Pohjois-Savon sairaanhoitopiirin Tietoturva- ja tietosuojapolitiikka

Kuntayhtymän johtoryhmä 25.1.2022

Sisällys

KÄSITTEITÄ

Eheys	Tieto on virheetöntä ja eheää, eikä se ole muuttunut tahallisen tai tahattoman teknisen tai inhimillisen toiminnan seurauksena.
Erityiset henkilötietoryhmät	Rotu tai etninen alkuperä, poliittiset mielipiteet, uskonnollinen tai filosofinen vakaumus, ammattiliiton jäsenyys, terveyttä koskevat tiedot, seksuaalinen suuntautuminen tai käyttäytyminen, geneettiset ja biometriset tiedot henkilön tunnistamista varten.
Henkilörekisteri	Jäsennelty tietojoukko, joka sisältää henkilötietoja ja tietoja voidaan hakea tietyllä perusteella. Rekisteri voi olla keskitetty, hajautettu tai jaettu maantieteellisesti.
Henkilötieto	Kaikki sellainen tieto, josta henkilön voi tunnistaa suoraan tai epäsuorasti. Suoraan tunnistamisesta esimerkkejä ovat nimi, henkilötunnus, silmänpohjankuva tai IP-osoite. Epäsuorasta tunnistamisesta esimerkkinä harvinainen diagnoosi yhdistettynä asuinpaikkakuntaan, joiden avulla henkilö voidaan päätellä.
Henkilötietojen käsittelijä	Taho, joka käsittelee henkilötietoja rekisterinpitäjän lukuun. Käsittelijä voi olla viranomainen, virasto, luonnollinen henkilö, oikeushenkilö tai muu elin.
Henkilötietojen käsittely	Kaikki ne toiminnot, joita kohdistetaan henkilötietoihin tai henkilötietoja sisältäviin tietojoukkoihin joko automaattista tietojenkäsittelyä käyttäen tai manuaalisesti, kuten tietojen kerääminen, tallentaminen, muokkaaminen, pseudonymisointi tai anonymisointi, haku, käyttö, tietojen luovuttaminen, säilyttäminen, poistaminen tai tuhoaminen Henkilötietojen käsittelyn on oltava asianmukaista ja sen on tapahduttava tiettyä tarkoitusta varten laissa säädetyn käsittelyyn oikeuttavan perusteen nojalla.
Kyberturvallisuus	Tietoturvallisuuden alalaji, jolla pyritään sähköisen ja verkotetun yhteiskunnan turvallisuuteen. Kyberturvallisuudessa tunnistetaan ja ehkäistään sähköisten ja verkotettujen järjestelmien häiriöitä sekä varaudutaan niiden mahdollisiin vaikutuksiin, jotka kohdistuvat yhteiskunnan kriittisiin toimintoihin.
Luottamuksellisuus	Tieto on vain siihen oikeutettujen saatavilla.
Rekisterinpitäjä	Voi olla viranomainen, virasto, oikeushenkilö, luonnollinen henkilö tai muu elin. Rekisterinpitäjä määrittää henkilötietojen käsittelyn tarkoitukset ja keinot yksin tai yhdessä toisten kanssa.
Riskienhallinta	Koordinoitu toiminta, jolla organisaatiota johdetaan ja ohjataan riskien osalta. Riskienhallinta sisältää riskien tunnistamisen, riskien analysoinnin, riskienhallintaan liittyvien toimenpiteiden suunnittelun, toteutuksen ja seurannan.
Saatavuus	Tarkoittaa esimerkiksi prosessien, tietojen ja tietojärjestelmien käytettävissä olemista.
Tietosuoja	Jokaiselle kuuluva perusoikeus, joka turvaa rekisteröidyn oikeuksien ja vapauksien toteutumisen henkilötietojen käsittelyssä.
Tietosuojaperiaatteet	• Henkilötietoja käsitellään lainmukaisesti, asianmukaisesti sekä läpinäkyvästi • Henkilötietoja käsitellään suunnitellun käyttötarkoituksen mukaisesti • Henkilötietoja kerätään käyttötarkoituksen mukaisesti • Henkilötietojen käsittely toteutetaan täsmällisesti

