Virva Hartonen

TIETOTURVAPOLITIIKKA KÄYTÄNTÖÖN
Suunnitelma sairaanhoitopiirin tietoturvallisuuden kehittämiseen

Opinnäytetyö
Sosiaali- ja terveysalan johtaminen ja kehittäminen
Ylempi ammattikorkeakoulututkinto

Huhtikuu 2013

MIKKELIN AMMATTIKORKEAKOULU
Mikkeli University of Applied Sciences

KUVAILULEHTI

MIKKELIN AMMATTIKORKEAKOULU Mikkeli University of Applied Sciences	**Opinnäytetyön päivämäärä** 23.4.2013
Tekijä(t) Virva Hartonen	**Koulutusohjelma ja suuntautuminen** Sosiaali- ja terveysalan johtaminen ja kehittäminen, ylempi AMK

Nimeke
Tietoturvapolitiikka käytäntöön –suunnitelma sairaanhoitopiirin tietoturvallisuuden kehittämiseen

Tiivistelmä

Tietoturvapolitiikka on organisaation ylimmän johdon kannanotto tietoturvallisuuden ja tietosuojan toteuttamiseen. Tämän kehittämistehtävän tarkoituksena oli jalkauttaa tietoturvapolitiikka sairaanhoitopiirin yksiköihin ja tehdä suunnitelma tietoturvallisuuden ja tietosuojan edistämiselle. Työ on osa sairaanhoitopiirin laajempaa tietoturvallisuuden kehittämisprosessia.

Tavoitteena oli selvittää hoitohenkilöstön tietosuoja- ja tietoturvaosaamista sekä organisaation tietoturvallisuuteen liittyviä keskeisiä kehittämistarpeita. Aineisto kerättiin haastattelemalla hoitotyön lähiesimiehiä, kirjaamalla kehittämistarpeita osastotunneilta ja analysoimalla tietoturvapoikkeamia. Aineiston pohjalta laadittiin tietoturvallisuuden kehittämissuosituksia toimenpide-ehdotuksineen sekä keskeisten kehittämistoimenpiteiden vuosikello vuodelle 2013.

Tietoturvallisuuden kehittämisalueita ovat:
- Tietoturvallisuuteen ja tietosuojaan liittyvä johtaminen
- Tietoturvapoikkeamaraportoinnin kehittäminen
- Tietoturvallisuuteen ja tietosuojaan liittyvä koulutus
- Tietoverkon ja tietojärjestelmien kirjautumisratkaisut
- Potilastietojen käytön seuranta ja valvonta
- Tietosuoja- ja tietoturvaohjeistusten kehittäminen

Kehittämistehtävän tulokset syventävät kuvaa sairaanhoitopiirin tietoturvallisuuden tasosta. Suositusten avulla kehittämistoimenpiteitä voidaan kohdentaa tehokkaammin. Osa suosituksista onkin jo jalkautettu käytännön toiminnaksi.

Asiasanat (avainsanat)

Tietoturva, tietosuoja, tietoturvapolitiikka, terveydenhuolto, hoitohenkilöstö, kehittäminen

Sivumäärä	**Kieli**	**URN**
40 + 1 liite	Suomi	

Huomautus (huomautukset liitteistä)

Ohjaavan opettajan nimi	**Opinnäytetyön toimeksiantaja**
Paula Mäkeläinen	Etelä-Savon sairaanhoitopiiri

DESCRIPTION

MIKKELIN AMMATTIKORKEAKOULU Mikkeli University of Applied Sciences	**Date of the master's thesis** 23.4.2013
Author(s) Virva Hartonen	**Degree programme and option** Masters`s Degree Programme in Development and Leadership in Health care and Social Services

Name of the master's thesis

Implementing the information security policy –a plan to develop hospital district´s information security

Abstract

The information security policy in a statement of the organisation`s management to implement information security and data protection. The purpose of this master´s thesis was to implement data security policy into organisation units and plan methods, which will improve the information security in the future. This thesis was a part of larger development process in hospital district.

In this development process, the nursing personnel´s competence of information security and data protection and essential demands of organisational information security were studied. The data was collected by interviewing the nursing managers, by documenting information from unit meetings and by analysing the information of security threats. Based on the results the recommendations were provided to the organisation.

The information security can be improved by:

- developing management and leadership of information security and data protection
- building up the process of collecting information security threats
- educating personnel
- developing login systems of information networks
- developing monitoring and controlling of medical records use
- clarifying information security and data protection instructions

The results of this master´s thesis support and deepen the image of the information security of the organisation. The recommendations can be utilised in targeting organisation´s activities by developing information security. Some of the recommendations are already implemented in practise.

Subject headings, (keywords)

Information security, data protection, data security policy, implementation, health care

Pages	**Language**	**URN**
40 + appendix	Finnish	

Remarks, notes on appendices

Tutor	**Master's thesis assigned by**
Paula Mäkeläinen	Etelä-Savo Hospital District

SISÄLTÖ

1 JOHDANTO

Terveydenhuolto on suuressa myllerryksessä. Palvelurakenteet, palveluiden sisällöt ja niiden tuottamisessa hyödynnettävät teknologiset ratkaisut muuttuvat. Samalla myös terveydenhuollon asiakkaat ja potilaat odottavat joustavampaa ja entistä laadukkaampaa palvelua. (Aarnio 2013, 7.) Sähköinen potilaskertomus on terveydenhuollon ammattilaisen tärkeimpiä työvälineitä. Sekä erikoissairaanhoidossa että perusterveydenhuollossa sähköisen kertomuksen levinneisyys oli vuonna 2010 100 % ja käyttöaste pääosin yli 90 %. (Winblad ym. 2012, 111─112.) Sähköisten tietojärjestelmien odotetaan parantavan asiakkaiden ja potilaiden hoitoa, kun tiedot ovat välittömästi ammattilaisten saatavilla alkuperäisessä muodossaan.

Tietojärjestelmäkehitys on tuonut mukanaan myös laajoja toimintaprosessien muutoksia. On syntynyt uusia tietoturvallisuuteen ja tietosuojaan liittyviä haasteita sekä tiedonhallinnan että asiakkaiden ja terveydenhuollon henkilöstön näkökulmasta. Kansalliset terveydenhuollon informaatioteknologiahankkeet ja sähköisten potilastietojärjestelmien alueellistaminen ovat nostaneet tietoturvallisuuteen ja tietosuojaan liittyvät asiat kehittämisen kohteiksi sekä lainsäädännöllisellä että toiminnallisella tasolla. Kun potilastieto on entistä laajemmin potilaan hoitoon osallistuvan henkilöstön käytettävissä, se asettaa myös suuremmat vaatimukset tietojen oikeelliselle käsittelylle ja valvonnalle. (Vrt. Kansallinen terveysarkisto 2009; Kansallinen terveysarkisto 2012.)

Tietoturvallisuuden kehittäminen on yksi keskeinen organisaatioiden turvallisuustekijä. Turvallisuussuunnittelu, tietoturvatoiminnan organisointi sekä johdon määrittelemät tietoturvapolitiikka ja periaatteet antavat perustan jatkuvalle kehittämiselle. Ajantasainen ja huolellisesti laadittu tietoturvapolitiikka mahdollistaa tietoturvallisuusasioiden selkeän ja olennaiseen keskittyvän henkilöstöviestinnän ja käytännön toiminnan edistämisen. (Valtionhallinnon tietoturvallisuuden johtoryhmä 2003; Valtionhallinnon tietoturvallisuuden johtoryhmä 2008.)

Koko henkilöstön sitoutuminen tietoturvallisuuden toteuttamiseen on tärkeää. Sitoutumista ei tapahdu, jos käyttäjät eivät ymmärrä mitä tietoturvallisuudella tarkoitetaan eivätkä miellä tietoturvallisuutta tärkeäksi osaksi omaa työtään. (Valtionhallinnon tietoturvallisuuden johtoryhmä 2003.) Tietoturvapolitiikan jalkauttaminen on edellytys organisaation tietoturvallisuuden kokonaisvaltaiselle kehittämiselle. Organisaation

ylimmän johdon asettamat tietoturvaperiaatteet ja tietoturvallisuutta edistävät toimintamallit istutetaan osaksi henkilöstön päivittäistä toimintaa. Jalkauttamisessa on pitkälti kyse tietoturvallisuuskulttuurin ja asenteiden muuttamisesta sekä osaamisen kehittämisestä. (Valtionhallinnon tietoturvallisuuden johtoryhmä 2008.)

Tietoturvallisuuden kehittämiselle antoi vahvan sysäyksen Etelä-Savon sairaanhoitopiirissä keväällä 2012 käyttöönotettu sähköinen lääkemääräys. Ajantasainen tietoturvapolitiikka sekä tietoturva- ja tietosuojakäytäntöjen päivittäminen olivat lääkemääräyksen käyttöönoton edellytyksiä. Myös terveydenhuoltolain mukaisen yhteisen potilastietokannan (ns. ESTER-kanta) käyttöönotto Etelä-Savon sairaanhoitopiirin alueella vauhditti omalta osaltaan tietoturvan kehittämistä.

Tietoturvapolitiikan jalkauttaminen tapahtui sairaanhoitopiirissä organisaation johdon ja tietoturvatyöryhmän aloitteesta. Käytännön organisointivastuu annettiin pitkälti tietokoordinaattorille eli minulle ja toimeksianto oli lähtökohta tämän kehittämistehtävän toteutukselle.

2 TIETOSUOJA JA TIETOTURVA TERVEYDENHUOLLOSSA

2.1 Tietosuojan merkitys luottamuksellisessa hoitosuhteessa

Tietojen suojaaminen on tärkeä osa terveydenhuollon toimintaa. Vaikka viranomaisten toiminta on periaatteessa julkista, terveydenhuollossa käsitellään usein salaista tai arkaluonteista tietoa, joka on suojattava asianmukaisesti. Toisaalta on välttämätöntä, että tiedot ovat tarvittaessa viranomaisten saatavilla oikeellisessa muodossa. (Vrt. Tammisalo 2005.)

Terveydenhuollossa potilastietojen salassapito on oleellinen osa hoitosuhteen luottamuksellisuutta. Salassapitovelvollisuuteen kuuluvat salaisiksi säädettyjen asiakirjojen salassapito (asiakirjasalaisuus), vaitiolo salassa pidettävistä seikoista esimerkiksi hoitosuhteessa (vaitiolovelvollisuus) ja salassa pidettävien tietojen hyväksikäyttökielto. (Andreasson ym. 2013, 22; Kotisaari & Kukkola 2012, 121.)

