Tietoturvapolitiikka

22.5.2018

Kanta-Hämeen sairaanhoitopiirin ky. • 13530 Hämeenlinna • Puh. 03 6291

Hämeenlinnan yksikkö
Ahvenistontie 20
13530 HÄMEENLINNA
vaihde 03 6291

Riihimäen yksikkö
Kontiontie 77, 11120 RIIHIMÄKI
PL 140, 11101 RIIHIMÄKI
vaihde 019 744 51

Sisällys

1. Visio

Kanta-Hämeen Sairaanhoitopiirin kuntayhtymän (jatkossa Sairaanhoitopiiri) lakisääteisenä tehtävänä on huolehtia alueen väestön tarpeen mukaisen hyvän ja laadukkaan erikoissairaanhoidon järjestämisestä. Sairaanhoitopiiri on luotettava ja ammattimainen terveydenhuollon toimija ja kumppani, jonka tietoturva ja tietosuoja toteutetaan hyvää hallintotapaa noudattaen. Sairaanhoitopiirille eri osapuolten luottamus on kunnia-asia.

Tietoturvallisuus- ja tietosuojatoimenpiteet ovat Sairaanhoitopiirin strategiaa ja arvoja tukevia sekä lakeihin ja säädöksiin perustuvia. Tietoturvatietoisuutta kehitetään ja käyttäjiä kannustetaan tietoturvatietoiseen käyttäytymiseen. Toiminnan ja kulttuurin kehittämisessä sekä kaikissa työtehtävissä huomioidaan tietoturvallisuus tärkeänä ominaisuutena. Tietoturvallisuuden toteutumista ja riittävyyttä mitataan vuosittain sairaanhoitopiiritason laatuarvioinnin yhtenä osana.

Sairaanhoitopiirin tietojenkäsittelyn ja sen turvaamisen periaatteet noudattavat kansallisia ja kansainvälisiä tietoturvallisuutta koskevia säädöksiä, standardeja, terveydenhuollon auditointivaatimuksia ja suosituksia. Näistä keskeisimpiä ovat EU:n tietosuoja-asetus, julkisuuslaki, laki potilaan asemasta ja oikeuksista sekä laki potilastietojen sähköisestä käsittelystä. Kaikessa toiminnassa noudatetaan hyvää tietojenkäsittelytapaa, velvoitteita ja sopimuksia. Tietoturvaratkaisujen tulee noudattaa myös taloudellisia realiteetteja, eivätkä ne saa vaikeuttaa merkittävästi tietojärjestelmien hyötykäyttöä ja asiakaspalvelua.

Sairaanhoitopiirin asiakkaiden, potilaiden ja kumppaneiden tietoja käsitellään ja säilytetään luottamuksellisesti huomioiden sekä sisäiset, että ulkoiset vaatimukset. Sairaanhoitopiirin oma ja Sairaanhoitopiirin asiakkaiden toiminta sekä erityisesti potilaiden turvallinen ja häiriötön hoito on varmistettu sekä vahinkomahdollisuudet on rajattu tasolle, joka on Sairaanhoitopiirin toiminnan kannalta hyväksyttävissä.

Sairaanhoitopiiri
- tekee sopimuksia ainoastaan sellaisten organisaatioiden kanssa, jotka huolehtivat tietoturvastaan Sairaanhoitopiirin vaatimusten mukaisesti
- arvioi ja seuraa kumppaneidensa tietoturvakäytäntöjen toteutumista, tarvittaessa itseauditoinnein tai Sairaanhoitopiirin määrittämän auditoijan toimesta

2. Yleistä

Tietoturvapolitiikan tarkoituksena on luoda organisaatiolle ohjaavat käsitteet ja tavoitteet, joiden kautta tietoturvatyötä tehdään. Tämä tietoturvapolitiikka koskee koko Sairaanhoitopiiriä ja sen henkilökuntaa, kumppaneita ja palveluntoimittajia. Kaikki henkilökunnan edustajat sekä tarpeen mukaan eri sidosryhmät, jotka toimivat Sairaanhoitopiirin lukuun, perehdytetään Sairaanhoitopiirin tietoturvapolitiikkaan sekä tarvittaviin ohjeisiin.