	• Henkilötietoja säilytetään käyttötarkoitukseen nähden tarkoituksenmukainen aika • Henkilötietojen käsittelyssä toteutetaan henkilötietojen eheyden ja luottamuksellisuuden periaatetta • Osoitusvelvollisuus
Tietoturvallisuus	Tietoturvallisuus koostuu tietoturvaan ja tietosuojaan liittyvistä vastuista ja käytännöistä. Käytännöillä pyritään varmistamaan tietojen ja tietojärjestelmien luottamuksellisuus, eheys ja saatavuus. Turvattava tieto voi ilmetä useassa eri muodossa, kuten fyysisenä tai digitaalisena tallenteena, tai tallentamattomana, kuten puheena. Tietoturva koskee tiedon suojaamista myös sen siirtämisen aikana.

1. JOHDANTO

Tietoturva- ja tietosuojapolitiikka määrittää Pohjois-Savon sairaanhoitopiirin ylimmän johdon asettaman tavoitetilan tietoturvallisuudelle ja tietosuojalle. Sairaanhoitopiirin hallitus riskienhallinnan ja tietosuoja- ja tietoturvaturvatoiminnan omistajana määrittelee tässä politiikassa johtamiseen, palveluihin ja toimintoihin liittyvät tietoturvallisuuden ja tietosuojan periaatteet, vastuut ja tavoitteet. Tietoturva- ja tietosuojapolitiikkaa täydentävät kaksi liitettä ja useat periaatedokumentit. Dokumentit tarkastetaan ja tarvittaessa päivitetään vuosittain.

Tietoturva- ja tietosuojapolitiikka (jatkossa: politiikka) kattaa Pohjois-Savon sairaanhoitopiirin; Kuopion yliopistollisen sairaalan ja perusterveydenhuollon liikelaitos Kysterin (jatkossa sairaanhoitopiirillä tarkoitetaan näitä molempia tässä dokumentissa). Politiikka käsittää automaattisen, manuaalisen, kirjallisen ja suullisen tietojenkäsittelyn. Politiikkaan sisältyy myös vaitiolovelvollisuuden piiriin kuuluva tieto, jonka tahtomattaan saa tietoonsa esimerkiksi nähdessään henkilöitä sairaalassa. Politiikka toimii sairaanhoitopiirin ylimmän tason turvallisuusasiakirjana, sekä perustana periaatteille ja ohjeille.

Tieto, tietojärjestelmät ja tietotekniset laitteet, kuten lääkintälaitteet ovat välttämätön edellytys sairaanhoitopiirin toiminnan kannalta sen tuottaessa lakisääteisiä sosiaali- ja terveydenhuollon palveluja. Digitaalisten ratkaisujen ja palveluiden osuus lisääntyy osana palveluiden tarpeen arviointia, diagnosointia, hoitoa ja näihin liittyvien palveluiden tuottamista. Digitaalisten palveluiden, mm. pilvipalvelut, mukanaan tuomat erilaiset kyberuhat tarkoittavat nopeatahtisia muutostarpeita myös tietoturva- ja tietosuojavaatimusten toteuttamiseen. Sairaanhoitopiirin johto on sitoutunut tietoturvallisuuden ja tietosuojan johtamiseen sekä sen jatkuvaan kehittämiseen osana potilaan turvallisen hoidon toteuttamista.

Tietoturva- ja tietosuojapolitiikan tarkoituksena on sitouttaa sairaanhoitopiirin henkilökunta, opiskelijat, palveluntuottajat, luottamushenkilöt ja muut sidosryhmät tietoturvallisuuden ja tietosuojan vaatimustenmukaiseen toteuttamiseen. Politiikan tarkoitus on myös linjata tietoturva- ja tietosuojakäytäntöjä, sekä vahvistaa tietoturvan ja tietosuojan vaatimustenmukaisuus, organisointi ja vastuut sekä seurantamenetelmät.