Tietosuojalla tarkoitetaan henkilötietojen suojaamista ja turvallista käsittelyä siten, ettei henkilöiden yksityisyyden suojaa tai oikeusturvaa vaaranneta. Tietosuojan ensisi-

jainen tarkoitus ei ole tietojen konkreettinen suojaaminen vaan asiakkaan ja potilaan yksityisyyden, itsemääräämisoikeuden, minäkuvan ja sosiaalisten suhteiden sekä luottamuksellisen hoitosuhteen suojaaminen. (Andreasson ym. 2013, 14; Kelan KanTa-palvelujen tietoturvapolitiikka 2011, 8; Ylipartanen 2010, 21─23.)

Tietosuojan tarkoituksena on henkilötietojen hyvän käsittelytavan luominen kaikissa tietojen käsittelyn vaiheissa sekä rekisteröityjen ja rekisterinpitäjien oikeusturvan varmistaminen. Näin ollen jokaisen terveydenhuollossa työskentelevän tulee tuntea keskeiset potilastietojen käsittelyä koskevat lait ja periaatteet. (Andreasson ym. 2013, 14; Ylipartanen 2010, 23─24.)

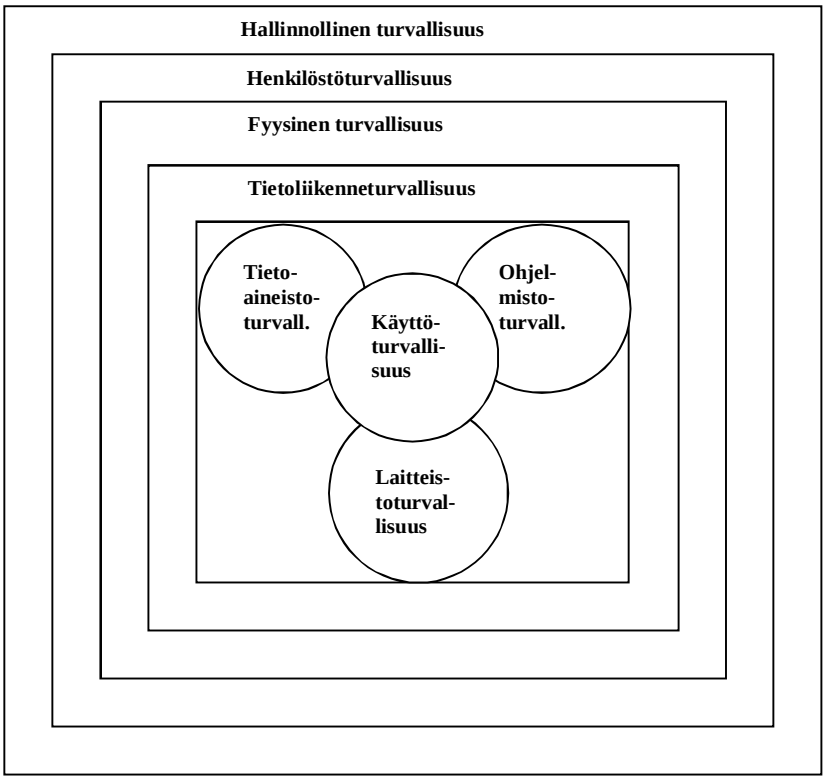
Potilastietojen käsittelystä ja säilytyksestä, käsittely- ja säilytystapojen turvallisuudesta ja käytettävien tietojen suojaamisesta säädetään useassa laissa ja asetuksessa. Potilas- ja asiakastietojen käsittelyyn vaikuttavat terveydenhuollon lainsäädännön lisäksi mm. henkilötietolaki (523/1999), laki ja asetus viranomaisen toiminnan julkisuudesta (621/1999) sekä arkistolaki (831/1994).

Potilaan hoitoon liittyvien potilasasiakirjojen ja potilastietojen asianmukainen käsittely toteutetaan toimintaprosessien määrittelyn avulla. Määrittelyssä suunnitellaan toiminnan tarpeet ja niihin liittyvien henkilötietojen käsittely sekä varmistetaan lainmukaisuus ja potilaan oikeuksien toteutuminen. Potilastietojen käsittelyyn liittyvät tietosuoja- ja muut riskit on kartoitettava. Potilasasiakirjat on säilytettävä siten, että hoidon järjestämiseen ja toteuttamiseen osallistuvat toimijat voivat käyttää potilastietoja ainoastaan niihin käyttötarkoituksiin, joihin ne on tarkoitettu. (Sosiaali- ja terveysalan lupa- ja valvontavirasto 2012; Tammisalo 2005.)

2.2 Tietoturvallisuus ja sen osa-alueet

Tietoturvallisuus on perusta hyvälle hallinto- ja tiedonhallintatavalle. Se on myös yksi organisaation laatutekijä. Tietoturvallisuuden ylläpito ja kehittäminen edellyttää johdon sitoutumista. Johdon on myös turvattava tarvittavat resurssit tietoturvallisen toiminnan toteuttamiseen. Avoimen ja läpinäkyvän johtamisen avulla henkilöstö on mahdollista saada mukaan aktiiviseen tietoturvatyön kehittämiseen. (Valtiovarainministeriö 2007, 15.)

Tietoturvallisuudella tarkoitetaan tietojen, järjestelmien, palvelujen ja tietoliikenteen asianmukaista suojaamista hallinnollisilla, teknisillä ja muilla toimenpiteillä. Tietoturva muodostuu käytännön toimenpiteistä, joiden tarkoituksena on varmistaa tiedon saatavuus, eheys ja käytettävyys sekä tietojen salassapito ja tietojen rajatut käyttöoikeudet. Tietoja turvataan laitteisto- ja ohjelmistovikojen, luonnontapahtumien sekä tahallisten, tuottamuksellisten tai tapaturmaisten tekojen aiheuttamilta uhilta ja vahingoilta. (Kelan KanTa-palvelujen tietoturvapolitiikka 2011, 8; Valtiovarainministeriö 2007, 7, 13.)



KUVIO 1. Tietoturvallisuuden osa-alueet (Jokinen 1999, 178.)

Tietoturvallisuus voidaan jakaa osa-alueisiin, joilla helpotetaan tietoturvatyön suunnittelua, toteutusta ja valvontaa. Yllä on kuvattu jaottelu, jota käytetään yleisesti terveydenhuollossa sekä mm. valtion ja kuntien tietoturvallisuuden osa-alueiden kuvaamisessa (Kuvio 1).

2.2.1 Hallinnollinen turvallisuus

Hallinnollinen tietoturvallisuus on kaikkien muiden tietoturvallisuuden osa-alueiden perusta. Sen avulla määritellään tietoturvallisuuden suuntaviivat ja turvallisuutta pa-

rantavat toimenpiteet. Hallinnollisella tietoturvallisuudella tarkoitetaan tietoturvan johtamiseen sekä toimintojen organisointiin liittyvää kokonaisuutta, joka muodostuu tietoturvallisuustoiminnan järjestelyjen, henkilöstön tehtävien ja vastuiden sekä ohjeistuksen, koulutuksen ja valvonnan määrittelystä. Sen tarkoituksena on luoda organisaatioon tietoturvastrategia ja istuttaa tietoturvalliset toimintamallit osaksi kaikkea toimintaa. Toimintamallien pohjalta luodut henkilöstön koulutusjärjestelyt sekä ohjeistus-, valvonta- ja tarkastusmenettelyt ovat välttämättömiä tietoturvallisuuden kehittämiseksi ja ylläpitämiseksi. Tietoturvan kehittäminen ja ylläpito ovat puolestaan osa organisaation yleistä turvallisuustoimintaa, riskien hallintaa ja sisäistä valvontaa. (Kelan KanTa-palvelujen tietoturvapolitiikka 2011, 9; Sosiaali- ja terveysministeriö 2010, 12.)

Hallinnollisessa tietoturvassa päämääränä on luoda organisaatioon toimintatapa, jolla pystytään välttämään tietoturvariskit. Tietoturvariskejä hallitaan erikseen määriteltävän riskienhallintaprosessin avulla. Organisaation johto määrittelee hyväksyttävän riskitason riskianalyysin tulosten perusteella ja yhteisesti valmisteltujen kriteeristöjen ja mittarien avulla. (Sosiaali- ja terveysministeriö 2010, 12.)

Hallinnollisessa tietoturvallisuudessa on oleellista, että työntekijät tietävät ja ymmärtävät ne periaatteet, joille organisaation tietoturvallisuus rakentuu. Tähän päästään aktiivisella, ongelmiin puuttuvalla ja hyvää tietoturvakäytäntöä edistävällä tietoturvan johtamisella. (Kulppi & Lohi 2011.)

2.2.2 Henkilöstöturvallisuus

Henkilöstö on keskeisessä roolissa terveydenhuollon tietoturvallisen toiminnan toteuttamisessa. Henkilöstöturvallisuuden perustana on osaava ja sitoutunut henkilökunta, jonka tietoturvallisuuteen liittyvät vastuut ja velvollisuudet on määritelty tehtäväkuvissa. Henkilöstöturvallisuus on henkilöstöön liittyvien riskien hallintaa, jossa tarkastellaan teknologian, organisaation, ihmisen, työtehtävän ja työympäristön välisiä yhteyksiä. Henkilöstö ja siitä aiheutuvat tietoturvariskit voivat uhata tietojen eheyttä, luottamuksellisuutta ja käytettävyyttä. Henkilöstöturvallisuuden arvioinnissa tulee määritellä mm. soveltuvuus ja toimenkuvat, sijaisjärjestelyt, tiedonsaanti- ja käyttöoikeudet, suojaaminen, koulutus ja tietojen käytön valvonta. (Valtiovarainministeriö 2007, 57─58; Valtiovarainministeriö 2008.)

Henkilöstöturvallisuuden perustaso edellyttää ohjeistusta esimiesten ja työntekijöiden vastuista, velvollisuuksista ja oikeuksista. Henkilöstölle järjestetään tietoturvakoulutusta säännöllisesti ja se on pakollinen kaikille, jotka käyttävät luottamuksellisia tietoja sisältäviä tietojärjestelmiä tai käsittelevät muilla tavoin luottamuksellista tietoa työssään. Uusille työntekijöille annetaan käyttäjätunnukset aluksi määräajaksi, jonka kuluessa työntekijän on osallistuttava tietoturvakoulutukseen. Kaikkiin tarpeellisiin tietojenkäsittelytehtäviin on nimetty vastuu- ja varahenkilöt ja vaaralliset työyhdistelmät on eliminoitu. Henkilöstön tulee noudattaa annettuja tietoturvaohjeita ja -käytäntöjä. Ohjeiden noudattamista valvotaan suunnitelmallisesti ja tietosuojarikkomukset käsitellään tietoturvatyöryhmässä. Väärinkäytösten varalle on laadittu sanktiojärjestelmä, joka on kaikkien tiedossa ja jota noudatetaan. (Sosiaali- ja terveysministeriö 2010, 18.)

