RIIHIMÄEN SEUDUN TERVEYSKESKUKSEN KY

Tietoturvapolitiikka

Riihimäen seudun terveyskeskuksen kuntayhtymä
Penttilänkatu 5, 11100 Riihimäki
Puh. +358 19 758 5500

Yhtymähallitus 18.4.2018

Sisällysluettelo

1 Johdanto

1.1 Yleistä

Riihimäen seudun terveyskeskuksen (jatkossa kuntayhtymä) hallinto- ja palvelutehtävien tehokas ja laadukas suorittaminen edellyttää hyvin toimivaa tietojenkäsittelyä. Toiminta edellyttää monenlaisia tietoja hallinnollisten päätösten kohteista ja palvelua saavista henkilöistä. Hallinto- ja palvelutehtävien yhteydessä syntyy myös uutta tietoa, jota tallennetaan myöhempää käyttöä varten. Toiminnan dokumentointi on monessa tapauksessa lakisääteinen velvollisuus ja olemassa olevan tiedon hyödyntäminen hyvään lopputulokseen johtavan toiminnan edellytys.

Luottamus tietojenkäsittelyyn on ehdoton edellytys toimiville hallinto- ja palveluprosesseille. Tietoturvan ensisijainen tarkoitus on varmistaa tietojen asianmukainen käsittely kuntayhtymän toiminnassa. Päivittäisessä työssä tämä tarkoittaa pääasiassa sitä, että tiedot ovat helposti käytettävissä, mutta tietoja voi käyttää ainoastaan niitä työssään tarvitsevat henkilöt. Järjestelmiä suunniteltaessa ja hankittaessa on otettava huomioon järjestelmille asetettavat käytettävyysvaatimukset sekä tiedon muuttumattomuuden turvaaminen.

Tietoturva pidetään kuntayhtymässä mahdollisimman korkealla tasolla ja se huomioidaan kaikessa toiminnassa ja toiminnan kehittämisessä. Tietoturva on tärkeää hoidon onnistumisen ja käytännön toiminnan kannalta. Kuntayhtymän perustehtävä on asiakkaille annettava terveyden- ja sairaanhoito. Hoidon antajalla on lakisääteinen velvollisuus dokumentoida potilaalle annettu hoito. Luottamus asiakkaan ja terveyskeskuksen välillä on onnistuneen hoidon edellytys. Jos potilas ei esimerkiksi luota siihen, että tieto pysyy luottamuksellisena, hän saattaa jättää hoidon kannalta olennaisia tietoja kertomatta. Kuntayhtymän toiminta on hyvin riippuvainen tiedoista ja tietotekniikasta. Hyvällä tietoturvalla taataan organisaation toiminnan onnistuminen ja häiriötön jatkuminen.

Kuntayhtymän tietojenkäsittelyn ja sen turvaamisen periaatteet noudattavat kansallisia ja kansainvälisiä tietoturvallisuutta koskevia säännöksiä, standardeja ja suosituksia. Säännöksistä keskeisimpiä ovat henkilötietolaki, laki viranomaisten toiminnan julkisuudesta, laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä sekä Euroopan Unionin tietosuoja-asetus ja -direktiivi. Kuntayhtymä noudattaa kaikessa toiminnassa hyvää tietojenkäsittelytapaa, velvoitteita ja sopimuksia. Tietoturvaratkaisujen tulee noudattaa myös taloudellisia realiteetteja, eivätkä ne saa vaikeuttaa merkittävästi tietojärjestelmien hyötykäyttöä ja asiakaspalvelua.

1.2 Soveltamisala ja tavoite

Kuntayhtymän tietoturvapolitiikkaa noudatetaan kaikessa toiminnassa ja se koskee koko kuntayhtymän palveluksessa olevaa henkilökuntaa, luottamushenkilöitä ja niitä ulkopuolisia tahoja ja yhteistyökumppaneita, joille kuntayhtymä on osoittanut vastuullaan olevia tehtäviä tehtäväksi ja/tai tietoja käsiteltäväksi. Tietoturvapolitiikka on voimassa toistaiseksi ja voimassaolo jatkuu, ellei sitä nimenomaisesti kumota.