Sairaanhoitopiirin tarjoama hyvä ja laadukas hoito edellyttää useita keskenään tukevia toimintoja, joista tärkeimpiä on potilastietojen käsittely. Hoidon yhteydessä tarvitaan erilaisia tietoja potilaasta ja hoitohistoriasta.

Hoidon yhteydessä syntyy myös uutta tietoa, jotka talletetaan myöhempää käyttöä varten. Hoidon dokumentointi on Sairaanhoitopiirin lakisääteinen velvollisuus ja olemassa olevan tiedon hyödyntäminen on hyvän hoidon edellytys.

Potilastietojen samoin kuin muiden henkilötietojen käsittelyssä noudatetaan seuraavia EU:n tietosuoja-asetuksen mukaisia tietosuojaperiaatteita:

- käsittelyn lainmukaisuus, kohtuullisuus ja läpinäkyvyys,
- käyttötarkoitussidonnaisuus,
- tietojen minimointi,
- tietojen täsmällisyys,
- tietojen säilytyksen rajoittaminen
- tietojen eheys ja luottamuksellisuus.

Mainitut periaatteet määritellään tarkemmin sairaanhoitopiirin tietosuojaperiaatteissa.

Tietoturvallisuudesta ja tietosuojasta huolehtii koko Sairaanhoitopiirin henkilöstö. Sairaanhoitopiirillä on operatiivinen vastuu tietojärjestelmien ja niiden käytön häiriöttömyydestä ja turvallisuudesta.

Potilaiden turvallinen ja häiriötön hoito edellyttävät tietoturvallisuuden luotettavaa järjestämistä. Tämän varmistamiseksi tietoturvallisuuden sekä tietosuojan toteutumista seurataan aktiivisesti. Poikkeamat kirjataan ja niihin puututaan nopeasti ennalta määriteltyjen menetelmien mukaisesti. Potilas-, asiakas- ja muita henkilötietoja käytetään vain sopimusten ja lainsäädännön sallimiin tarkoituksiin ja ne ovat vain niitä työhönsä tarvitsevien käytössä.

Tietoturvallisuutta toteutetaan ja kehitetään käyttäen tarkoituksenmukaisia ja vaatimustenmukaisia ratkaisuja. Toiminnassa huomioidaan henkilöstön, asiakkaiden ja sidosryhmien sopimukset, yksityisyyden suoja, salassapitovelvoitteet sekä muut lainsäädännölliset vaatimukset. Tietoturvallisuuden toteutuminen varmennetaan vuosittain toimintakertomukseen tai sen liitteeseen tulevalla maininnalla suoritetuista toimenpiteistä.

3. Käytännöt

Tietoturvatoimilla estetään tietojen luvaton käyttö ja haltuunotto. Suurin osa Sairaanhoitopiirissä käsiteltävästä tiedosta on luottamuksellista, arkaluonteista sekä salassa pidettävää ja voi paljastuttuaan rikkoa yksityisyyden suojaa.

Tietoturvatoiminnan tavoitteena on vastata siitä, että tieto on oikeaan aikaan, oikeassa paikassa ja oikean muotoisena niiden henkilöiden käytettävissä, joilla on siihen laillinen tai työtehtävänsä vaatima valtuutus.

Sairaanhoitopiirin henkilöstön ja sidosryhmien on tutustuttava tietoturva- ja tietosuojaohjeistuksiin. Lisäksi jokaisen potilas- tai henkilötietoja käsittelevän henkilön on käytävä tietoturva- ja tietosuojakoulutus hyväksytysti läpi vuosittain.

Tietosuoja- ja tietoturvaryhmä tekee yhteisesti päätökset tietoturvaan ja tietosuojaan kohdistuvissa parannuksissa ja korjaavissa toimenpiteissä.

Tietoturva tai tietosuoja eivät saa vaarantaa potilasturvallisuutta tai haitata potilaiden hoitoa.