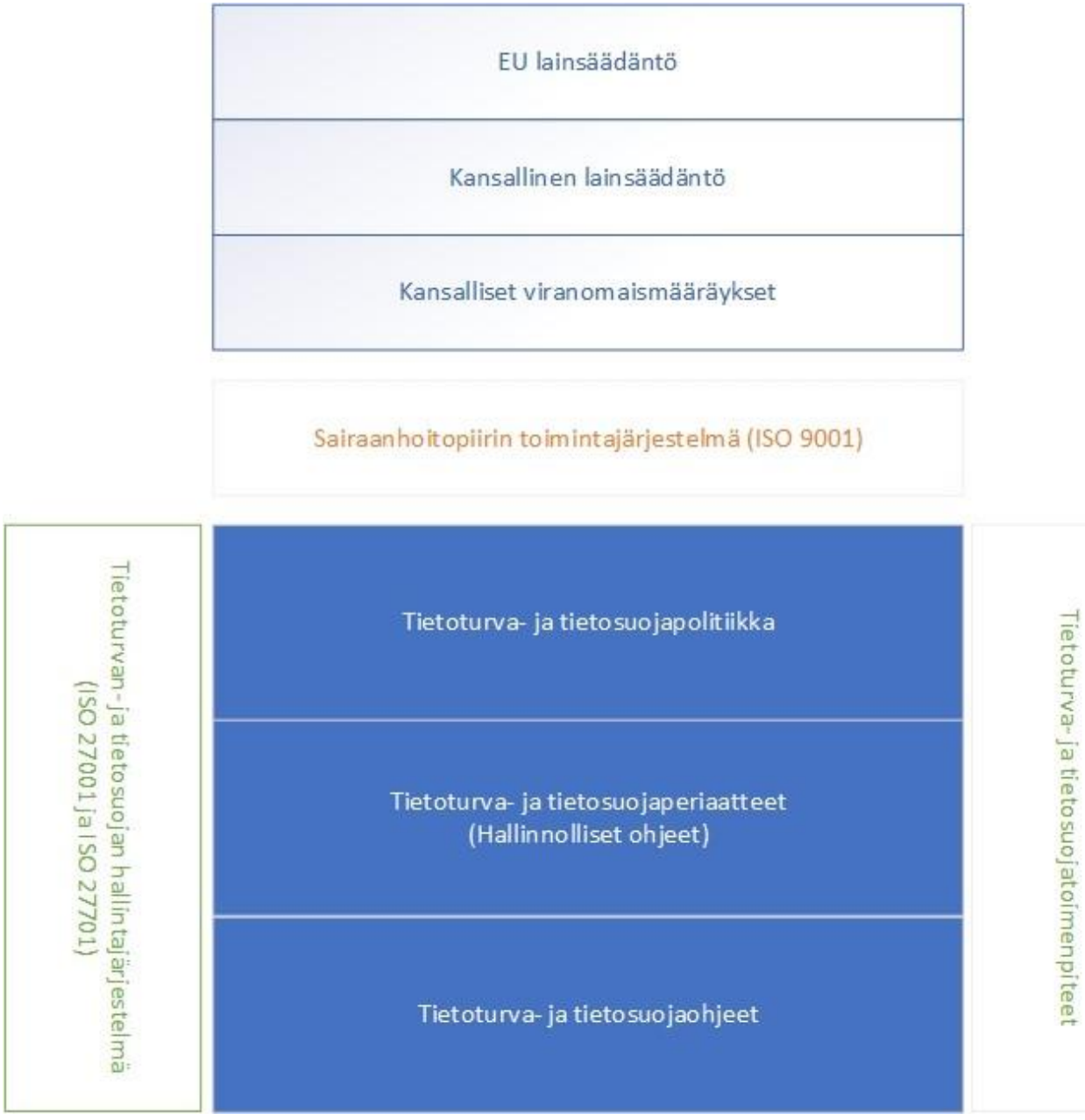
Sairaanhoitopiirin johto haluaa taata, että potilaat, asiakkaat, työntekijät, muut viranomaiset sekä muut sidosryhmät voivat luottaa siihen, että heidän tietojaan säilytetään turvallisesti, ne ovat täsmällisiä ja vain käyttötarkoituksen mukaisesti saatavissa. Tietojen käsittelyn lähtökohtana on virka- tai työtehtävien hoitaminen siinä laajuudessa kuin vastuut ja työtehtävät edellyttävät.