Tietoturvapolitiikka koskee kaikkea kuntayhtymän omistamaa ja säilyttämää tietoa, sekä kaikkia kuntayhtymän tietojärjestelmiä.

Tietoja käsitellään kuntayhtymän toiminnoissa niin, että kaikki osapuolet voivat luottaa käsittelyn asianmukaisuuteen. Samalla turvataan ensisijaisen hallinto- tai palvelutehtävän mahdollisimman sujuva ja häiriötön toiminta. Tietoturvallisuus ei saa estää tai haitata toimintaa, mutta samalla on toimittava säädösten vaatimalla tavalla. Tämän päämäärän saavuttamiseksi:

- kaikkien tietoa käsittelevien henkilöiden on ymmärrettävä tietojen käsittelyn periaatteet: mitä tietoa saa käsitellä, missä tarkoituksessa tietoa saa käsitellä, milloin tietoa saa käsitellä sekä myös tietyissä tilanteissa ymmärrettävä ja hyväksyttävä asiakkaiden halu ja oikeus kieltää tietojensa käsittely,
- käyttäjien, ylläpitäjien ja johdon tietoturvatietoisuus on oltava hyvä. Kaikkien tulee ymmärtää tehtävänsä ja velvollisuutensa tietoturvallisuuden ylläpidossa,
- tietoturvaa toteutetaan kaikilla tasoilla siten, että tietoturva on mukana kaikessa toiminnassa,
- tietojen luottamuksellisuuden, eheyden ja saatavuuden vaatimus toteutuu kaikessa tietojenkäsittelyssä ja se mahdollistaa tietoturvallisen asioinnin ja tietojen käytön,
- tietoturvallisuuden vaatimukset otetaan huomioon kaikessa kehittämistoiminnassa.

Tietoturvallinen toimintatapa on sisäänrakennettuna kuntayhtymässä, toimintaprosesseissa ja tietojärjestelmissä.

2 Tietoturvalinjaukset

2.1 Periaatteet

2.1.1 Luottamuksellisuus

Kuntayhtymän tai ulkoistetun palvelun tuottajan henkilökunta ei luovuta luottamuksellista tietoa, kuten potilastietoa, ulkopuolisille. Luottamuksellista tietoa ei luovuteta missään tiedon muodossa (sähköisesti, paperilla, suullisesti, jne.). Tietoa luovutetaan vain asianomistajan suostumuksella. Tietoja voidaan kuitenkin luovuttaa ilman potilaan suostumusta viranomaiselle ja muille tahoille, joilla on tiedon saantiin laissa säädetty oikeus.

Henkilökunta sitoutuu luottamuksellisuuteen allekirjoittamalla salassapito- ja käyttäjäsitoumukset. Käyttöoikeuksia tietojärjestelmiin annetaan vain työntekijän tehtävän vaatimiin tietoihin. Henkilökunnan käytössä on ajantasainen tietoturvaohjeistus. Henkilökunnalle annetaan säännöllisesti tietoturvakoulutusta ja henkilökunta ymmärtää tietoturvan merkityksen.

Kuntayhtymän tiedottamisesta vastaa yhtymäjohtaja tai johtajaylilääkärin tai heidän valtuuttamansa henkilö voimassaolevan tiedotussuunnitelman mukaisesti, elintarvikelain mukaisissa asioissa II kaupungineläinlääkäri tai hänen varahenkilönsä.

Tiedot ja tietojärjestelmät on suojattu niin, ettei sivullisilla ole mahdollisuutta nähdä, muuttaa tai tuhota tietoja.

Tietoja tuhottaessa tuhoaminen tehdään niin, ettei tuhottu materiaali ole sivullisten käytettävissä.

2.1.2 Eheys

Kuntayhtymän käytössä olevat järjestelmät ovat luotettavia ja tiedot on suojattu ulkopuolisilta uhilta, kuten rikoksilta, luonnontapahtumilta, laitteistohäiriöiltä, ohjelmistovirheiltä ja inhimillisen toiminnan häiriöiltä. Sähköisessä muodossa olevista tiedoista otetaan säännöllisesti ja systemaattisesti varmuuskopiot.

