Etelä-Pohjanmaan sairaanhoitopiirin tietoturva- ja tietosuojapolitiikka

1. Johdanto

Tietoturva- ja tietosuojapolitiikka määrittelee ne periaatteet, vastuut, toimintatavat sekä seurannan ja valvonnan, joita sairaanhoitopiirissä ja sen tuottamissa alueellisissa ICT-palveluissa noudatetaan tietoturvan toteuttamisessa ja kehittämisessä.

Tietoturva- ja tietosuojapolitiikkaa täydentävät tietoturva- ja tietosuojaperiaatteet ja -käytännöt – dokumentti sekä koko henkilökunnalle annetut ohjeet.

Tietojenkäsittely tukee sairaanhoitopiirin palvelujen tuottamista. Sairaanhoitopiiri tuottaa tietojärjestelmäpalveluita myös alueen julkisen terveydenhuollon organisaatioille. Tietoaineistot sisältävät potilaisiin, asiakkaisiin, työntekijöihin ja toimintaan liittyvää tietoa, joka on lainsäädännön perusteella suojattava. Tietojenkäsittelyn on oltava mahdollisimman luotettavaa, tehokasta ja virheetöntä. Tietojenkäsittelyyn liittyy aina inhimillisenä toimintana riskejä, joita minimoidaan mm. ohjeistuksilla, teknisillä ratkaisuilla ja koulutuksella. Vain pieni osa tietoturvariskeistä pystytään välttämään teknisillä ratkaisuilla. Tärkeintä on jokaisen henkilön päivittäisessä tietojen käsittelyssä tekemät ratkaisut ja toimenpiteet, jotka pohjautuvat lainsäädännön ja ohjeiden noudattamiseen.

Kyberturvallisuus käsittää yhteiskunnan elintärkeisiin toimintoihin ja kriittiseen infrastruktuuriin kohdistuvat toimenpiteet, joiden tavoitteena on saavuttaa kyky ennakoivasti hallita ja tarvittaessa sietää kyberuhkia ja niiden vaikutuksia, jotka voivat aiheuttaa merkittävää haittaa tai vaaraa. Terveydenhuollon toiminnot ovat jatkuvasti entistä riippuvaisempia ICT-teknologiasta ja palveluista sekä niiden toimintavarmuudesta. Tietojen käsittelyyn ja tietotekniikkaan liittyviä riskejä pitää tunnistaa ja hallita aktiivisesti. Riskien negatiivisia vaikutuksia minimoidaan teknisillä ja hallinnollisilla keinoilla.

Tietoturvalla tarkoitetaan tietojen, palvelujen, järjestelmien ja tietoliikenteen suojaamista. Tietosuoja on oleellinen osa tietoturvallisuutta. Tietosuojalla tarkoitetaan henkilötietojen ja muiden henkilön luottamuksellisten tai arkaluonteisten tietojen suojaamista ja rekisteröidyn henkilön oikeutettujen oikeuksien ja vapauksien tehokasta toteuttamista.

Tietoturvan tärkeyttä lisäävät myös kansalaisille suunnattujen sähköisten palveluiden laajentuminen, tietojärjestelmien etä- ja mobiilikäytön lisääntyminen sekä palvelutuotannon uudet menetelmät kuten pilvipalvelut.

Sairaanhoitopiirin henkilökunnan ja sen luottamushenkilöiden sekä ulkopuolisten terveydenhuollon toimijoiden, toimittajien ja muiden ulkopuolisten tahojen tulee sitoutua noudattamaan tätä tietoturva- ja tietosuojapolitiikkaa, sairaanhoitopiirin ohjeita, kansallisia normeja ja ohjeita.

2. Määritelmät

Tietoturvallisuuden keskeisillä käsitteillä tarkoitetaan seuraavaa:

Käytettävyys eli tieto on siihen oikeutettujen hyödynnettävissä haluttuna aikana.

Todentaminen (autentikointi) eli varmistuminen kohteen todenmukaisuudesta, oikeellisuudesta, alkuperästä tai varmistuminen käyttäjän aitoudesta halutulla luottamustasolla.

Kiistämättömyys ilmentää sitä, että tiedon lähettäjä tai vastaanottaja tai tietoon liittyvä tapahtuma voidaan varmistaa luotettavasti myös jälkikäteen.