1.1 Tietoturva- ja tietosuojatoimintojen organisoituminen

Sairaanhoitopiirin tietoturva- ja tietosuojatoimintojen organisoituminen roolien ja vastuiden osalta on määritelty ”Tietoturvallisuuden, tietosuojan ja henkilörekisterien vastuut” -liitteessä.

1.2 Vaatimuksenmukaisuus

Luottamus tietojenkäsittelyyn voidaan ansaita vain varmistamalla tietojen eheys, saatavuus ja luottamuksellisuus sekä tietosuojaperiaatteiden toteutuminen. Tietojenkäsittelyä arvioidaan riskilähtöisesti ja toteutetaan asianmukaiset riskienhallintakeinot. Keskeinen tietoturvallisuuden ja tietosuojan ohjaus tulee lainsäädännöstä, kansainvälisistä standardeista ja sairaanhoitopiirin toimintajärjestelmästä. Kuvio 1. esittää tätä kokonaisuutta.



Kuvio 1.

Ylin ohjaava taso sairaanhoitopiirin tietoturvallisuuden ja tietosuojan hallinnassa on lainsäädäntö. Soveltuvaa lainsäädäntöä on sekä EU-tasolla että kansallisella tasolla. Keskeinen lainsäädäntö on kuvattu tämän tietoturva- ja tietosuojapolitiikan liitteessä 2. Lainsäädännön lisäksi toiminnassa huomioidaan toimivaltaisten viranomaisten määräykset ja standardit.

Sairaanhoitopiirin toiminta perustuu ISO 9001- standardiin. Toimintajärjestelmän keskeisiä osa-alueita ovat toimintajärjestelmän kuvaus, prosessit ja ohjeet. Tietoturvallisuuden ja tietosuojan hallintajärjestelmässä noudatetaan soveltuvin osin ISO 27001 ja ISO 27701 standardeja. Standardeilla pyritään varmistamaan laadukas, ajantasainen ja vaatimustenmukainen tietoturvan ja tietosuojan hallintajärjestelmä.

Politiikka on saatavilla sähköisesti kaikille työntekijöille, potilaille, asiakkaille, opiskelijoille, palveluntuottajille, luottamushenkilöille ja muille sidosryhmille. Tietoturva- ja tietosuojaperiaatteilla ohjataan politiikan asettamien tavoitteiden toteuttamista. Periaatteet ovat saatavilla sairaanhoitopiirin sisäisesti.

Tietoturvallisuudesta- ja tietosuojasta ohjeistetaan myös sovellus- tai käyttötarkoituskohtaisilla ohjeilla.

Sairaanhoitopiiri ylläpitää velvollisuutensa mukaisesti tietoturvasuunnitelmaa, joka omalta osaltaan varmistaa toiminnan lainmukaisuutta.