Tietojärjestelmät, niiden käyttöoikeudet ja lokitietojen kirjaaminen on rakennettu niin, että henkilökunnan käyttämät tiedot ovat oikeita, ajantasaisia ja kiistämättömiä. Tietojen alkuperä ja koskemattomuus voidaan tunnistaa ja varmistaa. Tietojärjestelmissä tietoaineisto on luetteloitu ja luokiteltu loogisesti.

2.1.3 Käytettävyys

Tietoturvatoiminnan tavoitteena on vastata siitä, että tieto on oikeaan aikaan oikeassa paikassa ja oikean muotoisena niiden henkilöiden käytettävissä, joilla on siihen laillinen ja työtehtävänsä mukainen valtuutus. Tietoturvatoimilla vähennetään ja ennaltaehkäistään tietoturvariskien syntyminen, varmistetaan tietojen saatavuus poikkeuksellisissa olosuhteissa, toiminnan jatkuvuus, asiakkaiden oikeusturva ja yksityisyyden suoja lainsäädännön ja muiden määräysten edellyttämällä tavalla, tietojen oikeellisuus ja luotettavuus sekä se, että asianosaiset ovat tiedostaneet tietoturvan merkityksen.

Varsinaisten hallinto- ja palvelutehtävien suorittajien lisäksi on sekä arkistotoimella että tietohallinnolla yhteisenä tavoitteena tietojen saatavuuden ja käytettävyyden turvaaminen. Tiedon käytettävyydellä ja saatavuudella tarkoitetaan, että tieto on tallennettu siten, että se on luettavissa, ymmärrettävissä ja tulkittavissa oikein, tieto on kattavaa ja ajantasaista ja muuten käyttökelpoinen vaadittavalla tavalla. Tiedon, tietojärjestelmän ja palvelun on oltava saatavilla ja hyödynnettävissä siihen oikeutetuille riittävän esteettömästi, vaivattomasti ja nopeasti vaaditulla tavalla ja vaadittuna aikana.

2.2 Suojattavat kohteet

Turvattavia tietoja ovat sekä manuaalisessa että sähköisessä muodossa olevat tiedot. Erityistä huomiota kiinnitetään kuntayhtymän toiminnan kannalta kriittisiin tietojärjestelmiin ja niiden sisältämiin tietoihin.

Kriittisiä tietojärjestelmiä ovat mm. asiakastietojen hallintajärjestelmät sekä talous- ja henkilöstöhallinnon ohjelmat. Em. tietojärjestelmät kuuluvat samaan tietoturvaluokkaan ja niiden turvaamisesta vastataan yhdenmukaiset vaatimukset täyttävin menettelyin. Tiedot, tietojenkäsittelyjärjestelmät ja -palvelut pidetään asianmutkaisesti suojattuina sekä normaali- että poikkeusoloissa hallinnollisten, teknisten ja muiden toimenpiteiden avulla. Jokaisella tietojärjestelmällä tai sen osalla on yksiselitteinen omistaja tai haltija. Tietoturvallisuuden toteuttamista ohjaavat dokumentit ovat vahvistettuja ja asianomaisten kohderyhmien saatavissa.

2.3 Valvonta

Hyväksytyn tietoturvapolitiikan mukaiset tietoturvatoimet sisällytetään ajantasaisella ohjeistuksella ja koulutuksella luonnollisena osana kaikkeen toimintaan. Tietoturvan kehittäminen ja ylläpito ovat osa kuntayhtymän yleistä turvallisuustoimintaa, riskien hallintaa ja sisäistä valvontaa. Tietoturva on kuntayhtymän toiminnan kriittinen tekijä erityisesti henkilöiden tietojen käsittelyn osalta, koska henkilön on voitava luottaa tietojensa tietosuojaan. Tietoturvallisuustyön tulee luoda asiakkaille ja henkilöstölle luottamus siitä, että salassapito- ja vaitiolovelvollisuus sekä yksityisyyden suoja toteutuvat säädösten mukaisesti ja tietoja käsitellään kaikissa vaiheissa huolella ja asianmukaisesti.