Tietosuojaan liittyvät käsitteet **henkilötieto, henkilötietojen käsittely, henkilörekisteri, rekisterinpitäjä, rekisteröity** ja **suostumus** määritellään ja yleisessä tietosuoja-asetuksessa (2016/679).

Yksityisyyden suoja on tietoturvan ja tietosuojan toteuttamista organisaatiossa.

Tietoturva tarkoittaa tietojen käsittelyn turvaamista.

Tietosuojan keskeisiä periaatteita ovat:

lainmukaisuus, kohtuullisuus ja läpinäkyvyys;

käyttötarkoitussidonnaisuus; Henkilötietoja käytetään vain siihen käyttötarkoitukseen, joihin tiedot on kerätty;

tietojen minimointi; Henkilötietoja kerätään vain siinä määrin, kuin on välttämätöntä kyseessä olevan tehtävän hoitamiseksi;

täsmällisyys; Tietojen on oltava paikkansapitäviä ja täsmällisiä;

säilytyksen rajoittaminen; Tietojen säilyttämiselle on asetettava aika, jonka jälkeen tiedot on hävitettävä tai ainakin määriteltävä peruste, jonka mukaan säilytysaika määräytyy ja

eheys ja luottamuksellisuus; Tiedot on säilytettävä muuttumattomina ja turvallisesti niin, että niihin pääsee käsiksi vain sellaiset henkilöt, joiden tehtävien hoitamiseksi tiedot ovat välttämättömiä.

Potilaan mahdollisuus käyttää oikeuksiaan turvataan. Potilaan mahdollisuus valvoa ja määrätä häntä koskevien henkilötietojen käytöstä täydentää sairaanhoitopiirin toteuttamaa valvontaa.

Henkilötietojen käsittelyn on oltava läpinäkyvää ja potilaan luottamusta edistävää.

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 tietoturva- ja tietosuojapolitiikan mukaisen tietoturvan ja tietosuojan tulee olla luonnollisena lähtökohtana kaikessa toiminnassa. Tietoturvan ja tietosuojan kehittäminen ja ylläpito sekä sen seuranta ovat osa sairaanhoitopiirin yleistä turvallisuustoimintaa, riskien hallintaa ja sisäistä valvontaa.

Toimintalähtöisesti painottuvalla tietoturva- ja tietosuoja -asioiden hoidolla tuetaan oman organisaation toiminnalle asetettuja vaatimuksia. Lisäksi tietojen ja tietojärjestelmien huolellinen käsittely takaa osaltaan kansalaisten yksityisyyden suojaa. Tietoturvatyö on tietoturvan saavuttamiseksi tehtävien toimenpiteiden suunnittelua ja toteuttamista.

Tietosuoja on oleellinen osa tietoturvallisuutta. Tietosuojalla tarkoitetaan henkilötietojen ja muiden henkilön luottamuksellisten tai arkaluonteisten tietojen suojaamista ja rekisteröidyn oikeuksien tehokasta toteuttamista.

Lainsäädännön perusteella henkilötietoja suojataan 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. Terveydenhuollon 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.

Kyberturvallisuudessa tunnistetaan, ehkäistään ja varaudutaan sähköisten ja verkotettujen järjestelmien häiriöiden vaikutuksiin yhteiskunnan kriittisiin toimintoihin. Kyberturvallisuusajattelussa yhdistyy tietoturvallisuuden, jatkuvuuden hallinnan ja yhteiskunnan kriisivarautumisen ajattelua.

3. Tietoturvan ja tietosuojan toimintaa ohjaavat tekijät

Tietoturvatoimintaa ohjataan sekä EU:n että kansallisin säädöksin, määräyksin, ohjein ja suosituksin. Näihin liittyviä päätöksiä tehdään sekä omassa organisaatiossa että sen ulkopuolella.

Lainsäädännön lisäksi tulee noudattaa muita omalle organisaatiolle hyväksyttyjä tietoturvaan ja tietosuojaan liittyviä ohjeita ja määräyksiä. Organisaation omat päätökset, määräykset ja ohjeet eivät saa olla ristiriidassa tämän tietoturvapolitiikan tai organisaation ylemmän tason määräysten kanssa siten, että tietoturva tai tietosuoja heikkenee.

3.1 Organisaatiot ja vastuut

Tietoturvallisuus on koko sairaanhoitopiirin yhteinen asia.