1.3 Tavoite

Tietoturvallisuudelle ja tietosuojalle on asetettu seuraavat tavoitteet:

- varmistaa tietosuojaperiaatteiden toteutuminen.
- varmistaa sisäänrakennettu ja oletusarvoinen tietosuoja.
- varmistaa rekisteröityjen oikeuksien toteutuminen.
- edistää rekisteröityjen oikeuksien toteutumista.
- lisätä rekisteröityjen luottamusta sairaanhoitopiiriin turvallisena palveluntuottajana.
- varmistaa tietojenkäsittelyn luottamuksellisuus, eheys ja saatavuus.
- varmistaa riittävä osaamisen taso, jotta eri työtehtävissä voidaan noudattaa tietoturvallisuuden ja tietosuojan periaatteita.
- tietoturvallisuuden ja henkilötietojen käsittelyn vastuut ovat kuvattu ja vastuita noudatetaan.
- tietojenkäsittelyyn liittyviä riskejä arvioidaan jatkuvasti ja toteutetaan riskiä vastaavat hallintatoimenpiteet.
- tietoturvallisuuden ja tietosuojan hallintajärjestelmällä varmistetaan systemaattinen hallinta jatkuva kehittäminen.
- muutostarpeet ja poikkeamat tietoturvallisuuden ja tietosuojan hallintajärjestelmässä dokumentoidaan ja analysoidaan säännönmukaisesti.

Tietoturvallisuuden ja tietosuojan tavoitteiden saavuttamista seurataan systemaattisesti erilaisten mittarien avulla. Raportointi tapahtuu säännönmukaisesti neljännesvuosittain ja vuosittain. Tietoturvallisuuden ja tietosuojan vuosikellolla hallitaan mm. tavoitteiden toteutumisen seurantaa, kehittämistä ja raportointia

1.4 Hallintatoimenpiteiden tarkoitus

Oikeinmitoitetuilla ja oikea-aikaisilla tietoturvallisuuden ja tietosuojan hallintatoimenpiteillä pyritään vähentämään todennäköisyyttä tietojen väärinkäyttöön ja muihin tietoturvaloukkauksiin. Suuri osa sairaanhoitopiirissä käsiteltävästä tiedosta on lainsäädännön nojalla

joko luottamuksellista, erityisiä henkilötietoja tai salassa pidettävää ja voi paljastuttuaan aiheuttaa riskin yksityisyydensuojalle ja yksilön oikeuksille ja vapauksille.

Tietoturvallisuuden ja tietosuojan hallintatoimenpiteillä varmistetaan tietojen saatavuus, eheys ja luottamuksellisuus. Toimenpiteillä vähennetään ja ennaltaehkäistään tietoturva- ja tietosuojariskejä. Tietoturvallisuuden ja tietosuojan toimenpiteillä varmistetaan henkilöiden oikeusturva ja yksityisyydensuoja vaatimusten mukaisesti.

1.5 Suojattavat kohteet

Tietojen ja tietojärjestelmien luokitukset on esitetty niitä käsittelevissä periaatteissa ja ohjeissa. Erityistä huomiota kiinnitetään organisaation toiminnan kannalta kriittisiin tietojärjestelmiin ja niiden sisältämiin tietoihin. Kriittisiä tietojärjestelmiä ovat asiakas- ja potilastietojärjestelmät sekä talous- ja henkilöstöhallinnon tietojärjestelmät. Suojattavat kohteet luetteloidaan ja priorisoidaan kriittisten kohteiden tunnistamisen perustaksi.

Ensisijaiset suojattavat kohteet sairaanhoitopiirissä ovat:

- Toimintaprosessit (esimerkiksi potilaiden hoitoprosessit)
- Tieto (henkilötiedot, erityiset henkilötiedot, julkiset tiedot, salassa pidettävät tiedot)
- Laitteistot
- Ohjelmistot
- Tietoverkko
- Fyysiset tilat

2 TIETOTURVALLISUUDEN JA TIETOSUOJAN TOTEUTTAMINEN

Tietoturvallisuuden ja tietosuojan hallintajärjestelmän jatkuvaa ylläpitämistä toteutetaan hallinnollisten, fyysisten ja teknisten hallintatoimenpiteiden avulla. Tässä politiikassa määritellään linjaukset tietoturvallisuuden ja tietosuojan vaatimustenmukaisuudelle.