Noin puolet kaikista tietoturvarikkomuksista liittyy organisaation menettelytapoihin, ei yksinomaan henkilöstön aiheuttamiin tietoturvauhkiin. Keskeistä onkin suunnitelmallinen henkilöstön kehittäminen, johtaminen ja henkilöstöhallinto. Suunnitelmallisella tietoturvallisuustyöllä vähennetään henkilöstön aiheuttamaa tuottamuksellista tietoturvauhkaa muun muassa ohjeistamalla ja kouluttamalla henkilöstöä sekä kehittämällä työmenetelmiä ja työprosesseja. (Valtionvarainministeriö 2007, 57; Valtiovarainministeriö 2008.) Aktiivisella johtamisella voidaan vaikuttaa työyhteisön tietoturvakulttuuriin ja -asenteisiin (Kulppi & Lohi 2011).

2.2.3 Fyysinen turvallisuus

Fyysisen turvallisuuden tarkoituksena on turvata organisaation häiriötön toiminta. Tähän osa-alueeseen kuuluvat muun muassa kamera- ja kulunvalvonta, vartiointi, palo-, vesi- ja sähkö-, ilmastointi- sekä murtovahinkojen torjunta. Toimenpiteiden avulla varmistetaan teknisten järjestelmien toiminta ja suojataan kiinteistö- ja erikoistiloja luvattomia tai rikollisia toimia, onnettomuuksia ja luonnontuhoja vastaan. Fyysinen turvallisuus on kokonaisuus, joka sisältää rakenteellisen turvallisuuden, valvonnan ja valvontatekniikan sekä vartioinnin. Näillä toimilla estetään mm. tietojen joutuminen luvattomiin käsiin. Fyysisten tilojen suunnittelussa tulee ottaa huomioon tietosuoja-, tietoturva- ja työturvallisuusnäkökohdat. Henkilöstön näkökulmasta fyysistä turvallisuutta on mm. henkilökohtaisen työhuoneen lukitseminen huoneen jäädessä tyhjäksi ja

ymmärrys siitä, miten vaaratilanteissa tulee toimia. (Sosiaali- ja terveysministeriö 2010, 17; Valtiovarainministeriö 2007, 59.)

2.2.4 Tietoliikenneturvallisuus

Tietoliikenneturvallisuus käsittää tiedonsiirtoyhteyksien käytettävyyteen, tiedonsiirron suojaamiseen ja salaamiseen, käyttäjien tunnistamiseen ja tietoverkon varmistamiseen liittyvät turvallisuustoimenpiteet. Toimenpiteitä ovat mm. tietoverkkojen dokumentointi ja niiden suunnitelmallinen laajennus, käyttöoikeuksien hallinnointi ja varmistaminen, tietoliikennelokin ja käyttöhäiriöiden säännöllinen seuranta, ohjelmien ja laitteiden turvallisuuden sekä tietoliikenneviestien sisällön muuttumattomuuden todentaminen. (Sosiaali- ja terveysministeriö 2010, 17; Valtiovarainministeriö 2007, 61.)

2.2.5 Tietoaineistoturvallisuus

Tietoaineistoturvallisuudella tarkoitetaan tietojen ja tietoaineistojen käytettävyyttä, oikeellisuutta, turvallista käsittelyä, salassa pitämistä sekä turvallista ja säädöstenmukaista säilyttämistä ja hävittämistä. Tietoaineistoturvallisuutta ja tietosisällön perusteella tehtävää tietojenkäsittelyä määrittelevät, rajoittavat ja ohjaavat yleiset ja terveydenhuollon lait, asetukset, viranomaismääräykset ja ohjeet. Tietoaineistotuvallisuuteen kuuluvat myös tietojärjestelmien käsittelysäännöt sekä tietojen ja asiakirjojen luokittelu julkisuus- ja salassapitosäännösten mukaisesti. (Sosiaali- ja terveysministeriö 2010, 13; Valtiovarainministeriö 2007, 55.)

Kaikkia terveydenhuollon ammattihenkilöitä koskee vaitiolovelvollisuus ja salassapitosäännökset. Luottamuksellisia tietoja voivat käsitellä vain henkilöt, jotka tarvitsevat niitä työssään, eikä niitä luovuteta ulkopuolisille. Sivullisille ei saa antaa tietoja ilman potilaan kirjallista suostumusta. Sivullisella tarkoitetaan muita kuin asianomaisessa toimintayksikössä tai sen toimeksiannosta potilaan hoitoon tai siihen liittyviin tehtäviin osallistuvia henkilöitä. Tiedon luovutuksen organisaation ulkopuolelle tulee perustua lakeihin ja pääsääntöisesti potilaan suostumukseen. Tietoja säilytetään ja vanhentuneet tiedot hävitetään arkistonmuodostussuunnitelman mukaisesti. (Sosiaali- ja terveysministeriö 2010, 14.)

Henkilöstön tulee tuntea terveydenhuollon henkilötietojen käsittelyä koskevat yleiset periaatteet ja oman organisaation toimintaa ohjaavat säännöt ja ohjeet, tietojärjestelmien sisältämän tietoaineiston käsittelyä koskevat turvaohjeet ja -säännöt sekä tietojen ja asiakirjojen luokittelu ja noudattaa niitä toiminnassaan (Sosiaali- ja terveysministeriö 2010, 14).

2.2.6 Käyttöturvallisuus

Käyttöturvallisuudella luodaan ja ylläpidetään olosuhteita, jolla varmistetaan tietotekнologian turvallinen käyttö. Käyttöturvallisuudella huolehditaan tekniikan toimivuuden valvonnasta, käyttöoikeuksista, käytön ja lokien valvonnasta, ohjelmistotukeen, ylläpito-, kehittämis- ja huoltotoimintoihin liittyvistä turvallisuustoimenpiteistä sekä tietojen varmistamisesta ja häiriötilanteiden raportoinnista. Henkilöstön osalta tämä tarkoittaa mm. tietojärjestelmiä käyttävien työntekijöiden tunnistamista ja todentamista ohjeistusten mukaisesti, käytössä olevia käyttäjätunnus-, salasana-, toimikortti- ja PIN-koodimenettelyjä, tietokonevirusten ja haittaohjelmien torjuntaohjeita sekä suojausten riittävyyden varmistamista ja käytönvalvontaa väärinkäytösten varalta. (Sosiaali- ja terveysministeriö 2010, 14─16; Valtiovarainministeriö 2007, 65.)

2.2.7 Ohjelmistoturvallisuus

Ohjelmistoturvallisuuden tavoitteena on varmistaa tietojärjestelmien jatkuva toiminta ja luotettavuus. Sillä tarkoitetaan käyttöjärjestelmien, ohjelmistojen ja sovellusten suojausominaisuuksia, valvonta- ja lokimenettelyjä sekä ohjelmistojen määrittelyyn, suunnitteluun, kehittämiseen ja hankintaan sekä ylläpitoon ja päivitykseen liittyviä turvallisuustoimenpiteitä. Ohjelmistoturvallisuuden periaatteita ovat mm. saatavuus, käytettävyys, luottamuksellisuus, eheys ja yhteensopivuus sekä saatavuuden turva. (Sosiaali- ja terveysministeriö 2010, 12─14.)

Tietojärjestelmien ylläpidosta huolehditaan organisaatiossa ohjelmistotoimittajien kanssa tehdyillä ylläpitosopimuksilla. Henkilöstön tulee tuntea organisaation ohjelmistoturvallisuuteen liittyvät toimintaperiaatteet, kuten tietohallintoon keskitetty ohjelmien asentaminen ja hankinta. Tietohallinto hyväksyy kaikki työasemille asennettavat ohjelmat. Henkilöstön tulee säilyttää mahdolliset hallussaan olevat ohjelmien asennuslevyt, samoin kuin niiden kopiot tietoturvaohjeiden mukaisesti. Työasemien

käyttäjät vastaavat omien työhön liittyvien tiedostojensa varmistamisesta. Muiden kuin työhön liittyvien tiedostojen tallentaminen tietoverkkoon on kielletty. (Sosiaali- ja terveysministeriö 2010, 12─14.)

2.2.8 Laitteistoturvallisuus

Laitteistoturvallisuus liittyy erilaisten laitteistojen käytettävyyteen, toimintaan, ylläpitoon sekä saatavuuteen. Turvatoimenpiteet kohdistuvat tietoteknisten ja tutkimuslaitteistojen ja tietoverkon rakenteeseen, ohjelmiin, käyttöjärjestelmiin, huoltoon, keskitettyyn operointiin, varmistuksiin sekä pääsynsuojaukseen. Laitteistoturvallisuuden perustaso edellyttää, että tietoverkot, tietotekniset ja tutkimuslaitteistot on dokumentoitu toipumissuunnitelmaan ja varajärjestelmien käytettävyys poikkeusoloissa on varmistettu. Lisäksi perustaso edellyttää, että laitteistojen fyysisen kunnon tarkistamiseksi on laadittu ohjeet ja niitä noudatetaan. Myös huolto- ja ylläpitosopimusten tulee olla ajan tasalla ja vastata käytettävyysvaatimuksia. (Sosiaali- ja terveysministeriö 2010, 16; Valtiovarainministeriö 2007, 63.)

2.3 Tietoturvapolitiikka käytännön toiminnaksi

Tietoturvapolitiikka on johdon linjaus organisaation tietoturvallisuuden ja tietosuojan toteuttamiseen. Se kertoo organisaation tietojenkäsittelyn eri osa-alueiden lainmukaisen turvaamisen tavoitteet, periaatteet ja käytännön toimenpiteet. Organisaation johto osoittaa politiikalla sitoutumisensa tietoturvatoiminnan ylläpitoon ja kehittämiseen sekä sovittujen periaatteiden ja käytäntöjen noudattamiseen. Tietoturvallisuuden merkityksen ja periaatteiden dokumentointi ja niiden viestintä koko henkilöstölle on keskeinen osa organisaation tietoturvakulttuurin luomista. (Tammisalo 2005; Valtiovarainministeriö 2007, 25.)

Tietoturvapolitiikka kertoo organisaation kanssa asioiville, että se panostaa tietoturvallisuuden ylläpitoon ja kehittämiseen. Politiikka antaa osaltaan luotettavan kuvan organisaation toiminnasta. Terveydenhuollossa henkilötietojen, kuten potilastietojen, käsittely on tarkoituksenmukaista kuvata tietoturvapolitiikassa. Tällöin voidaan todentaa jokaiselle, jonka henkilötietoja organisaatiossa käsitellään ja säilytetään, että tietoja käsitellään turvallisesti, luottamuksellisesti ja hyvien tietojenkäsittelytapojen mukaisesti. (Tammisalo 2005.)

