihin ja -järjestelmiin liittyviä väärinkäyttöepäilyjä ja tekee toimenpide-ehdotuksia yhdessä tietosuojavastaavan ja tietoturvavastaavan kanssa.
- Saattaa väärinkäyttöepäilyt/tietoturvaloukkaukset toimenpiteitä varten sairaanhoitopiirin johtajalle.
- Harkitsee ja toteuttaa osaltaan sisäiset sanktiot ja yhteydenotot ulkopuolisiin valvontaviranomaisiin.
- Vastaa tietovirtakaavioista henkilöstöhallinnon tietojen osalta.

Johtajaylilääkäri

- Vastaa potilastiedoista ja potilasrekistereistä sekä niiden asianmukaisesta käsittelystä.
- Päättää potilastietoja sisältävien järjestelmien roolikohtaisista käyttöoikeuksista
- Vastaa, että järjestelmien ja laitteiden, jotka sisältävät potilastietoja, käyttöoikeudet toteutetaan asianmukaisesti.
- Ohjeistaa ja valvoo potilastiedon ja potilastietojärjestelmien käyttöä ja tietojen luovutusta.
- Vastaa potilastietojärjestelmien lokitietojen käytön valvonnasta.
- Käsittelee HaiPro-järjestelmässä olevat tietoturvailmoitukset ja muuta kautta esiin tulleet tietoturvaloukkaukset koskien potilastietoihin ja potilastietojärjestelmien käyttöön liittyviä väärinkäyttöepäilyjä ja tekee toimenpide-ehdotuksia yhdessä tietosuojavastaavan ja tietoturvavastaavan kanssa.
- Saattaa väärinkäyttöepäilyt/tietoturvaloukkaukset toimenpiteitä varten sairaanhoitopiirin johtajalle.
- Harkitsee ja toteuttaa osaltaan sisäiset sanktiot ja yhteydenotot ulkopuolisiin valvontaviranomaisiin.
- Vastaa tietovirtakaavioista potilastietojen osalta

Sairaanhoitopiirin johtaja

- Vastaa kokonaisturvallisuudesta.
- Huolehtii, että sairaanhoitopiirissä on ajantasainen tietoturvallisuuspolitiikka.
- Vastaa, että tietoturvallisuustyö on organisoitu sairaanhoitopiirissä.
- Vastaa tietoturvallisuutta koskevasta viestinnästä ja sen organisoinnista.
- Osallistuu tietotilinpäätöksen valmisteluun ja esittelee sen yhtymähallitukselle ja tarkastuslautakunnalle.
- Vastaa, että riskienarviointi toteutetaan ja riskienhallintapolitiikka päivitetään vuosittain.
- Vastaa, että järjestelmien ja laitteiden, jotka sisältävät vain muita henkilötietoja kuin potilastietoja, käyttöoikeudet, muun muassa kulunvalvonta, avaimien koodaus ja kameravalvonta, toteutetaan asianmukaisesti.
- Käsittelee HaiPro-järjestelmässä olevat tietoturvailmoitukset ja muuta kautta esiin tulleet tietoturvaloukkaukset, jotka koskevat niitä järjestelmiä ja laitteita, joissa on vain muita henkilötietoja kuin potilastietoja ja tekee toimenpide-ehdotuksia yhdessä turvallisuuspäällikön, tietosuojavastaavan ja tietoturvavastaavan kanssa.
- Koordinoi johdon katselmukset ja auditoinnit.

- Vastaa, että tietoturvaloukkaukset selvitetään ja ilmoitetaan tarvittaessa valvontaviranomaisille 72 tunnin kuluessa tapahtuneesta.
- Vastaa, että tietoturvaloukkauksista informoidaan tarvittaessa rekisteröityä
- Harkitsee ja toteuttaa osaltaan sisäiset sanktiot ja vie ne tarvittaessa yhtymähallituksen käsiteltäviksi
- Ottaa tarvittaessa yhteyttä ulkopuolisiin valvontaviranomaisiin ja muihin viranomaisiin.
- Tekee esityksen tietoturvallisuustyön organisoinnista ja vastuista johtoryhmälle ja päättää muutokset tietoturvallisuuspolitiikan liitteisiin.
- Vastaa tiedonhallintamallin kuvaamisesta, ylläpidosta ja muutosvaikutusten arvioinnista.
- Vastaa jatkuvuus- ja varautumissuunnittelusta