2.1 Tärkeimmät hallinnolliset tietoturvallisuuden toimenpiteet

<u>Osaamisen varmistaminen</u>
Tietoturva- ja tietosuojapolitiikan, ohjeiden ja koulutusten saatavuudesta koko henkilöstölle ja sidosryhmille huolehditaan.

<u>Jatkuvuudenhallinta</u>
Kriittisten tietojärjestelmien ja tietoverkkojen keskeytymätön toiminta pyritään turvaamaan kaikissa tilanteissa. Tietojen ja tietojärjestelmien valtuudeton käyttö ja tahaton tai tahallinen tiedon tuhoutuminen tai vääristyminen pyritään estämään, sekä minimoidaan mahdollisesti aiheutuvat vahingot. Normaaliajan toiminnan tietojenkäsittelyn turvaamisen lisäksi varaudutaan toiminnan mahdollisesti keskeyttäviin uhkatilanteisiin.

Sairaanhoitopiirin tiedot, tietojenkäsittelyjärjestelmät ja -palvelut pidetään asianmukaisesti suojattuina sekä normaali- että poikkeusoloissa hallinnollisten, teknisten ja muiden toimenpiteiden avulla.

<u>Tietojen suojaaminen</u>
Sairaanhoitopiirin tiedot, tietojärjestelmät ja laitteet ovat tarkoitettu vain työtehtävien hoitamiseen ja muu käyttö pääsääntöisesti on kielletty. Sairaanhoitopiirille tai sen sidosryhmille mahdollisesti aiheutetun vahingon osalta vahingonkorvauksia voidaan vaatia vaarantumisen aiheuttajalta.

Poikkeamienhallinta
Sairaanhoitopiiri on ohjeistanut tietoturvapoikkeamien ja henkilötietojen tietoturvaloukkausten ilmoittamisesta sekä käsittelystä erillisessä dokumentissa.

Riskienhallinta
Tietoturvallisuuden ja tietosuojan riskejä hallitaan riskienhallintaprosessin avulla. Hyväksyttävän riskitason määrittelee johtoryhmä riskianalyysin tulosten perusteella ja yhteisesti valmisteltujen kriteeristöjen ja mittarien avulla. Tämä on kuvattu erillisessä dokumentissa: Tietoturva- ja tietosuojariskienhallinnan periaatteet.

Omistajuus ja vastuut
Kaikille prosesseille, tietoaineistoille, tietovarannoille, tietojärjestelmille ja laitteistoille, sekä sairaanhoitopiirin omille ja ulkoistetuille palveluille on määritetty omistajat sekä vastuuhenkilöt. Nämä omistajat ja vastuuhenkilöt kirjataan ja ylläpidetään tietojärjestelmien osalta tiedonhallintamallissa. Tiedonhallintamallin tietoja ylläpidetään tietojärjestelmäsalkussa. Tietojärjestelmäsalkkuun merkitään myös tietojärjestelmän kriittisyystaso ja mahdollinen korotettu tietoturvan ja tietosuojan taso.

Omistaja sekä vastuuhenkilö vastaavat tietoturvallisuudesta ja tietosuojasta koko elinkaaren ajan voimassa olevan lainsäädännön ja sairaanhoitopiirin tietoturva- ja tietosuojapolitiikan, periaatteiden ja ohjeiden mukaisesti. Näihin kuuluvat vastuu tietojärjestelmään sisältyvien henkilörekisterien oikeellisuudesta ja lainmukaisuudesta, kuten tietosuoja-asetuksen mukaisista rekisterinpitäjän velvollisuuksista sekä asianmukaisesta riskihallinnasta.

2.2 Tärkeimmät hallinnolliset tietosuojatoimenpiteet

Riskilähtöinen lähestymistapa
Sairaanhoitopiirissä on nimetty tietosuojavastaava, joka raportoi ylimmälle johdolle.