Tietoturvapolitiikka määrittää tietoturvallisuuden vähimmäistason ja ohjaa kaikkea tietoturvallisuuteen liittyvää toimintaa niin henkilöstön, hallinnon kuin teknisestäkin näkökulmasta. Tietoturvallisen toiminnan lähtökohta on, että kaikki ymmärtävät oman merkityksensä ja tehtävänsä tietoturvallisuuden ylläpidossa. Tätä varten tietoturvapolitiikassa on määritelty tietoturvatehtävät, tietoturvatyön organisointi ja eri toimijoiden roolit organisaation kaikilla tasoilla. (Sosiaali- ja terveysministeriö 2010.)

Tietoturvapolitiikan jalkauttamisessa on kyse organisaation tietoturvallisuustason kehittämisestä, jolloin politiikan tulee olla koko organisaation tiedossa. Keskeistä tietoturvallisuuden kehittämisessä on johdonmukainen jalkautussuunnitelma henkilöstö- ja johtotasolle sekä selkeät toimintaohjeet potilastietojen lainmukaisesta käsittelystä ja tietoturvarikkomusten sanktioista. (Ensio & Reponen 2005, 48─50; Reponen 2006, 72.)

Tietoisuutta ja ymmärrystä tietoturva-asioista voidaan lisätä organisaatiotasolla mm. selvittämällä, miten eri tiedotuskanavat saavuttavat henkilöstön ja varmistamalla sekä johdon että henkilöstön sitoutuminen tietoturvallisiin toimintatapoihin. Tietoturvatietoisuutta lisätään lisäksi tarkistamalla, yhdenmukaistamalla ja julkituomalla tietoturvarikkomusten sanktiojärjestelmä organisaatiotasolla. (Ensio & Reponen 2005, 48─50; Reponen 2006, 72; Tammisalo 2005.)

Keskeisimpiä kehittämiseen liittyviä toimenpiteitä ovat käyttäjien oikea ja riittävä ohjeistus sekä koulutus. Näiden avulla voidaan nostaa tietoturvatietämyksen tasoa organisaatiossa, herättää henkilöstö miettimään tietoturvaa omassa työssään ja sitä kautta luoda sitoutumista organisaation turvalliseen toimintaan. (Ensio & Reponen 2005, 48─50; Valtionhallinnon tietoturvallisuuden johtoryhmä 2003.)

Näkemykseni mukaan tietoturvallisuuden kehittämisen ei tule kuitenkaan pysähtyä tietoturvapolitiikan jalkauttamiseen, vaan organisaation tulee pyrkiä jatkuvaan kehittämiseen. Näin ollen tietoturvapolitiikan juurruttaminen voidaan nähdä jatkuvana prosessina, jossa politiikkaan tehdyt muutokset sekä kehityskohteet implementoidaan organisaatioon ja organisaatiosta tulevat muutostarpeet puolestaan ohjaavat tietoturvapolitiikan päivittämistä. (Vrt. Kairamo 2008.)

Etelä-Savon sairaanhoitopiirin tietoturvapolitiikka on tehty sairaanhoitopiirin johdossa ja sen on hyväksynyt sairaanhoitopiirin hallitus. Tietoturvapolitiikka on käsitelty myös sairaanhoitopiirin yhteistyötoimikunnassa. Johdolla on viimekädessä vastuu politiikan toteutumisen seurannasta. Vaikka johto on sitoutunut tietoturvapolitiikan toteuttamiseen, linjaukset vaativat avaamista, soveltamista ja koulutusta, ennen kuin niiden voidaan olettaa juurtuvan käytännön toiminnaksi kaikilla organisaation tasoilla. Muutoksen eteenpäin viemisessä lähiesimiehillä on keskeinen rooli. Lähiesimiehet toimivat henkilöstön keskustelun herättäjinä, asenteiden muokkaajina ja viime kädessä myös tietoturvallisen toiminnan käytännön valvojina ja ohjeistajina. Kun esimies toimii aktiivisesti tietoturvaan liittyvissä kysymyksissä, johtaminen on näkyvää ja mahdollisiin ongelmiin puututaan ajoissa, henkilöstö luottaa organisaation tietoturvan kehittämiseen ja sitoutuu myös omassa toiminnassaan siihen tehokkaammin (Kulppi & Lohi 2011). Tietoturvallisuuden sitominen laajempiin käytännön kokonaisuuksiin antaa opittaville asioille syvällisemmän ja vaikuttavamman merkityksen (Nykänen 2011, 275).

3 KEHITTÄMISTEHTÄVÄN TARKOITUS JA TAVOITTEET

Tämän kehittämistehtävän lähtökohtana oli Etelä-Savon sairaanhoitopiirissä alkuvuodesta 2012 käyttöönotettu tietoturvapolitiikka. Se linjaa organisaation tietoturvallisuuden vähimmäistason ja ohjaa tietoturvallisuuteen liittyvää toimintaa niin henkilöstön, hallinnon kuin teknisestäkin näkökulmasta. Politiikka määrittää tietoturvallisuuden perusperiaatteet, toimintamallit, organisoinnin ja vastuut. (Etelä-Savon sairaanhoitopiirin tietoturvapolitiikka 2012.)

Kehittämistehtävän tarkoituksena oli jalkauttaa tietoturvapolitiikka Etelä-Savon sairaanhoitopiirin yksiköihin ja tehdä suunnitelma tietoturvallisuuden ja tietosuojan jatkuvalle seurannalle ja kehittämiselle.

Tavoitteena oli

- selvittää hoitohenkilöstön tietosuoja- ja tietoturvaosaamisen taso
- selvittää tietoturvallisuuteen ja tietosuojaan liittyvät keskeiset kehittämistarpeet
- laatia suosituksia tietoturvallisuuden ja tietosuojan seuraamiseksi ja kehittämiseksi

- suunnitella tietoturvallisuuden seuranta- ja kehittämismenetelmiä, jotka ovat käytettävissä sekä hoitohenkilöstön että muiden henkilöstöryhmien tarpeisiin
- laatia viitteellinen aikataulu keskeisten kehittämistarpeiden toteutukselle.

4 KEHITTÄMISTEHTÄVÄN TOTEUTUS

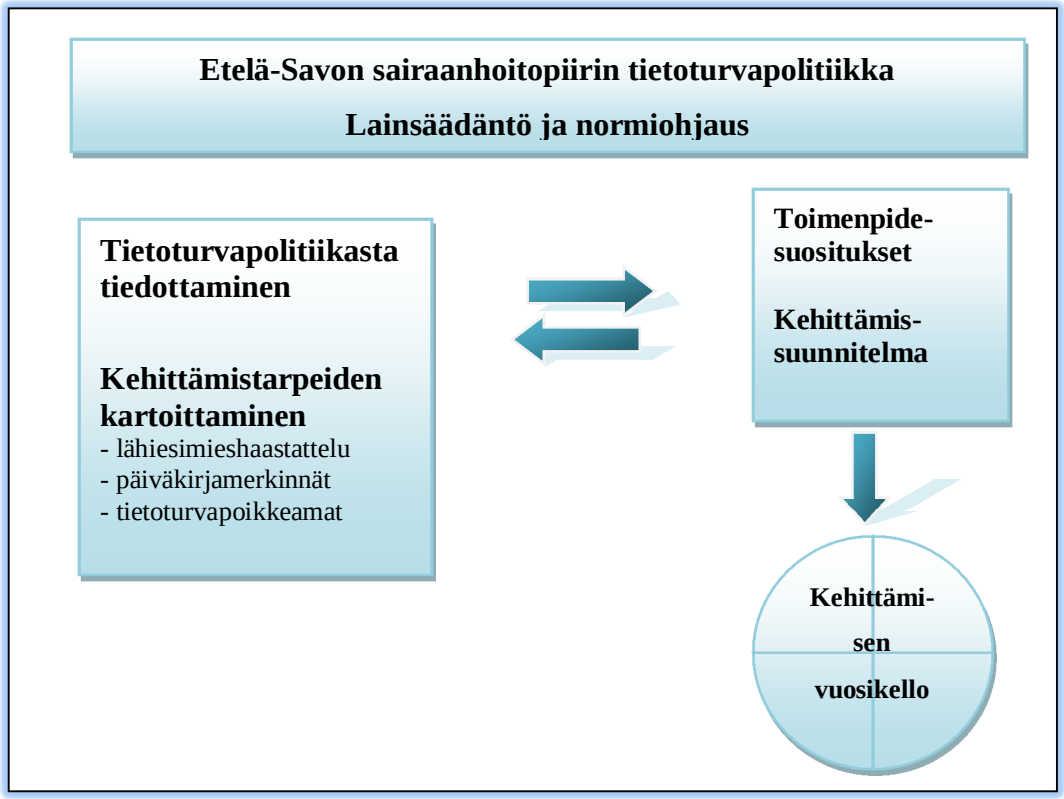
4.1 Kehittämisen viitekehys, kohderyhmä ja organisointi

Kehittämistehtävän toimeksiantaja oli Etelä-Savon sairaanhoitopiirin kuntayhtymä. Toimeksianto liittyi Etelä-Savon sairaanhoitopiirissä käynnissä olevaan, koko organisaatiota koskevaan tietoturvallisuuden kehittämistyöhön, jonka tarkoituksena on tuoda tietoturvallisuus ja tietosuoja kiinteäksi osaksi käytännön toimintaa. Tietoturvallisuuden seurantaa ja kehittämistä koordinoi tietoturvapolitiikan määrittelyn mukaisesti tietoturvatyöryhmä. Tietoturvatyöryhmän jäseniä ovat johtajaylilääkäri, sairaalajohtaja, hallintoylihoitaja, tietopalvelupäällikkö, turvallisuuspäällikkö, tietojärjestelmäsuunnittelija sekä arkistotoimesta vastaava tietopalvelusihteeri ja tietokoordinaattori, joka toimii myös tietosuojavastaavan tehtävissä.

Tietoturvapolitiikan jalkauttaminen tapahtui organisaation johdon ja tietoturvatyöryhmän toimesta. Käytännön organisointivastuu annettiin pitkälti tietokoordinaattorille eli minulle. Tämä kehittämistehtävä on osa jalkauttamistyötä. Ohjausryhmän muodostivat tietoturvatyöryhmän jäsenet. Toimeksiantajan edustajana ja työelämäohjaajana toimivat turvallisuuspäällikkö ja hallintoylihoitaja.