Kaikissa tiedon käsittelyyn liittyvissä epäselvissä asioissa tulee ottaa yhteyttä tietosuoja- ja tietoturvaryhmään.

3.1. Tietoturva

Tietoturvalla tai tietoturvallisuudella tarkoitetaan tietoliikenne-, laitteisto-, ohjelmisto- ja tietoaineistotoiminnan turvallisuutta, joilla turvataan verkkojen ja palvelujen eheys, tietojen luottamuksellisuus ja käytettävyys. Eheydellä tarkoitetaan tiedon paikkansapitävyyttä. Tieto ei saa muuttua tahattomasti tai hyökkäyksen seurauksena. Luottamuksellisuudella tarkoitetaan, että tietoa voivat käsitellä vain sellaiset henkilöt, joilla on siihen oikeus. Käytettävyydellä tarkoitetaan saatavuutta, eli tiedon on oltava saatavilla, kun sitä tarvitaan. Tietoturvallisuuden ohjauksessa avainasemassa ovat yhteistyö ja tiedonvaihto. Tietoturvariskejä arvioidaan ja analysoidaan.

Kaikilla organisaation tiedoilla ja tietoja hallinnoivilla järjestelmillä on vastuullinen omistaja.

Fyysisestä tietoturvallisuudesta tulee huolehtia asianmukaisesti.

Sairaanhoitopiirin järjestelmien käyttöoikeus- ja pääsynhallinta tehdään keskitetysti. Kaikkien käyttöoikeuksien tulee perustua tarpeeseen ja tarpeen poistuttua oikeudet tulee poistaa. Kaikkia käytössä olevia järjestelmiä ja palveluja saa käyttää ainoastaan omin henkilökohtaisin tunnuksin ja käyttäjäoikeuksia katselmoidaan sekä auditoidaan säännöllisesti. Jokaisella käyttövaltuudella ja järjestelmällä on oltava omistaja.

Tietoturvallisuuden varmistamiseksi Sairaanhoitopiiri valvoo ja tarvittaessa rajoittaa ohjelmistoja, laitteita ja tiedostomuotoja, joita järjestelmissä käytetään. Vain hyväksyttyjen ohjelmistojen ja laitteiden käyttö on sallittua.

Tietoturvatason parantaminen ja ylläpitäminen edellyttävät toiminnan systemaattista ja jatkuvaa valvontaa. Valvontaa suorittavia henkilöitä sitoo osaltaan vaitiolovelvollisuus ja heiltä edellytetään vaitiolositoumusta. Tietoturvatilanteesta raportoidaan sisäisen valvonnan sekä sisäisten ja ulkoisten tarkastusten yhteydessä.

Palveluntuottajien ja muiden kumppaneiden on sitouduttava noudattamaan Sairaanhoitopiirin määrittämiä tietoturvavaatimuksia ja ne varmistetaan sopimuksin. Palveluntuottajat ja muut kumppanit ovat velvollisia ilmoittamaan poikkeamista Sairaanhoitopiirille. Toimittajille ja kumppaneille voidaan tehdä tarkastuksia tietoturvallisuuden toteutumisen varmistamiseksi.

Sairaanhoitopiirillä on menetelmät tietoturvapoikkeamien havaitsemiseksi ja suunnitelmat poikkeustilanteiden varalle. Poikkeamat kirjataan ja niihin puututaan ennalta määriteltyjen menetelmien mukaisesti.

3.2. Tietosuoja

Tietosuojalla tarkoitetaan EU tietosuoja-asetuksen mukaista henkilötietojen käsittelyä ja keruuta koskevien vaatimusten huomioimista, jotta voidaan turvata tiedon kohteen yksityisyys, edut, oikeudet ja oikeusturva. Henkilöllä on oikeus tarkastaa, mitä tietoja hänestä on tallennettu rekisteriin ja saada virheelliset tiedot korjatuksi. Henkilötietoja ei saa kerätä ilman yksilön suostumusta. Viranomaisella on oikeus kerätä ja käsitellä henkilötietoja laissa säädettyjen tehtäviensä hoitamiseksi (laki terveydenhuollon valtakunnallisista henkilörekistereistä / laki potilastietojen sähköisestä käsittelystä).