Riskilähtöisyys ohjaa henkilötietojen käsittelyä sairaanhoitopiirissä ja on tärkeä osa rekisterinpitäjän osoitusvelvollisuuden toteuttamista. Sairaanhoitopiirissä arvioidaan henkilötietojen käsittelyn riskejä. Mikäli käsittelystä aiheutuu todennäköisesti korkeita riskejä ihmisten oikeuksille ja vapauksille laaditaan vaikutustenarviointi. Jos todennäköisiä korkeita riskejä ei saada sairaanhoitopiirin toimenpitein laskettua, tulee tehdä ennakkokuulemispyyntö tietosuojavaltuutetulle. Vaikutustenarviointi on jatkuvan riskienhallinnan työkalu ja sen tuloksia käytetään riskienhallintakeinojen määrittelemisessä. Sairaanhoitopiiri valitsee arvioidun riskitason mukaiset tarvittavat hallintatoimenpiteet.

Henkilötietojen siirtoon EU:n tai ETA-alueen ulkopuolelle kohdistuu erityisiä vaatimuksia. Sairaanhoitopiirissä noudatettavat menettelyt määritellään erillisessä ohjeessa.

Sairaanhoitopiiri toteuttaa sisäänrakennetun ja oletusarvoisen tietosuojan periaatetta ja sisällyttää tietoturva- ja tietosuojaperiaatteet ja -vaatimukset jo aikaisessa vaiheessa osaksi henkilötietojen käsittelyä. Näin varmistetaan, että käsittely vastaa tietosuoja-asetuksen sekä muun lainsäädännön ja määräysten asettamia vaatimuksia. Tietosuojan toteuttamisessa sairaanhoitopiiri varmistaa tietosuojalainsäädännön vaatimusten toteutumisen koko käsiteltävien henkilötietojen elinkaaren ajan.

Sairaanhoitopiirin järjestelmä- ja sovelluskehitysprosesseissa on mukana työvaiheet, joissa varmistetaan henkilötietojen käyttötarkoituksiin sovellettavien tietosuojavaatimusten täyttyminen. Riskitason perusteella valitaan tilanteeseen sopivat hallintakeinot riskitason hallitsemiseksi ja vaatimustenmukaisuuden saavuttamiseksi. Hallintakeinojen valinnassa huomioidaan parhaat mahdolliset käytännöt tietoturvan ja tietosuojan suhteen.

Tietosuojariskien hallinta on osa sairaanhoitopiirin riskienhallintaprosessia, ja merkittävän tason riskit raportoidaan johdolle saakka.

Toimittajat ja henkilötietojen käsittelijät
Sairaanhoitopiiri voi rekisterinpitäjänä ulkoistaa valitsemansa osan henkilötietojen käsittelystä toimeksisaajalle ts. henkilötietojen käsittelijälle.

Sairaanhoitopiiri valitsee sopimuskumppanikseen vain sellaisia henkilötietojen käsittelijöitä, jotka noudattavat hyvää henkilötietojen käsittelytapaa asianmukaisten teknisten ja organisatoristen toimenpiteiden avulla sekä täyttävät tietosuoja-asetuksen ja muun lainsäädännön sekä määräysten vaatimukset ja pystyvät huolehtimaan rekisteröidyn oikeuksien toteutumisesta. Henkilötietojen käsittelyä sisältävien hankintojen kohdalla tietoturvaan ja tietosuojaan liittyvät näkökohdat huomioidaan jo hankinnan suunnitteluvaiheessa ja saatetaan ne osaksi tarjouspyyntöä.

Sairaanhoitopiirin ja henkilötietojen käsittelijän välille laaditaan kirjallinen sopimus. Tietosuoja-asetuksen mukaan sopimuksessa tulee määritellä henkilötietojen käsittelyn kohde, tarkoitus ja kesto sekä sopia käsiteltävät henkilötiedot ehtoineen. Sopimuksen sisältö vaatimuksineen tulee määritellä mahdollisimman tarkasti.

Sairaanhoitopiiri rekisterinpitäjänä sisällyttää tietosuojan myös mm. kehittämishankkeiden ja tieteellisen tutkimuksen osaksi.