Sairaanhoitopiirissä työskentelee vakinaisessa tehtävässä yli 1200 henkilöä. Kehittämistehtävän pääkohderyhmäksi ja pilotiksi tietoturvatyöryhmä valitsi hoitohenkilöstön, joka on sairaanhoitopiirin suurin henkilöstöryhmä. Hoitohenkilöstö on keskeisessä roolissa potilaiden hoitoon liittyvän tietoturvallisen toiminnan toteuttamisessa ja kehittämisessä. Hoitotyön johtaminen on sairaanhoitopiirissä varsin hyvin organisoitua, joten voitiin olettaa, että lähiesimiehet tuntevat omien yksikköjensä tietoturvallisuuteen liittyvät tarpeet. Näin ollen hoitotyön lähiesimiehet toimivat informantteina aineistonkeruuvaiheessa. Koska pääkohderyhmänä oli hoitohenkilöstö, luvan opinnäytetyön toteuttamiseen antoi Etelä-Savon sairaanhoitopiirin hallintoylihoitaja.

Kehittämisprosessin lähtökohtana oli Etelä-Savon sairaanhoitopiirin tietoturvapolitiikka sekä sitä ohjaava lainsäädäntö ja normit. Aluksi tietoturvapolitiikasta tiedotettiin koko henkilöstölle muun muassa intranetissa, henkilöstölehdessä ja osastokokouksissa, minkä jälkeen kartoitin tietoturvallisuuteen ja tietosuojaan liittyviä kehittämistarpeita eri aineistonkeruumenetelmien avulla. Kartoitusten pohjalta laadin kehittämissuosituksia, jotka hyväksyttiin ja joiden edistämiseen sitouduttiin tietoturvatyöryhmässä. Lisäksi kuvasin ohjeellisen kehittämistoimenpiteiden toteutussuunnitelman aikatauluineen vuosikellossa vuodelle 2013. (Kuvio 2.)



KUVIO 2. Kehittämistehtävän viitekehys

Kehittämisprosessi toteutettiin kokonaisuudessaan lokakuun 2011 ja joulukuun 2012 välisenä aikana (LIITE 1).

4.2 Tietoturvapolitiikan esittely hoitohenkilöstölle

Tietoturvapolitiikan jalkauttaminen aloitettiin hoitohenkilöstöstä. Syksystä 2011 alkaen järjestin Etelä-Savon sairaanhoitopiirin tietosuojavastaavan roolissa tietoturvallisuuteen ja tietosuojaan liittyviä osastotunteja ja työpaikkakokouksia, joissa luennon

lisäksi keskusteltiin ajankohtaisista kysymyksistä ja kehittämistarpeista. Lisäksi tietoturva- ja tietosuoja-asioista uutisoitiin monipuolisesti mm. sairaanhoitopiirin intranetissä sekä koulutus- ja perehdytystilaisuuksissa. Tietoturvapolitiikan sisällöt integroitiin myös muihin kehittämisprojekteihin, kuten yhteisen potilastietojärjestelmän ja eResepti-koulutuksiin yhteistyössä tietohallintopalveluiden kouluttajien kanssa.

4.3 Kehittämistarpeiden kartoittaminen

4.3.1 Aineiston hankinta

Tietoturvallisuuden ja tietosuojan nykytilan ja kehittämistarpeiden kokonaiskuvan muodostamiseksi keräsin aineistoa kolmella eri menetelmällä. Menetelminä käytin osastonhoitajien haastattelua, osastotunneilla ja työpaikkakokouksissa pidettyä päiväkirjaa sekä tietoturvapoikkeamaraporttien analyysiä.

Haastatteluun osallistuminen oli vapaaehtoista. Tulokset raportoin siten, ettei yksittäisiä vastauksia tai dokumenttien sisältöjä voi tunnistaa. Haastattelu- ja päiväkirja-aineistot tuhottiin kehittämistehtävän valmistuttua.

Lähiesimiesten haastattelu

Lähiesimiehet ovat vastuussa tietoturvallisuuden jalkauttamisesta ja kehittämisestä omaan yksikkönsä osalta. Työyksikkötason osaamista ja kehittämistarpeita kartoitin haastattelemalla lähiesimiehinä toimivia osastonhoitajia puolistrukturoidun haastattelulomakkeen avulla. Hirsjärvi ja Hurme (2004, 47) toteavat, että puolistrukturoidussa haastattelussa suurin osa kysymyksistä on määrämuotoisia, mutta lomakkeella on myös joko kokonaan avoimia tai sekamuotoisia kysymyksiä. Puolistrukturoidussa haastattelussa kaikille haastateltaville voidaan esittää samat tai lähes samat kysymykset samassa järjestyksessä, mutta haastateltavat voivat vastata niihin omin sanoin. Joidenkin näkemysten mukaan osittain strukturoitu ja osittain avoin haastattelu sijoittuu strukturoidun lomakehaastattelun ja teemahaastattelun välille.

Aineistonkeruumenetelmänä puolistrukturoitu haastattelu tuo joustavuutta: tiettyihin kysymyksiin saadaan yksiselitteiset vastaukset, mutta avoimet kysymykset ja haastattelutilanne antavat tilaa täsmennyksille, laajemmalle pohdinnalle ja asioille, joita ei

suunnitteluvaiheessa vielä täsmällisesti osaa ajatella (Tilastokeskus 2006). Varasin haastattelulomakkeelle erillisiä avoimia sarakkeita haastattelusta nousevia kommentteja varten.

Haastattelun kohderyhmän muodostivat Etelä-Savon sairaanhoitopiirin osastonhoitajat, jotka toimivat haastatteluhetkellä hoitotyön lähiesimiehinä. Koska kehittämisen näkökulmana oli pääsääntöisesti potilastyöhön liittyvä tietoturva ja tietosuoja, rajasin haastattelun ulkopuolelle ne osastonhoitajat, jotka eivät johda välitöntä potilastyötä tekeviä yksiköitä. Lisäksi ulkopuolelle rajautui muilla ammattinimikkeillä toimivia lähiesimiehiä erityistyöntekijäryhmistä. Otos oli kokonaisotanta. Yksi osastonhoitaja ei osallistunut haastatteluun, joten lopullinen otos oli 22 henkilöä (N = 22).

Kokosin haastattelulomakkeen tämän raportin teoriaosan, lähdekirjallisuuden sekä Etelä-Savon sairaanhoitopiirin tietoturvapoikkeamien seurantatuloksista aiemmin nousseiden kysymysten pohjalta. Jaottelin kysymykset teemoittain. Teemoja olivat seuraavat alueet: taustatiedot, tietoturvallisuus ja tietosuoja esimiestyössä, hallinnollinen tietoturvallisuus, potilastietojen käsittely, tietojärjestelmien käyttö ja käyttäjätunnukset, osaaminen ja koulutus, tietoturvallisuuden häiriö- ja poikkeustilanteet sekä tietoturvallisuuden kehittäminen.

Lomake sisälsi monivalinta- ja sekamuotoisia kysymyksiä, Likert-asteikolla toteutettuja kysymyksiä sekä avoimia kysymyksiä. Osa kysymyksistä oli strukturoituja, jolloin vastauksista tuli keskenään vertailukelpoisia. Sekamuotoiset ja avoimet kysymykset antoivat syvällisempää tietoa kyseisestä teemasta. (Vrt. Vilkka 2005, 84, 86.) Kysymystyypit ja yksittäisten kysymysten numerot haastatteluteemoittain on esitetty taulukossa 1.

TAULUKKO 1. Kysymystyypit ja kysymysten numerot haastatteluteemoittain

		Kysymystyyppi ja kysymyksen numero			
Haastatteluteemat		Monivalintakysymys	Sekamuotoinen kysymys	Likert -asteikko	Avoin kysymys
	Taustatiedot	2, 3	-	-	1, 4
	Tietoturvallisuus ja tietosuoja esimiestyössä	-	-	-	5, 6, 7, 8
	Hallinnollinen tietoturvallisuus	9	-	10	11
	Potilastietojen käsittely	-	13, 14, 15	12	16
	Tietojärjestelmien käyttö ja käyttäjätunnukset	22, 23	17, 18, 19, 20, 21, 24	-	25
	Osaaminen ja koulutus	28, 29, 31, 35	26, 27, 34, 36	-	30, 32, 33, 37
	Tietoturvallisuuden häiriö- ja poikkeustilanteet	-	38	39	40
	Tietoturvallisuuden kehittäminen	-	42, 43	-	41, 44

Kävin haastattelulomakkeen läpi yhdessä ohjaavan opettajan, työelämäohjaajien ja tietoturvatyöryhmän kanssa. Kommenttien perusteella poistin joitakin kysymyksiä sekä tein täsmennyksiä kysymysten muotoon. Haastattelulomakkeen esitestasi kolme hoitotyön ammattihenkilöä, jotka toimivat tai ovat lähiaikoina toimineet osastonhoitajan tehtävissä. Testaustilanteissa haastateltavat kokivat, että kysymyksiä oli vaikea hahmottaa niitä näkemättä, joten annoin heille kysymyslomakkeen vastaamisen tueksi. Esitestausten perusteella tarkensin kysymysten sanamuotoja ja järjestystä sekä poistin yhden avoimen kysymyksen, joka tuotti päällekkäisiä vastauksia kahden muun kysymyksen kanssa.

Haastattelin osastonhoitajat syys- ja lokakuussa 2012 osastonhoitajien työhuoneissa yksilöhaastatteluna. Esitestauksessa syntyneiden kokemusten perusteella haasteltavat saivat haastattelutilanteessa nähtäväkseen kysymykset, mikä helpotti kysymysten hahmottamista. Haastateltavilla oli mahdollisuus kommentoida ja täydentää vastauksiaan avoimesti myös varsinaisten kysymysten ulkopuolelta. Kirjasin vastaukset käsin

haastattelulomakkeelle ja identifioin jokaisen lomakkeen yksilöllisellä koodilla analyysia varten. Vein haastatteluaineiston jokaisen haastattelusession jälkeen Webropol-ohjelmaan.

Päiväkirjamerkinnät

Toisena aineistonkeruumenetelmänä käytin päiväkirjaa, johon keräsin tietoa edellä mainittujen osastotuntien ja työpaikkakokouksien sisällöistä. Kirjasin tilaisuuksien aikana asiasanoja ja lauseita, jotka kuvasivat keskustelun sisältöä ja esille nousevia kehittämiskohteita. Yksilöin jokaisen tapaamisen ajankohdan ja työyksikön mukaan, jotta kehittämistarpeet voidaan tarvittaessa kohdentaa tiettyyn yksikköön. Lisäksi kirjasin jokaisen tapaamisen ajankohdan ja kohderyhmän Excel-taulukkoon tapaamisten kokonaiskuvan hahmottamiseksi.