Kuntayhtymän toimintaa ohjaavat mm. tietosuojasäädökset sekä muut lait, säädökset, ohjeet ja standardit. Tietoturvallisuutta koskevat määräykset ovat keskeisiä ja velvoittavia. Velvoitteissa korostetaan salassapidon, vaitiolovelvollisuuden ja yksityisyyden suojan toteutumista sekä tietoturvallisuuden, tietosuojan, hyvän tietojenkäsittelytavan ja laadun merkitystä.

Kuntayhtymän tietoturvallisuuden kehittäminen tapahtuu kansallisten ja kansainvälisten tietoturvallisuutta koskevien lakien ja asetusten pohjalta sekä erilaisia tietoturvallisuudesta annettuja ohjeita ja suosituksia hyödyntäen. Asiakkaiden informointi henkilön tietojen käytöstä toteutetaan lakien ja valtakunnallisten ohjeiden sekä vaatimusten mukaisesti. Kuntayhtymän tietosuojavastaava vastaa ohjeiden jalkautuksesta ja tarvittavan koulutuksen järjestämisestä. Kuntayhtymän henkilöstölle on laadittu tietotekniikan käyttöön liittyen tietoturvaohje.

Voimassa olevat velvoittavat säädökset on luetteloitu ja niiden vaikutukset tietoturvajärjestelyihin on selvitetty. Lainsäädäntöä ja ohjeistusta seurataan jatkuvasti. Muutosten vaikutus otetaan huomioon kuntayhtymän tietoturvallisuuden kehittämisessä. Kuntayhtymän tiedot, tietojenkäsittelyjärjestelmät ja -palvelut pidetään asianmutkaisesti suojattuina sekä normaalien että poikkeusoloissa hallinnollisten, teknisten ja muiden erikseen kuvattujen toimenpiteiden avulla. Tietoturvariskejä hallitaan erikseen määritellyn ja kuvatun riskienhallintaprosessin avulla.

Tietoturvan toteutumista seurataan ja valvotaan säännöllisesti tietoturva- ja tietosuojavastaavien toimesta. Henkilökunta on velvollinen raportoimaan tietoturvarikkomuksesta.

3 Organisointi ja vastuut

3.1 Tietoturvaorganisaatio ja vastuut

Yhtymähallitus

- hyväksyy tietoturvapolitiikan.

Kuntayhtymän johtoryhmä

- vastaa tietoturvasta ja -suojasta yleisesti (ohjeistus, tiedottaminen ym.),
- huolehtii tietoturvapolitiikan täytäntöönpanosta,
- nimeää tietoturva- ja tietosuojavastaavat sekä tietoturvaryhmän.

Tietoturvaryhmä

- seuraa tietoturvan kehitystä yleisesti ja valmistelee asiaan liittyvää ohjeistusta,
- käsittelee tietoturvaan liittyviä ongelmia,
- kehittää tietoturvaa,
- seuraa ja raportoi tietoturvapoikkeamista johtoryhmälle,
- esittää johtoryhmälle ratkaisuja ja parannuksia tietoturvaan liittyvissä asioissa.

Tietoturvavastaava

- valvoo tietoturvan toteutumista,
- tunnistaa tietoturvaan liittyvät ongelmat ja vie ne tietoturvaryhmän käsiteltäväksi,
- osallistuu alueelliseen tietoturvaan liittyvään yhteistyöhön.

Tietosuojavastaava

- valvoo tietosuojan toteutumista,
- tunnistaa tietosuojaan liittyvät ongelmat ja vie ne tietoturvaryhmän käsiteltäväksi,
- osallistuu alueelliseen tietosuojaan liittyvään yhteistyöhön.

3.2 Tietoturvatyö käytännössä

Tietoturvatyö jakaantuu käytännössä kolmeen osa-alueeseen:

- Tietoturvaryhmä kehittää tietoturvaa teknisesti, huolehtii henkilöstön tietoturvaosaamisesta ja ylläpitää tietoturvaohjeistusta.
- Tietoturva- ja tietosuojavastaavat suorittavat valvontaa ja selvittävät mahdolliset yksittäiset ongelmat ja epäilyt.
- Johtoryhmä tekee tietoturvaan liittyvät päätökset tietoturvaryhmän esitysten perusteella.

Käytännön tietoturvatyö on kuvattu tarkemmin sisäisissä ohjeissa.