3.1.1 Ylin vastuu

Tietoturvallisuudesta vastaa sairaanhoitopiirin hallitus ja sitä johtaa sairaanhoitopiirin johtaja. Sairaanhoitopiirin hallitus päättää sairaanhoitopiirin kokonaisturvallisuuden eri osa-alueiden kehittämistoiminnan tavoitteista, organisoinnista, resursseista ja toimintavaltuuksista sekä nimeää tietoturvavastaavan ja tietosuojavastaavan. Potilastietojen tietoturvasta vastaa johtajaylilääkäri.

Sairaanhoitopiirin potilastietoja sisältävien henkilörekistereiden suojaamisesta ja valvonnasta vastaa osaltaan tietosuojavastaava. Tietoturvavastaava vastaa osaltaan sairaanhoitopiirin tietoturvatyön kokonaisuudesta johdolta saamiensa resurssien ja toimintavaltuuksien puitteissa.

3.1.2 Esimiesten vastuut

Tietoturva- ja tietosuoja-asioiden toteutumisesta, tiedottamisesta ja valvonnasta omassa yksikössään vastaavat yksiköiden esimiehet. Jokaisen esimiehen on huolehdittava, että tietoturva- ja tietosuojamääräykset ja ohjeet koulutetaan ja perehdytetään henkilöstölle. Esimiesten tulee valvoa, että henkilöstö noudattaa tietoturvasta ja tietosuojasta annettuja määräyksiä ja ohjeita.

3.1.3 Henkilöstön vastuu

Jokainen organisaation tietoja ja tietojärjestelmiä käyttävä on velvollinen ilmoittamaan havaitsemistaan tietoturvallisuuden puutteista, uhkista tai menettelyvirheistä eteenpäin tietohallinnon ohjeistamalla tavalla. Tietoturvallisuudesta annettujen ohjeiden toteutumisesta vastaa kukin toimintayksikkö. Yksiköiden pää- ja vastuukäyttäjät vastaavat, että yksiköissä on riittävä tietämys tietojärjestelmien käyttämisestä ja annetuista ohjeista.

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 tietosuojavastaavalle ja/tai johtajaylilääkärille, henkilöstötietoihin liittyvät asiat raportoidaan henkilöstöjohtajalle ja tietosuojavastaavalle. Tietoturvavastaavalle raportoidaan havaituista tietoturvan puutteesta, tietoturvaan liittyvästä väärinkäytöksestä tai epäilemästään tietoturvarikkomuksesta.

3.1.4 Tehtävät

Tietoturva- ja tietosuojavastaavilla on velvollisuus valvoa, seurata ja raportoida havaittujen tietoturvan heikkouksia. Tietoturva- ja tietosuojavastaava antavat tietotilinpäätöksen raporttina sairaanhoitopiirin hallitukselle kerran vuodessa. Tietoturvavastaava ja tietosuojavastaava vastaavat osaltaan tietoturva- ja tietosuojaperiaatteet ja -käytännöt -dokumentin tekemisestä ja ylläpidosta, toteutuksen valvonnasta ja tietoturvatietouden edistämisestä.

Tietoturva- ja tietosuojavastaavien toiminnan tukena on tietoturva- ja tietosuojaryhmä, jonka asettaa sairaanhoitopiirin johtoryhmä. Tietoturva- ja tieto-

suojaryhmä käsittelee tietoturvan linjaukset ja ohjeet ennen kuin ne esitellään johdolle hyväksyttäväksi. Ryhmä ottaa tarvittaessa kantaa valmisteltaviin asioihin. Ryhmä käsittelee osaltaan HaiPro-ilmoitukset koskien tietoturvaa ja tietosuojaa. Ryhmään kuuluvat ainakin tietoturvavastaava, tietosuojavastaava, tietohallintojohtaja, arkistopäällikkö, turvallisuuspäällikkö, kaksi lääkäriedustajaa ja ylihoitaja. Ryhmän jäsenet tuovat työryhmän käsiteltäväksi esiin nousseita tietoturvaan ja tietosuojaan liittyviä asioita. Tietosuojavastaava toimii tietoturva- ja tietosuojaryhmän puheenjohtajana.

Tietosuojavastaava osallistuu suunnittelutoimintaan, ohjeiden valmisteluun ja ylläpitoon sekä tietosuojakoulutuksiin. Tietosuojavastaava tukee henkilökuntaa ja rekisteröityjä tietosuoja-asioissa sekä seuraa ja valvoo henkilötietojen käsittelyä sekä suojausmenettelyä.