Tietoturvapoikkeamaraportin hyödyntäminen

Kolmantena menetelmänä hyödynsin sairaanhoitopiirin tietoturvapoikkeamailmoituksista koottua raporttia, joka kuvaa organisaatiossa tapahtuneita tietoturvallisuuteen ja tietosuojaan liittyviä ongelma- ja häiriötilanteita. Tietoturvapoikkeamat kirjataan Excel-taulukkoon, jossa kuvataan tapahtuma-aika ja kesto, tapahtuman kuvaus, poikkeaman ilmoittaja ja vastuuhenkilö sekä luokitellaan tapahtuma ennalta sovitun luokittelun mukaisesti. Poikkeamat käsitellään ja tarvittavista jatkotoimenpiteistä sovitaan kuukausittain tietoturvatyöryhmän kokouksessa. Tässä kehittämistehtävässä kuvasin poikkeamailmoitusten sisältöä yleisellä tasolla niiden arkaluonteisuuden vuoksi.

4.3.2 Aineiston analyysi

Haastatteluaineiston analyysissä hyödynsin Webropol-ohjelmaa. Ohjelma käsitteli strukturoidut kysymykset valmiiksi tilastolliseen muotoon. Kävin vastaukset läpi kohta kohdalta päätarkoituksena saada näkyville keskeisimmät tietoturvallisuuteen ja tietosuojaan liittyvät kehittämiskohteet. Käsittelin aineiston pääsääntöisesti kuvaamalla vastausten jakaumat lukumäärinä. Koska aineisto oli pieni, prosenttiosuuksia ei raportissa kuvata. Joidenkin muuttujien riippuvuussuhdetta kuvasin ristiintaulukoinnin avulla, mikäli kysymys oli koettu merkittäväksi käytännön kehittämisen näkökulmasta.

Haastatteluaineiston avoimet kysymykset, päiväkirjamerkinnät ja tietoturvapoikkeamat analysoin soveltaen teoriaohjaavaa sisällönanalyysia. Vilkka (2005, 140) sekä Tuomi ja Sarajärvi (2009, 95─97, 117) toteavat, että tällä menetelmällä etsitään tutkimusaineistosta tyypillistä logiikkaa tai käsitteitä aikaisemman teoriaan perustuvan tiedon ohjaamana. Analyysissä on tunnistettavissa aikaisemman tiedon merkitys, mutta etenemistapa on uutta luova ja aineistolähtöinen. Aineistoa pelkistämällä ja tiivistämällä se ryhmitellään kokonaisuudeksi, käsitteiksi tai luokitteluiksi, jotka liitetään teoreettisiin käsitteisiin.

Kävin aineiston huolellisesti läpi useaan kertaan, ja luokittelin vastaukset teoriaosuudesta nousevien pääkäsitteiden eli teema-alueiden alle. Lisäksi kvantifioin aineiston eli laskin lukumäärinä, kuinka monta kertaa sama asia esiintyy aineistossa. Tietoturvapoikkeamien osalta suoritin analyysin kuvaten ilmiöt pääkäsitteiden avulla yleisyysjärjestyksessä, sillä poikkeamat ovat organisaation sisäiseen käyttöön tarkoitettua, ei julkista aineistoa.

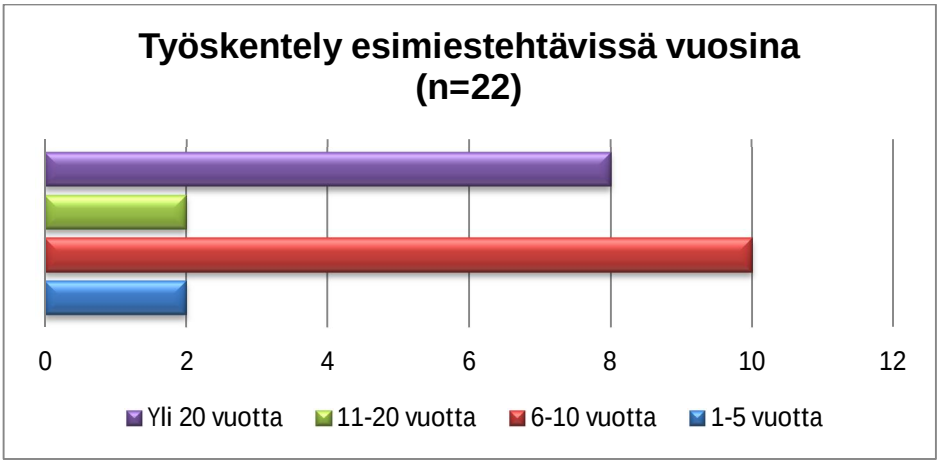
5 TULOKSET

5.1 Haastattelun tulokset

Kuvaan osastonhoitajien haastattelutulokset teema-alueiden pohjalta. Teemoja olivat taustatiedot, tietoturvallisuus ja tietosuoja esimiestyössä, hallinnollinen tietoturvallisuus, potilastietojen käsittely, tietojärjestelmien käyttö ja käyttäjätunnukset, osaaminen ja koulutus, tietoturvallisuuden häiriö- ja poikkeustilanteet sekä tietoturvallisuuden kehittäminen. (Taulukko 1.)

5.1.1 Haastateltavien taustatiedot

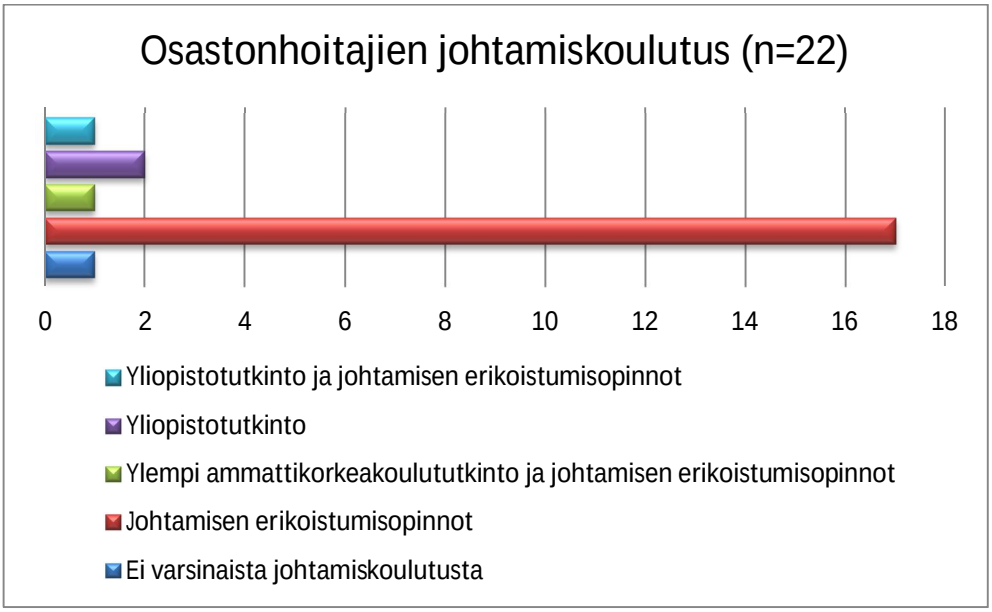
Esimiestehtävissä vastaajat olivat työskennelleet varsin pitkään, keskimäärin 15 vuotta (vaihteluväli 5–32 vuotta; n=22). Alle vuoden esimieskokemusta ei ollut kellään, yli 20 vuotta kokemusta oli kahdeksalla vastaajalla. Lähes puolella vastaajista (n=10) kokemusta oli 6–10 vuotta. (Kuvio 3.)



KUVIO 3. Työskentely esimiestehtävissä vuosina (n=22)

Kolmasosa vastaajista (n=7) työskenteli ensihoidon, päivystyksen tai konservatiivisella tulosalueella, kolmasosa (n=7) operatiivisella ja lähes kolmasosa (n=6) psykiatrisella tulosalueella. Yksi vastaaja ilmoitti tulosalueekseen jonkin muun alueen.

Johtamiskoulutuksena enemmistöllä vastaajista (n=17) oli johtamisen erikoistumisopinnot tai vastaava tutkinto. Yhdellä vastaajalla oli yliopistotutkinto ja kahdella yliopistotutkinto täydennettynä johtamisen erikoistumisopinnoilla. Yksi vastaaja oli suorittanut ylemmän ammattikorkeakoulututkinnon ja johtamisen erikoistumisopinnot. Yhdellä vastaajalla ei ollut varsinaista johtamiskoulutusta. (Kuvio 4.)



KUVIO 4. Osastonhoitajien johtamiskoulutus (n=22)

Tietoturvallisuuteen tai tietosuojaan liittyvää koulutusta oli kolmella vastaajalla. Kaksi heistä oli suorittanut muutaman opintopisteen laajuisen erillisen opintojakson yliopistossa. Yhden vastaajan mukaan johtamiskoulutus sisältyi hänen perusopintoihinsa.

5.1.2 Tietoturvallisuus ja tietosuoja esimiestyössä

Tietoturvalliseen toimintaan sisältyy vastaajien mielestä potilastietojen asianmukainen käsittely sekä tietojärjestelmissä että muulla tavoin esimerkiksi suullisesti potilaan asioita hoidettaessa (23 mainintaa). Vastaajat korostivat salassapitoa ja vaitiolovelvollisuutta erityisesti potilaiden hoitoon liittyvissä asioissa. Keskeistä on työntekijöiden tietoturvatietoisuus, osaaminen ja asenne, niin sanottu ”tietoturvaomatunto” (21 mainintaa).

”Samalla tavoin, kun meillä hoitajilla on sisäänrakennettu aseptinen omatunto, pitäisi olla myös tietoturvaomatunto.”

”Tietoturva on niin tärkeä asia, että mieti ennen kuin puhut, teet, kirjaat jne., - tietoturvan on oltava jokaisella hanskassa henkilökohtaisesti.”

Tietoturvalliseen toimintaan sisältyy työasemien, tietojärjestelmien ja sovellusten turvallinen käyttö sekä käyttäjätunnusten asianmukainen käsittely (19 mainintaa). Tärkeänä pidettiin myös tietoturvallista toimintaympäristöä, kuten tietokoneiden riittävää määrää ja oikeaa sijoittelua, potilaiden ohjaamiseen tarkoitettujen tilojen riittävyyttä ja yksityisyyttä sekä salassa pidettävien asiakirjojen oikeaa säilyttämistä (6 mainintaa).