Talousjohtaja

- Vastaa taloushallinnon tiedoista ja rekistereistä sekä niiden asianmukaisesta käsittelystä.
- Ohjeistaa ja valvoo taloushallinnon tietojen ja järjestelmien käyttöä sekä tietojen luovuttamista
- Päättää taloushallinnon järjestelmien roolikohtaisista käyttöoikeuksista - potilastietoa sisältävissä järjestelmissä johtajaylilääkärin antamia ohjeita noudattaen.
- Vastaa taloushallinnon järjestelmien lokitietojen käytön valvonnasta.
- Käsittelee HaiPro-järjestelmässä olevat tietoturvailmoitukset ja muuta kautta esiin tulleet tietoturvaloukkaukset koskien taloushallinnon tietoihin ja -järjestelmiin liittyviä väärinkäyttöepäilyjä ja tekee toimenpide-ehdotuksia yhdessä tietosuojavastaavan ja tietoturvavastaavan kanssa.
- Saattaa väärinkäyttöepäilyt/tietoturvaloukkaukset toimenpiteitä varten sairaanhoitopiirin johtajalle.
- Harkitsee ja toteuttaa osaltaan sisäiset sanktiot ja yhteydenotot ulkopuolisiin valvontaviranomaisiin.
- Vastaa tietovirtakaavioista taloushallinnon tietojen osalta.

Tekninen johtaja

- Vastaa tekniikan tiedoista ja rekistereistä, jotka eivät sisällä henkilötietoa sekä niiden asianmukaisesta käsittelystä.
- Päättää ja vastaa teknisten järjestelmien, jotka eivät sisällä henkilötietoja, käyttöoikeuksista.
- Vastaa, että lääkintälaitteiden tietoturvallisuus on toteutettu asianmukaisesti noudattaen sairaanhoitopiirin johtajan, johtajaylilääkärin sekä turvallisuuspäällikön ohjeistusta.
- Vastaa, että jokaisella laitteella on omistaja ja seuraa, että laitetiedot on kirjattu sähköiseen hallintajärjestelmään.
- Vastaa tietokonesalien, verkon aktiivilaitteiden ja varavirran piirissä olevien pistorasioiden sähkön syötöstä ja varasyötöstä.
- Vastaa tietokonesalien jäähdytyslaitteiden ja ilmastoinnin toimivuudesta.
- Vastaa kaikkien tilojen kulunvalvonnan, lukitusjärjestelmän ja paloturvallisuuden toteuttamisesta mukaan lukien muun muassa tietokonesalit ja arkistot.
- Saattaa mahdolliset väärinkäyttöepäilyt toimenpiteitä varten sairaanhoitopiirin johtajalle ja tarvittaessa ulkopuolisille valvontaviranomaisille.

Tiedottaja

- Edistää tiedotuksen avulla yhdessä tietoturvallisuustoimijoiden kanssa henkilökunnan ja potilaiden/asiakkaiden tietoisuutta ja ymmärrystä tietosuoja- ja tietoturva-asioissa.
- Vastaa yhdessä tietoturvallisuustoimijoiden kanssa tietoturvallisuutta koskevan aineiston (ohjeet, suunnitelmat, tiedotteet yms.) päivityksestä ja löytymisestä LSHP:n internetissä ja henkilökunnan intranetissä.

Tietohallintojohtaja

- Koordinoi sairaanhoitopiirin johdon toimeksiannosta tietojärjestelmien ja niiden käytön sekä tietoturvan teknisen toteutuksen suunnittelua, toteutumista ja raportointia.
- Vastaa tietojärjestelmien tietoturvasta.