Tietoturvavastaava vastaa osaltaan sairaanhoitopiirin tietoturvallisuustason määrittämisestä, arvioinnista ja raportoinnista sekä muusta hallinnollisesta tietoturvasta.

3.1.5 Kolmannet osapuolet

EPSHP:lle palveluja tuottavat tahot tulee velvoittaa nimeämään tietoturva- sekä tietosuoja-asioihin yhteyshenkilö, joka heillä vastaa sovitun tietoturva- ja tietosuojatason noudattamisesta. Kumppanien tulee viipymättä ilmoittaa omista organisaatioon vaikuttavista tietoturvapoikkeamistaan ilmoitetuille yhteyshenkilöille. Kumppaneille asetettavat vaatimukset (mm. varautumisesta) tulee kuvata kunkin sopimuksessa tai sen erillisessä liitteessä.

3.1.6 Tietoturvallisuuteen ja tietosuojaan kohdistuvat uhat

Tietoturvallisuuteen kohdistuvat uhat aiheuttavat riskin tietojen, tietojärjestelmien tai tietoliikenteen luottamuksellisuudelle, eheydelle ja käytettävyydelle.

Henkilöiden mahdollinen osaamattomuus, huolimattomuus ja välinpitämättömyys aiheuttavat merkittävimmän uhan organisaation tietoturvallisuudelle. Lisäksi uhkia aiheuttavat tietoisesti tehty tietojen väärinkäyttö, tietomurrot, virheellisesti toimivat ohjelmistot ja laitteet, virukset, haittaohjelmat, palvelunestohyökkäykset sekä tekniset ongelmat. Merkittäviä uhkia voi liittyä myös ulkopuolisten palvelujen tuottamiseen, mikäli palveluntuottajien kanssa ei ole tehty sopimuksia, joissa huomioidaan tietoturvaan, tietosuojaan ja varautumiseen liittyvät asiat sekä rikkomuksiin liittyvät sanktiot.

EPSHP:n organisaatiossa, prosesseissa, projekteissa ja tietojärjestelmissä tulee huolehtia tietoturvaan ja tietosuojaan sekä laajemminkin tietotekniikkaan liittyvien riskien hallinnasta.

4. Tietoturvallisuuden merkitys ja toteuttaminen

4.1 Turvattavat kohteet

Toiminnan tietoturvallisuuden kannalta tärkeimmät turvattavat kohteet ovat henkilöt, tilat, laitteet, tietoliikenne, tietojärjestelmät, ohjelmistot, palvelut sekä tiedot ja tietoaineistot kaikissa olomuodoissaan.

Näiden kohteiden turvaamisen tavoitteena on operatiivisten järjestelmien ja sisäisen tietojenkäsittelytoiminnan ja tietosuojan turvaaminen sekä palvelujen tuottaminen normaalioloissa ja normaaliolojen häiriötilanteissa, sekä poikkeusoloissa.

4.2 Tietoturvaperiaatteet

Yhteisesti noudatettavat tietoturva- ja suojaperiaatteet ovat seuraavat:

- Asiat pitää tehdä tietoturvallisesti, millä tarkoitetaan tiedon suojaamista monenlaisilta uhkilta. Tarkoituksena on varmistaa toiminnan jatkuvuus, minimoida toiminnalliset riskit sekä maksimoida investoinneista ja toiminnan mahdollisuuksista saatu tuotto.
- Tietoturva- ja tietosuoja-asiat pitää huomioida välineestä riippumatta eli ne eivät liity vain **tietojärjestelmien käyttämiseen.**
- Paperiset asiakirjat, sähköiset tietovarannot, tietojärjestelmät, tietotekniset laitteet, tietoverkot ja niihin liittyvät palvelut on pidettävä asianmukaisesti suojattuina sekä normaali- että poikkeusoloissa.
- Tietoturvallisuuden saavuttamiseksi toteutetaan tarvittavia turvamekanismeja, jotka muodostuvat toimintaperiaatteista, prosesseista, organisaatiorakenteista ja ohjelmisto- ja laitteistotoiminnoista.
- On varmistettava, että luottamukselliset, arkaluonteiset ja muut salassa pidettävät asiat kuuluvat vaitiolovelvollisuuden piiriin riippumatta siitä, miten tai mihin niitä on tallennettu tai millä tavalla tiedot on saatu.
- Tietosuojanäkökulma on otettava huomioon kaikessa toiminnassa siten, että henkilötietojen turvallinen käsittely on toiminnan lähtökohtana.
- Sairaanhoitopiirin valvontaa täydentää rekisteröidyn mahdollisuus itse valvoa ja määrätä henkilötietojensa käytöstä mm. tarkastamalla häntä koskevat tiedot ja vaatimalla virheellisten tietojen korjaamista.