Esimiestyön näkökulmasta merkittävin tietoturvallisuuteen vaikuttava asia oli henkilöstön ohjaaminen ja opastaminen tietoturvalliseen toimintaan (19 mainintaa). Vastaajat pitivät tärkeänä, että henkilöstö tuntee vastuunsa ja oikeutensa potilastietojen käytössä sekä käsitellessään tietoja sähköisessä potilastietojärjestelmässä että esimerkiksi työtiloissa tai puhelimessa. Esimiestyön näkökulmasta tietoturvallisuutta loi henkilöstön riittävästä perehdytyksestä ja koulutuksesta huolehtiminen (8 mainintaa). Vastaajat kertoivat seuraavansa työntekijöiden asennetta ja ”tietoturvaomatuntoa”, ja herättelevänsä sitä tarvittaessa (5 mainintaa). Vastaajat pitivät tärkeänä esimiehen vaitiolovelvollisuutta ja tietosuojaa työntekijöihin liittyvissä asioissa (6 mainintaa). Myös

oman osaamisen kehittämistä ja esimerkkinä toimimista pidettiin esimiestyön kannalta tärkeänä (5 mainintaa).

Tietoturvallisuuteen ja tietosuojaan liittyvien asioiden toteutumista omalla vastuualueellaan vastaajat seurasivat henkilöstöä opastamalla, neuvomalla, tukemalla ja ohjaamalla koulutuksiin (35 mainintaa). Osastonhoitajat seurasivat käytännön työskentelyä yksiköissä ja puuttuivat sitä kautta ongelmatilanteisiin (20 mainintaa). He kertoivat sulkevansa auki jääneitä tietokoneita, muistuttavansa henkilöstöä asiamukaisesta potilastietojen käsittelystä ja seuraavansa tilojen turvallista käyttöä. Seurantaan liittyi myös potilastietojen käytön jälkikäteisvalvonta lokitietojen seurannan avulla (7 mainintaa).

5.1.3 Hallinnollinen tietoturvallisuus

Sairaanhoitopiirin tietoturvallisuudesta vastaa yhdentoista vastaajan mukaan ensisijaisesti sairaanhoitopiirin johtaja. Yhdeksän vastaajan mukaan vastuussa on johtajaylilääkäri ja yhden mukaan sairaalajohtaja.

Suurin osa vastaajista (n=18) koki, että ylimmän johdon tekemistä tietoturvallisuutta koskevista päätöksistä tiedotetaan esimiehille selkeästi. Myös tietoturvapolitiikkaa piti selkeänä suurin osa (n=15) vastaajista. Lähes puolet (n=10) kuitenkin koki, että johdon tekemiä päätöksiä on hankala toteuttaa käytännössä.

Yli puolet (n=14) vastaajista oli sitä mieltä, että johto toimii esimerkkinä tietoturvallisen toiminnan toteuttamisessa. Toisaalta yli puolet (n=12) ei saanut omalta esimieheltään riittävästi tukea tietoturvallisen toiminnan johtamiseen. Osastonhoitajat ja henkilöstö keskustelivat keskenään tietoturvallisuuteen liittyvistä asioista. Lähes kaikki yksiköt pystyivät vastaajien mukaan (n=19) toimimaan tietoturvallisesti nykyisillä henkilöstöresursseilla, taloudellisten resurssien riittämättömyys haittasi kuitenkin toimintaa kuuden vastaajan mielestä. Taloudellisten resurssien riittämättömyys liittyi tilojen epäkäytännöllisyyteen ja ahtauteen, esimerkiksi potilaiden ohjaamiseen ei ollut riittävästi rauhallisia tiloja. Omia valmiuksiaan tietoturvallisen toiminnan johtamiseen piti riittävinä tai melko riittävinä suurin osa eli 18 vastaajaa. (Taulukko 2.)

TAULUKKO 2. Tietoturvallisuuden johtaminen, kommunikointi ja valmiudet (n=22)

	Täysin samaa mieltä (n)	Osittain samaa mieltä (n)	Osittain eri mieltä (n)	Täysin eri mieltä (n)	Ei samaa eikä eri mieltä (n)
Ylimmän johdon tekemistä tietoturvallisuutta koskevista päätöksistä tiedotetaan esimiehille selkeästi	5	13	3	0	1
Sairaanhoitopiirin tietoturvapolitiikka on selkeä ja toteutettavissa käytännön työssä	4	11	6	1	0
Johdon tekemiä päätöksiä on hankala toteuttaa käytännössä	1	9	5	7	0
Johto toimii esimerkkinä tietoturvallisen toiminnan toteuttamisessa	7	7	4	0	4
Saan esimieheltäni riittävästi tukea tietoturvallisuuden johtamiseen vastuualueellani	6	1	5	7	3
Keskustelen työntekijöiden kanssa tietoturvallisuuteen liittyvistä asioista	16	6	0	0	0
Henkilöstö pohtii tietoturvallisuuteen liittyviä asioita avoimesti	15	6	1	0	0
Pystymme toimimaan tietoturvallisesti nykyisillä henkilöstöresursseilla	12	7	3	0	0
Pystymme toimimaan tietoturvallisesti nykyisillä taloudellisilla resursseilla	10	6	5	1	0
Minulla on riittävät valmiudet tietoturvallisen toiminnan johtamiseen omalla vastuualueellani	3	15	4	0	0

Tietoturvapolitiikassa ja ohjeissa koettiin olevan jonkin verran päällekkäisyyttä ja ristiriitaa, jotka hankaloittivat niiden soveltamista käytäntöön. Lisäresursseina haastateltavat toivoivat potilastietojen käyttöä helpottavaa teknologiaa kuten kämmentietokoneita. Myös omaan tietoturvaosaamisensa kehittämiseen haastateltavat toivoivat tukea sairaanhoitopiiriltä esimerkiksi esimieskoulutusten muodossa (vrt. 5.1.6).

5.1.4 Potilastietojen käsittely

Lähes kaikki (n=21) vastaajat olivat sitä mieltä, että henkilöstö tuntee potilastietojen käsittelyä koskevan lainsäädännön ja noudattaa potilastietojen käsittelystä annettuja ohjeita (n=18). Henkilöstö oli myös saanut koulutuksen potilastietojen käsittelyyn.

Kaikkien mielestä (n=22) työntekijät tietävät, missä yhteydessä potilastietoja saa käsitellä. Kuusi vastaajaa kuitenkin totesi, ettei täysin tiedä, käsitelläänkö yksikössä potilastietoja lain ja ohjeiden mukaisesti. Lähes kaikki (n=21) tunsivat potilastietojen käytön seurantaan liittyvät esimiehen velvollisuudet ja pitivät potilastietojen käytön seurantaprosessia toimivana (n=17). Kuitenkin puolet vastaajista (n=11) haluaisi tehostaa potilastietojen käytön seurantaa ja valvontaa. Lähes kaikkien vastaajien (n=19) mielestä myös henkilöstö tuntee potilastietojen käytön valvontaperiaatteet. Potilastietojärjestelmän lokitietojen seurantaa kaikki (n=22) pitivät tärkeänä osana tietosuojan käytännön toteutusta. Potilastietojen käytön seuranta kului esimiehen tehtäviin kahdenkymmenen vastaajan mielestä. (Taulukko 3.)

TAULUKKO 3. Potilastietojen käyttö ja seuranta (n=22)

	Täysin samaa mieltä (n)	**Osittain samaa mieltä (n)**	**Osittain eri mieltä (n)**	**Täysin eri mieltä (n)**	**En osaa sanoa (n)**
Henkilöstö tuntee potilastietojen käsittelyä koskevan lainsäädännön	7	14	1	0	0
Henkilöstö noudattaa potilastietojen käsittelystä annettuja ohjeita	6	12	4	0	0
Työntekijät tietävät, missä yhteydessä ja laajuudessa potilastietoja saa käsitellä	13	9	0	0	0
Henkilöstö on saanut koulutuksen potilastietojen käsittelyyn	13	7	2	0	0
En tiedä, käsitelläänkö yksikössäni potilastietoja lain ja ohjeiden mukaisesti	0	6	7	9	0
Tunnen potilastietojen käytön seurantaan liittyvät esimiehen velvollisuudet	18	3	1	0	0
Potilastietojen käytön seurantaprosessi on toimiva	12	5	1	2	2
Potilastietojen käytön seurantaa ja valvontaa tulisi tehostaa	5	6	7	3	1

Tarkentavina kommentteina haastateltavat pohtivat, ymmärtävätkö työntekijät, mitä potilastietojen käytön seuranta kunkin omalla kohdalla tarkoittaa ja mihin tietojen väärinkäyttö voi johtaa. Esimiehen näkökulmasta lokiraportteja pidettiin vaikeaselkoisina ja potilastietojen käytön seurantaan toivottiin koulutusta ja automatisointia.

5.1.5 Tietojärjestelmien käyttö ja käyttäjätunnukset

Kaikilla (n=22) haastateltavien vastuualueiden työntekijöillä oli henkilökohtaiset tietojärjestelmien käyttäjätunnukset. Käyttäjätunnusten hakuprosessia piti toimivana kaksitoista vastaajaa, mutta yhdeksän mielestä se vaatii kehittämistä, sillä tunnuksia ei toimiteta uusille työntekijöille riittävän nopeasti.

Käyttäjätunnusten hakuprosessin koettiin olevan liian byrokraattinen ja epäselvä. Tietojärjestelmien tunnuksia joudutaan hakemaan useista eri paikoista. Tunnukset tulevat hitaasti, työntekijä ei saa kaikkia pyydettyjä oikeuksia kerralla tai saadut tunnukset eivät toimi. Vastaajat kokivat, että koko tunnustenhallinta pitäisi keskittää yhteen paikkaan ja hakuprosessi sähköistää kokonaisuudessaan. Kehitystyöhön tulisi ottaa tiiviimmin mukaan myös esimiehet.