- Vastaa, että jokaisella tietojärjestelmälle on nimetty omistaja.
- Vastaa osaltaan, että tietoturvallisuusasiat on organisoitu ja toteutettu toimipaikoissa ja yksiköissä.
- Varmistaa tietohallinnon resurssit tietoturvallisuuteen liittyvään kehittämiseen ja hankkeisiin.
- Vastaa, että tietojärjestelmille vaaditut turvatasot on asetettu.
- Vastaa tietoturvakontrollien valinnasta ja toteutuksesta.
- Vastaa säännöllisten tietoturvatoimenpiteiden toteuttamisesta, mm. palomuurisäännösten auditoinneista.
- Vastaa tietoturvaloukkausten seurannasta ja käsittelystä ja saattaa asian tiedoksi tietoturva- ja tietosuojatyöryhmälle sekä osaksi tietotilinpäätöstä.
- Vastaa lokitietojen käytön valvonnan teknisestä toteuttamisesta ja saattaa mahdolliset väärinkäyttöepäilyt toimenpiteitä varten sairaanhoitopiirin johtajalle.
- Vastaa, että tietovirtakaaviot on dokumentoitu ylläpito- ja hallintajärjestelmään.
- Vastaa, että tietojärjestelmien varmistukset ovat lainsäädännön ja tietoturvallisuuspolitiikan mukaiset.

Tietosuojavastaava

- Tukee tietosuojan erityisasiantuntijana henkilökuntaa ja rekisteröityjä tietosuoja-asioissa.
- Osallistuu rekisterinpitäjän hyväksymiä tietosuoja- ja tietoturvaohjeita koskevaan valmisteluun ja ylläpitoon.
- Seuraa ja valvoo henkilötietojen käsittelyä ja niiden suojausmenetelmiä
- Käsittelee HaiPro-järjestelmän kautta tulleet tietoturvailmoitukset ja tekee toimenpide-ehdotuksia yhteistyössä rekistereistä vastuussa olevien sekä tietoturvavastaavan kanssa.
- Toteuttaa lokien valvonnan yhdessä tietoturvavastaavan ja rekisterissä vastuussa olevan kanssa.
- Osallistuu rekisterinpitäjän henkilöstölle annettavan tietosuojakoulutuksen suunnitteluun ja toteuttamiseen
- Raportoi organisaation johdolle tietosuojan (ja tietoturvallisuuden) tilasta ja kehittämistarpeista (sisäiset auditoinnit ja käytönvalvonta)
- Laatii tietotilinpäätöksen yhteistyössä tietoturvavastaavan kanssa.
- Toimii yhdyshenkilönä valvontaviranomaisiin tietosuojaan liittyvissä asioissa
- Toimii tietosuojan erityisasiantuntijana tietoturvallisuuden kehittämisessä, edistämisessä ja ohjeistamisessa.
- On rekisteröityjen yhteyshenkilö henkilötietojen käsittelyyn liittyvissä asioissa.
- Valvoo tietoaineistojen käsittelyä ja tiedonhallintaa.
- Valvoo tietoturvallisuustoimenpiteiden noudattamista siltä osin, kun se liittyy henkilötietojen käsittelyyn.

Tietoturvavastaava

- Toimii tietoturvan erityisasiantuntijana tietojärjestelmien käyttöönotoissa ja ylläpidossa.
- Osallistuu rekisterinpitäjän hyväksymiä tietosuoja- ja tietoturvaohjeita koskevaan valmisteluun ja ylläpitoon.
- Toteuttaa lokien valvonnan yhdessä tietosuojavastaavan ja rekisterissä vastuussa olevan kanssa.
- Huolehtii, että tietoturvaan (ohjelmistot, laitteet, tietoliikenne) liittyvät ohjeistukset on laadittu asiamukaisesti ja ne ovat esimiesten käytettävissä.
- Laatii ja ylläpitää kriittisten järjestelmien osalta toipumis- ja varajärjestelmäsuunnitelman järjestelmän omistajan, teknisen johtajan sekä tietosuojavastaavan kanssa.
- Osallistuu tietojärjestelmäselosteiden laadintaan.
- Seuraa tietoturvaloukkauksia ja käsittelee ne yhteistyössä tarvittavien osapuolien kanssa sekä tekee toimenpide-ehdotuksia eri osapuolille.
- Raportoi organisaation johdolle tietoturvan tilasta ja kehittämistarpeista yhteistyössä tietosuojavastaavan kanssa (sisäiset auditoinnit ja käytönvalvonta)
- Laatii tietotilinpäätöksen yhteistyössä tietosuojavastaavan kanssa.

- Toimii tietoturvan erityisasiantuntijana tietoturvallisuuden kehittämisessä, edistämisessä ja ohjeistamisessa.