Henkilötietoja saa käsitellä ainoastaan kyseisissä työtehtävissä kulloinkin niitä tarvitsevat henkilöt. Tietosuojakäytäntöjen toteutumista valvoo tietosuojavastaava. Henkilötietoja sisältäviin järjestelmiin tehdään tietoturvatarkastuksia.

Tietoja käsitellään Sairaanhoitopiirissä niin, että kaikki osapuolet voivat luottaa käsittelyn asianmukaisuuteen. Samalla turvataan hoidon mahdollisimman sujuva ja häiriötön toteutuminen.

Palveluntuottajien ja tarpeen mukaan muiden kumppaneiden on sitouduttava noudattamaan Sairaanhoitopiirin määrittämiä tietosuojavaatimuksia ja ne varmistetaan sopimuksin. Sopimuksen nojalla nämä ovat velvollisia ilmoittamaan poikkeamista Sairaanhoitopiirille.

4. Rikkomukset ja seuraamukset

Tietoturvarikkomus on Sairaanhoitopiirin tulkinnan mukaan mikä tahansa tietoturvapolitiikan, tietoturva- tai tietosuojaohjeistuksen vastainen toiminta. Kaikki rikkomusepäilyt tutkitaan.

Tietoturvallisuutta seurataan hallinnollisesti ja teknisesti. Seurannassa noudatetaan lakeja, sopimuksia ja hyviä valvontaperiaatteita. Rikkomustilanteet käsitellään lojaliteettirikkomuksina ja työnantajan ohjeiden vastaisina toimina. Rikkomuksista saattaa seurata kurinpidollisia sekä rikosoikeudellisia toimenpiteitä.

Sairaanhoitopiirillä on erillinen kirjallinen ohje tietoturvaloukkaustilanteissa toimimiseen.

5. Vastuut ja organisointi

Sairaanhoitopiirin hallitus vastaa kuntayhtymän riskienhallinnan järjestämisestä sekä hyvän tiedonhallintatavan ja hyvän henkilötietojen käsittelyn toteuttamisesta. Näin ollen hallitus myös ohjaa tietoturvallisuutta ja valvoo sen toteutumista kuntayhtymässä.

Sairaanhoitopiirin johtoryhmä varmistaa tietoturvapolitiikan ja siihen liittyvien periaatteiden toimeenpanon organisaatiossa, toimii tietosuojatyön ohjausryhmänä (3-4 krt vuodessa) ja seuraa tietosuojatyön etenemistä (mm. tietosuojasuunnitelman ja tietotilinpäätöksen esittelyt johtoryhmässä) sekä määrittää tarkemmat vastuut ja käsittelee tietoturvapolitiikkaan ja siihen liittyviin periaatteisiin ja ohjeisiin tehtävät muutokset sekä huolehtii resursoinnista (henkilöstö, järjestelmät, osaaminen).

Rekisterinpitäjä vastaa henkilötietojen käsittelyn lainmukaisuudesta. Jokaiselle henkilörekisterille on nimettävä operatiivinen vastuuhenkilö.

Tietoturvapäällikkö vastaa sairaanhoitopiirin tietoturvallisuuden kehittämisestä, johtaa tietoturva- ja tietosuojaryhmää, toimii tietoturvan asiantuntijana, koordinoi tietojärjestelmien turvallisuustoimenpiteiden toteutusta, selvittää teknisten ja oikeudellisten kysymysten rajapintoja yhdessä tietosuojavastaavan kanssa, käsittelee tietojärjestelmiin ja tietoturvaan liittyvät HaiPro -ilmoitukset, huolehtii tietoturva-asioista tiedottamisesta yleisellä tasolla Sairaanhoitopiirin sisällä yhteistyössä viestintäpäällikön kanssa sekä raportoi tietoturvasta Sairaanhoitopiirin johtoryhmälle. Tietoturvapäällikölle nimetään varahenkilö, joka huolehtii tehtävästä hänen poissa ollessaan.