Rekisteröityjen oikeudet
Sairaanhoitopiirissä on määritetty toimintaprosessit ja ohjeet liittyen toimintaan rekisteröityjen käyttäessä tietosuojalainsäädännön mukaisia oikeuksiaan.

Koulutus ja perehdyttäminen
Sairaanhoitopiiri on asettanut koko henkilöstöä koskevat vaatimukset tietoturvallisuuden ja tietosuojan koulutuksille. Organisaatioon tulevat uudet työntekijät perehdytetään tietosuoja-asioihin järjestelmällisesti ja osaamista ylläpidetään säännönmukaisesti.

2.3 Tärkeimmät tekniset tietoturvatoimenpiteet

Toiminnan jatkuvuuden hallintaprosessin avulla varaudutaan onnettomuuksien ja häiriöiden (joita voivat aiheuttaa esim. luonnonmullistukset, onnettomuudet, laiteviat ja ilkivalta) aiheuttamiin keskeytyksiin. Jatkuvuussuunnitelmia kehitetään ja toteutetaan varmistamaan, että toimintaprosessit saadaan ylläpidettyä myös keskeytyksen aikana ja palautettua riittävän nopeasti. Suunnitelmia pidetään yllä ja harjoitellaan integroituna osana toimintaa.

Käyttöturvallisuudella luodaan ja ylläpidetään tietotekniikan turvallisen käytön vaatimat toimintaolosuhteet. Tämä tapahtuu huolehtimalla ICT:n toimivuuden valvonnasta, käyttöoikeuksista, käytön- ja lokien valvonnasta, ohjelmistotuesta, ylläpito-, kehittämis- ja huoltotoimintoihin liittyvistä turvallisuustoimenpiteistä, varmuus- ja suojakopioinnista sekä häiriöraportoinnista.

Kriittisten komponenttien, palvelinten, työasemien, käyttöjärjestelmien sekä ohjelmistojen turvapäivityksiä varten palveluntuottajilla on toimintasuunnitelma. Päivitystarvetta seurataan aktiivisesti ja päivitysten kriittisyys arvioidaan ennakolta. Kriittiset päivitykset asennetaan viivytyksettä ja asennukset dokumentoidaan. Tietoturvapäivitysten asennukset keskitetään ja automatisoidaan mahdollisuuksien mukaan.

Lokien muuttumattomuus ja kiistämättömyys varmistetaan. Lokeja säilytetään lakien tai muun sääntelyn edellyttämä aika. Kansalaisen tiedonsaanti lokitiedoista lainsäädännön sekä määräysten mukaisesti.

Sairaanhoitopiiri vastaa järjestelmien tietoturvasta (saatavuus, eheys ja luottamuksellisuus) ja laadusta yhdessä palveluntuottajien kanssa tehtyjen sopimusten mukaisesti. Palveluiden saatavuus, käytettävyys, luotettavuus, hallinnointi ja valvonta on sovittu palveluntuottajien kanssa tehtävissä sopimuksissa.

Käyttövaltuushallintaprosessi vastuineen ja poikkeusmenettelyineen (erillinen ohjeistus) on määritelty ja kuvattu käyttövaltuushallinnan periaatteissa ja ohjeissa. Käyttöoikeudet perustuvat henkilön tehtävään ja vastuisiin. Käyttäjälle myönnetään tehtävänmukaiset oikeudet tietoihin ja tietojärjestelmiin.

Sairaanhoitopiirissä on prosessi hankinnoissa ja projekteissa tehtävälle tietoturva- ja tietosuoja-arvioinnille. Tämän prosessin avulla varmistetaan asianmukainen riskienhallinta ja lainsäädännön sekä tämän politiikan mukaisten periaatteiden toteutuminen hankinnoissa ja projekteissa. Prosessissa käytetään vahvistettuja tietoturva- ja tietosuojavaatimuksia.