4.3 Tietoturvallisuuden toteutumista tukevia käytäntöjä

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

Sairaanhoitopiirin tietoturvaperiaatteet perustuvat EU:n tasoisiin, kansallisiin, yleisiin ja toimialakohtaisiin tietoturvaa, henkilörekistereitä, hyvää tiedonhal-

lintatapaa ja tiedon laatua ohjaaviin ja velvoittaviin säädöksiin, ohjeisiin ja standardeihin. Lainsäädännön ja ohjeistuksen muutokset otetaan huomioon sairaanhoitopiirin tietoturvan kehittämisessä.

Tietoturvan toteuttaminen ja ylläpito kuvataan tietoturva- ja tietosuojaperiaatteet ja -käytännöt -dokumentissa. Tietoturvan tavoitteiden saavuttaminen on jatkuva prosessi, jota tuetaan hallinnollisten ja teknisten ratkaisujen avulla. 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 määritteleminen tapahtuvat säännöllisesti suoritettavilla turvallisuusanalyyseillä.

Käyttäjien toimintaa ohjataan henkilökohtaisella ja riittävällä perehdytyksellä, saatavilla olevilla toimintaohjeilla sekä koulutuksella. Jokainen käyttäjä sitoutuu noudattamaan tietoturva- ja tietosuojaohjeita saadessaan oikeuden tehtäviensä mukaiseen tietojärjestelmien ja tietoaineistojen käyttöön.

4.4 Tietojärjestelmien hankinta ja omistaminen

Jokaisella tietojärjestelmällä on omistajayksikkö ja pääkäyttäjä. Laajemmilla järjestelmillä voi olla myös erikseen vastuukäyttäjiä. Omistaja on mukana järjestelmien hankintavaiheesta alkaen koko elinkaaren ajan.

Uusien tietojärjestelmien, prosessien sekä tilojen tietoturva-asiat tulee huomioida ja testata hankintavaiheessa. Tietojärjestelmien toimintaa ja käyttöä tulee valvoa. Sisäisten tietojärjestelmien tietojen käyttö tulee pääsääntöisesti sallia vain työtehtävien tai niihin rinnastettavien tehtävien hoitamiseen sekä yhteistyökumppaneilla vastaavasti sopimusten ja lupien mukaisten tehtävien hoitamiseen.

Organisaatioille ja tietojenkäsittely-ympäristöille voidaan asettaa eritasoisia teknisiä ja hallinnollisia vaatimuksia (tietoturvallisuustasoja) muun muassa sen mukaan millaisia tietoja kohteessa käsitellään.

Tietoturvan ja tietosuojan toteuttamisessa tulee käyttää tarvittaessa ulkopuolisten asiantuntijoiden apua. Tietoturvan ja tietosuojan vaatimusten toteutuminen tietojärjestelmissä ja projekteissa on hyvä tarkastaa eli auditoida ulkopuolisella asiantuntijataholla tai sisäisesti jo määrittelyvaiheessa, mutta pakollista se on ennen kuin uusi tietojärjestelmä voidaan ottaa tuotantokäyttöön. Sellaisille tietojen käsittelytoimille, joista mahdollisesti aiheutuu riski tietosuojan toteutumiselle, eli riski henkilötietojen käsittelyssä, on ennen käsittelytoimen ryhtymistä toteutettava vaikutustenarviointi. Palvelujen hankintaan ja ulkoistuksiin liittyvissä sopimuksissa pitää huomioida turvallisuuteen ja varautumiseen liittyvät asiat. Sopimuskumppanit sitoutetaan sopimuksin noudattamaan tietosuojalainsäädännön vaatimuksia, tekemään yhteistyötä tietoturvan ja tietosuojan kehittämisessä sekä tiedottamaan havaitsemistaan poikkeuksista.