Tietosuojavastaava toimii asiantuntijana EU-tietosuoja-asetuksen noudattamista koskevissa asioissa, neuvoo henkilötietojen käsittelyä koskevissa kysymyksissä, valvoo tietosuojaohjeiden olemassaoloa ja noudattamista, käsittelee tietosuojaan liittyvät HaiPro -ilmoitukset, antaa pyydettäessä neuvoja tietosuojaa koskevasta vaikutusten arvioinnista ja valvoo sen toteutumista sekä toimii organisaation yhteyshenkilönä ao. valvontaviranomaisiin. Tietosuojavastaavalle nimetään varahenkilö, joka huolehtii tehtävästä hänen poissa ollessaan.

Tietosuoja- ja tietoturvaryhmä tukee tietoturvapäällikköä ja tietosuojavastaavaa sekä organisaatiota jokapäiväisessä tietoturvaan liittyvässä työssä johdolta saamiensa resurssien ja toimintavaltuuksien puitteissa. Ryhmä valmistelee ohjeita ja laatii suosituksia, suunnittelee koulutuksia ja kehittää edelleen tietosuojaa ja tietoturvaa sekä seuraa määräysten noudattamista. Ryhmä huolehtii osaltaan henkilöstön ja sidosryhmien tietoturvatietoisuudesta ja tietoturvauhkiin valmistautumisesta. Ryhmä käsittelee sille toimitetut tietojärjestelmiin, tietoturvaan ja tietosuojaan liittyvät HaiPro -ilmoitukset.

Tulosyksikön johtaja vastaa yksikössään tietoturvapolitiikan ja siihen liittyvien periaatteiden ja ohjeiden läpikäymisestä ja valvoo niiden noudattamista sekä huolehtii siitä, että myös uudet työntekijät perehdytetään näihin.

Kaikkien organisaation jäsenten velvollisuutena on tutustua annettuihin ohjeisiin ja noudattaa niitä sekä tiedottaa havaituista tietoturvauhista ja -riskeistä tietosuoja- ja tietoturvaryhmälle.

Tietoturvapolitiikkaa noudatetaan kaikessa toiminnassa ja ne koskevat kaikkia Sairaanhoitopiirin palveluksessa olevia henkilöitä, luottamushenkilöstöä ja sidosryhmiä.

6. Ohjehierarkia, päätöksenteko ja viestintä

Sairaanhoitopiirillä on yksi tietoturvapolitiikka, joka sisältää sekä tietoturvan että tietosuojan linjaukset. Tätä dokumenttia täydennetään erillisillä tietoturva- ja tietosuojaperiaatteilla sekä -ohjeilla.

Hallintosäännön 98 §:n mukaan sairaanhoitopiirin hallitus vastaa hyvän tiedonhallintatavan ja hyvän henkilötietojen käsittelyn toteuttamisesta. Näin ollen hallitus hyväksyy tämän asiakirjan. Tietoturva- ja tietosuojaperiaatteet hyväksyy johtoryhmän käsittelyn jälkeen sairaanhoitopiirin johtaja päätöksellään.

Tietoturvapolitiikka julkaistaan sairaanhoitopiirin internet- ja intrasivuilla ja siitä tiedotetaan henkilöstöä ja sidosryhmiä. Periaatteet ja ohjeet ovat tarkoitettu vain Sairaanhoitopiirin sisäiseen ja sidosryhmien käyttöön.

Tietoturvaan ja tietosuojaan liittyvät tarpeet huomioidaan sairaanhoitopiirin viestintä- ja koulutussuunnitelmissa.

7. Liittyvät dokumentit

Tietoturvaperiaatteet
Tietosuojaperiaatteet
Tietoturvaohje
Tietosuojaohje
Ohje tietoturvaloukkaustilanteissa toimimiseen
Tietosuojan ja -turvan omavalvontasuunnitelma