Turvallisuuspäällikkö

- Suunnittelee turvateknisten järjestelmien ja laitteiden, jotka sisältävät muita henkilötietoja kuin potilastietoja, käyttöoikeudet yhteistyössä sairaanhoitopiirin johtajan kanssa.
- Vastaa riskienhallinnan yhteistyöstä ja organisoinnista.
- Vastaa turvallisuussuunnittelusta.
- Vastaa normaaliolojen häiriötilanteiden ja poikkeusolojen varautumissuunnittelun koordinoinnista.
- Toimii turvallisuuden asiantuntijana toimitilaturvallisuuden kehittämisessä.
- Saattaa mahdolliset väärinkäyttöepäilyt toimenpiteitä varten sairaanhoitopiirin johtajalle ja tarvittaessa ulkopuolisille valvontaviranomaisille.
- Osallistuu tarvittaessa asiantuntijana tietoturvaloukkausten käsittelyyn yhteistyössä ko. rekisteristä vastuussa olevan, tietosuojavastaavan ja tietoturvavastaavan kanssa.
- Osallistuu tietoturvallisuuden kehittämisen suunnitteluun osana kokonaisturvallisuutta.

Yhtymähallitus

- Hyväksyy tietoturvallisuuspolitiikan
- On lainsäädännössä tarkoitettu rekisterinpitäjä
- Huolehtii, että tietoturvallisuustyöhön käytettävissä on riittävät resurssit

Tietoturvallisuustyön organisointi

Tietoturvallisuustehtävät on vastuutettu edellä olevan mukaisesti. Vastuissa on määritelty eri rekistereistä vastaavat viranhaltijat. Tietoturvallisuuteen liittyvää valmistelua, valvontaa ja kehittämistä varten sairaanhoitopiirissä toimii tietoturva- ja tietosuojatyöryhmä, jonka tehtävät liittyvät kaikkiin tietoturvallisuuden osa-alueisiin. Tietoturvallisuutta käsitellään lisäksi potilaskertomustyöryhmässä erityisesti henkilöstö-, käyttö- ja ohjelmistoturvallisuuden näkökulmasta, valmius- ja riskienhallintatyöryhmässä henkilöstö-, fyysisen-, käyttö- ja laitteistoturvallisuuden näkökulmasta sekä potilasturvallisuustyöryhmässä hallinnollisesta näkökulmasta.

Työryhmien välinen yhteistyö on tärkeää siksi, etteivät eri työryhmät esitä tai suunnittele toimenpiteitä, jotka ovat ristiriidassa keskenään. Työryhmien välisen yhteistyön koordinointivastuu on työryhmien puheenjohtajilla, varapuheenjohtajilla ja sihteereillä. Näiden toimijoiden velvollisuutena on vastata siitä, että tehdyillä päätöksillä ja toimenpiteillä saavutetaan yhteinen päämäärä eikä päällekkäisiä toimenpiteitä tehdä. Ryhmien välinen yhteistyö tapahtuu pääosin koordinointivastuussa olevien toimesta.

Tietoturva- ja tietosuojatyöryhmä

Työryhmän nimeää sairaanhoitopiirin johtaja. Työryhmää täydennetään tarvittaessa. Työryhmään voidaan kutsua asiantuntijoita.

Työryhmän kokoonpano

- tietohallintojohtaja (pj)
- johtajaylilääkäri (vpj)
- tietosuojavastaava (sihteeri)
- turvallisuuspäällikkö
- henkilöstöjohtaja
- arkistopäällikkö
- eri tulosalueiden edustus

Tehtävät

- Valmistelee, seuraa, raportoi ja edistää tietoturvaan ja tietosuojaan liittyviä asioita.
- Seuraa ja arvioi tietoturvan ja tietosuojan tilaa ja toimivuutta sairaanhoitopiirissä.
- Nostaa esille kehittämistarpeita ja hyviä käytänteitä.
- Osallistuu tietoturvaan ja tietosuojaan liittyvien määräysten ja ohjeiden laatimiseen ja päivittämiseen.
- Ohjeistaa ja tuo kehittämistarpeita tietosuojan ja tietoturvan valvonnan käytänteisiin.
- Osallistuu tietoturvallisuuden kehittämishankkeiden valmisteluun.
- seuraa sisäistä ja ulkoista tietoturvallisuustilannetta ja reagoi tarvittaessa havaittuihin ongelmiin ja uhkiin.
- Osallistuu tieturvaa ja tietosuojaa koskevaan sisäiseen tiedottamiseen ja koulutusten suunnitteluun.