4.5 Jatkuvuus

Toiminnan jatkuvuus tulee turvata toipumissuunnittelulla, joka sisältää häiriöiden ennalta ehkäisemisen ja mahdollistaa niistä nopean toipumisen. Toipumissuunnittelussa tulee erityisesti huomioida mahdolliset liiketoiminnan riskit ja prioriteetit. Tietosuojan näkökulmasta on turvattava rekistereiden palautettavuus ja käytettävyys häiriötilanteissa. Rekisterissä olevan tiedon on oltava käytettävissä ja ongelmatilanteissa on varmistettava tietojen säilyvyys, eheys, ja palautettavuus mahdollisimman tehokkaasti.

Tietojärjestelmiin ja tietojen käsittelyyn liittyvissä suunnitelmissa, järjestelyissä sekä ohjeissa varaudutaan tietoturvallisuutta ja tietosuojaa koskevien laiminlyöntien, vahinkojen tai virheiden jälkikäteisselvittämiseen.

4.6 Turvatoimet

Turvatoimien järjestys tilanteissa, joissa joudutaan toteuttamaan priorisointia.

- henkilön hengen tai terveyden turvaaminen
- arkaluonteisen tai muuten erittäin merkittävän tiedon luottamuksellisuuden turvaaminen
- tietojärjestelmien ja rekistereiden eheyden turvaaminen
- käyttö- ja toimintaympäristön käytettävyyden turvaaminen

5. Tietoturvallisuuden hallintajärjestelmä

Hallintajärjestelmän avulla toteutetaan tietoturvan hallintaa ja seurantaa sekä arvioidaan tietoturvatoimien tehokkuutta ja tarkoituksenmukaisuutta. Järjestelmän jatkuva kehittäminen parantaa valmiuksia hallita tietoturvallisuutta järjestelmällisesti. Vaikutustenarvionti on osa tietosuojan jatkuvaa kehittämistä ja tietoturvariskien muutokset ja riskien kehitys on otettava jatkuvalla tavalla huomioon.

6. Tietoturva- ja tietosuojakoulutus ja -ohjeet

Uusien työntekijöiden perehdytyksessä hyödynnetään Intra-sivujen sähköistä perehdytysosiota. Tietoturvallisuus tulee olla sisällytettynä perehdytysprosessiin. Koulutusta järjestetään ja mahdollistetaan kaikille työntekijöille määräajoin. EPSHP:n tietoturva- ja tietosuojaohjeet pidetään ajan tasalla ja niistä kerrotaan työntekijöille sekä kaikille organisaation tietoja ja tietojärjestelmiä käyttäville muille henkilöille. Ohjeistuksiin tehtävistä muutoksista tulee tiedottaa käyttäjiä ja tarvittaessa järjestää lisäkoulutuksia.

Tietojärjestelmien käyttäjiltä edellytetään käyttö- ja salassapitositoumuksen hyväksyminen.

Tietoturvaan ja tietosuojaan liittyvien ohjeiden sisällöstä ja ajantasaisuudesta vastaavat nimetyt tietoturvan ja tietosuojan vastuuhenkilöt.

7. Tiedottaminen

Tietoturva- ja tietosuoja-asioista tiedotetaan tarpeen mukaan. Tietoturva-asioiden sisäisestä tiedottamisesta vastaavat tietoturvan ja tietosuojan vas-

tuuhenkilöt yhdessä viestinnästä vastaavan tahon kanssa. Tietoturva- ja tietosuoja-asioihin liittyvät ohjeet ovat saatavilla EPSHP intranet-sivuilta. Ulkopuolisille tiedottamisessa noudatetaan sairaanhoitopiirin Viestintäohjetta. Rekisteröidylle tiedottamisessa noudatetaan, mitä lainsäädännössä on määrätty niin säännönmukaisesta tiedottamisesta, kuin myös tiedottamisesta häiriötilanteissa. Rekisteröidyn tiedottaminen on osa rekisteröidyn oikeuksien käyttämisen tehokkuuden toteuttamista.

8. Valvonta ja rikkomusten seuraamukset

Tietojen ja tietojärjestelmien käyttöä valvotaan olemassa olevien lakien ja asetusten mukaisesti huomioiden yksityisyyden suoja työelämässä.

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 tai sen perusteella on mahdollista päättää työ- tai virkasuhde. Tietoturvarikkomuksesta voi seurata myös rikosoikeudellinen vastuu.

Toiminnan oikeellisuus on epävarmuustilanteessa varmistettava ensisijaisesti lähiesimieheltä tai tietoturva- ja tietosuojavastaavalta.