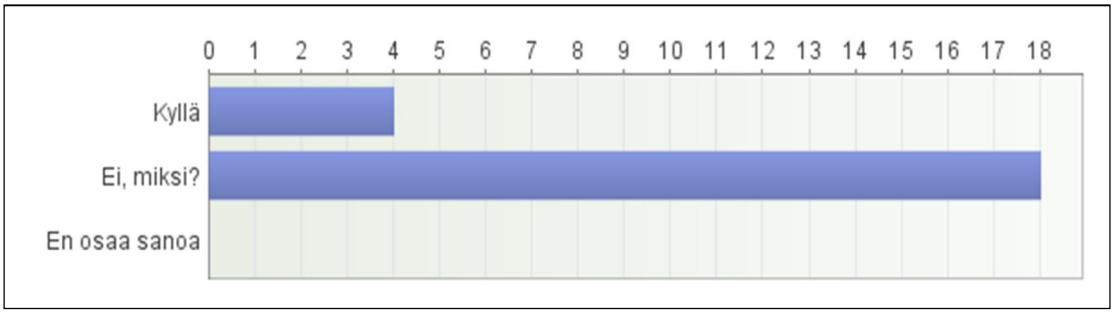
Lähes puolessa yksiköistä (n=10) työntekijät tekevät tietojärjestelmien ja tietoliikenneverkon käyttäjäsitoumuksen osastonhoitajan kanssa käyttäjätunnusten hakemisen yhteydessä. Yli puolet vastaajista (n=12) oli kuitenkin sitä mieltä, että sitoumusta ei tässä yhteydessä tehdä. Käyttäjätunnushakemukset tehdään usein jo ennen työsuhteen alkua, jolloin työntekijä ei ole fyysisesti paikalla. Hakemuksia tehdään myös rekrytointiyksikössä ja ylihoitajien luona, eivätkä vastaajat olleet tietoisia käytännöistä, joiden mukaan siellä toimitaan. Kaikki vastaajat eivät tunteneet tietojärjestelmien ja tietoliikenneverkon käyttäjäsitoumusta tai siihen liittyviä ohjeita. Lähes kaikki vastaajat (n=21) kertoivat työntekijälle, että käyttäjätunnukset ovat henkilökohtaiset eikä niitä saa luovuttaa muille.

Kahdeksan vastaajaa oli sitä mieltä, että henkilöstön Internetin ja sosiaalisen median palveluiden, kuten Facebookin käyttö yksityisasioissa haittaa työtehtävien hoitoa. Eräs vastaaja kommentoi, että ongelmatilanteita on silloin tällöin, mutta ne on saatu keskustelemalla hallintaan. Palveluiden käytöstä koettiin olevan eniten haittaa psykiatrisella tulosalueella. (Taulukko 4.)

TAULUKKO 4. Internetin ja sosiaalisen median palveluiden yksityiskäytön haittaavuus tulosalueilla (n=22)

Tulosalue	Haittaa toimintaa (n)	Ei haittaa toimintaa (n)
Konservatiivinen, ensihoito, päivystys	2	5
Operatiivinen	1	6
Psykiatrinen	4	2
Alueelliset ja keskitetyt palvelut	0	1
Muu	1	0
Yhteensä	8	14

Yli puolet (n=13) vastaajista kertoi, että tietokoneet jäävät auki ilman valvontaa päivittäin tai viikoittain.



KUVIO 5. Nykyiset kirjautumisratkaisut mahdollistavat joustavan tietojärjestelmien käytön potilashoidossa (n=22)

Nykyiset kirjautumisratkaisut mahdollistavat joustavan tietojärjestelmien käytön potilashoidossa ainoastaan neljän vastaajan mielestä. Jopa yli kolme neljäsosaa (n=18) piti nykyisiä tietokoneiden ja -järjestelmien kirjautumisratkaisuja liian hitaana ja monimutkaisena. (Kuvio 5.)

5.1.6 Osaaminen ja koulutus

Työntekijät saivat tietoturvallisuuteen ja tietosuojaan liittyvissä asioissa ohjausta sekä työhöntulovaiheessa että sen jälkeen oman tarpeen mukaan työsuhteen kestosta riippumatta. Lähes kaikki (n=21) vastaajat kertoivat, että työntekijät ovat suorittaneet tietoturva ja tietosuojakoulutuksen Kanta-sivuilla. Puolet vastaajista (n=11) koki, että sairaanhoitopiiri tarjoaa esimiehille riittävästi koulutusta tietoturvallisuuteen liittyvistä asioista, mutta toisen puolen mielestä koulutusta voisi olla enemmän. Koulutusta toivottiin lainsäädännöstä sekä tietosuojan ja tietoturvallisuuden ”perusasioista”. Erityisesti toivottiin esimiehen tehtäviin liittyvää käytännönläheistä koulutusta ja ”työkaluja”.

Hieman yli puolet vastaajista (n=12) koki, että sairaanhoitopiiri tarjoaa riittävästi tietoturvallisuuteen liittyvää koulutusta työntekijöille. Seitsemän mielestä sitä ei kuitenkaan ollut riittävästi. Koulutusta toivottiin lisää lainsäädännöstä, työntekijän oikeuksista ja velvollisuuksista sekä tietojärjestelmien ja potilastietojen käsittelystä. Sen toivottiin olevan käytännönläheistä ja tapausesimerkkejä sisältävää. Eräs vastaaja kuvasi, että koulutus voisi olla *”konkreettinen polku hoitajille ja lääkäreille…minun tietoturvallisuuteni”*.

Tietoturvallisuuteen liittyvää koulutusta tulisi järjestää, kun lainsäädännössä, toimintatavoissa, -ympäristössä tai tietojärjestelmissä tapahtuu muutoksia (15 mainintaa). Koulutusta pidettiin tärkeänä uusien työntekijöiden perehdytysvaiheessa (13 mainintaa). Kaikille työntekijöille tulisi järjestää kertauskoulutusta säännöllisesti ja erityisesti silloin, jos työyhteisössä on tullut esille jokin ongelmatilanne (7 mainintaa).

Vastaajien mielestä tietoturvallisuuteen liittyvää koulutusta tulisi järjestää ensisijaisesti osastotunneilla ja työpaikkakokouksissa (n=21). Verkkokurssia piti toimivana 14 vastaajaa ja luento-opetusta auditoriossa 10 vastaajaa. Muita ehdotuksia (n=2) olivat kehityskeskustelut sekä tentit ja pistokokeet. Myös osaamisen seurantamahdollisuutta toivottiin verkkokurssin avulla.

Työntekijän tulisi osallistua tietoturva- ja tietosuojakoulutukseen vuoden välein 13:sta vastaajan mielestä. Kolmen vuoden väliä piti sopivana kuusi vastaajaa ja viittä vuotta

yksi vastaaja. Säännönmukaista koulutusta ei tarvittu lainkaan yhden vastaaja mielestä. Hän koki, että koulutusta tulee järjestää tarpeen mukaan.

Kaksi kolmasosaa (n=16) vastaajista koki, että tietojärjestelmien käyttöön on saatavissa riittävästi asiantuntevaa tukea. Kuuden vastaajan mukaan tuki ei ollut riittävää, koska ongelmien ratkaisu vei liian kauan, eikä asian etenemisestä tiedotettu riittävästi. Vastaajat kokivat palvelun ”kasvottomana” ja toivoivat asiantuntijoiden jalkautumista yksikköihin.

5.1.7 Tietoturvallisuuden häiriö- ja poikkeustilanteet

Tietoturvallisuutta vaarantavan tekijän tai tilanteen huomatessaan vastaajat pyrkisivät korjaamaan asian ensisijaisesti itse (n=18). Seuraavaksi asiasta ilmoitettaisiin turvallisuuspäällikölle (n=13) tai tehtäisiin turvallisuuspoikkeamailmoitus (n=11). Omalle esimiehelleen asiasta kertoi ilmoittavansa kahdeksan vastaajaa ja muina toimina otettiin yhteyttä ongelman vastuutahoon tai tietokoordinaattoriin (n=6). Tietoturvallisuuteen liittyvissä poikkeustilanteissa toimimiseen on annettu selkeät ohjeet useimpien mielestä (n=16). Vastaajat kokivat, että yksiköissä osataan toimia oikein tietojärjestelmien käyttökatkojen aikana (n=19) ja tiedetään, minne poikkeustilanteissa otetaan yhteyttä (n=17). Tukihenkilöiden antamia ohjeita pitivät selkeinä lähes kaikki vastaajat. Kirjallisten ohjeiden löytymistä piti helppona tai melko helppona 14 vastaajaa. Jotkut vastaajat pitivät ohjeita vaikeaselkoisina ja liian pitkinä ja Intranetin rakennetta sekavana. Yli puolet vastaajista (n=13) oli sitä mieltä, että kulunvalvontaa ja kulkurajoitteita tulisi lisätä. (Taulukko 5.)

TAULUKKO 5. Tietoturvallisuuteen liittyvissä häiriö- ja poikkeustilanteissa toimiminen

	Täysin samaa mieltä (n)	Osittain samaa mieltä (n)	Osittain eri mieltä (n)	Täysin eri mieltä (n)	En osaa sanoa (n)
Poikkeustilanteissa toimimiseen on annettu selkeät ohjeet	9	7	2	2	2
Yksikkömme osaa toimia oikein tietojärjestelmien käyttökatkon aikana	13	8	1	0	0
Yksikössämme tiedetään, minne ottaa yhteyttä häiriö- tai poikkeustilanteissa	15	5	2	0	0
Tukihenkilöiden antamat ohjeet ovat selkeitä	11	9	2	0	0
Kirjalliset ohjeet löytyvät helposti	5	9	3	1	4
Kulunvalvontaa ja kulkurajoitteita tulisi lisätä	4	9	1	6	2

5.1.8 Tietoturvallisuuden kehittäminen

Tärkeimpinä tietoturvallisuuteen liittyvinä kehittämiskohteina pidettiin tietojärjestelmien ja niihin liittyvien toimintaprosessien kehittämistä käyttäjäystävällisemmäksi. Erityisesti esille nousi kirjautumisratkaisujen kehittäminen nopeammaksi ja vähemmän salasanojen muistamista vaativaksi (12 mainintaa). Myös käyttäjätunnusten hakuprosessin selkiyttämistä ja keskittämistä toivottiin (2 mainintaa). Lisäksi toivottiin teknisiä estoja esim. Internetin tai sosiaalisen median käyttöön (2 mainintaa).

Toinen merkittävä kehittämiskohde oli henkilöstön tietoturvallisuuteen liittyvän asenteen kehittäminen ja siihen liittyvä koulutus (10 mainintaa). Myös ohjeistuksia tulisi selkeyttää ja niiden löydettävyyttä parantaa (6 mainintaa). Tietosuojan valvonnan kehittämiseen, esimiesten rooliin ja valvonnassa käytettäviin työvälineisiin tulisi kiinnittää jatkossa enemmän huomiota (5 mainintaa). Seurantaa tulisi tehostaa, mutta samalla siihen tulisi hankkia tehokkaat työvälineet.

Tietoturvallisuutta koskevan kartoituksen omalla vastuualueellaan koki tarpeelliseksi puolet vastaajista (n=11) ja koko sairaanhoitopiirissä 13 vastaajaa. Kartoitusta pidettiin tarpeellisena kokonaisuuden hahmottamisen kannalta, ja sitä pidettiin yhtenä sisäisen laadunhallinnan välineenä. Toisaalta ne vastaajat, jotka eivät pitäneet kartoitusta

tarpeellisena, perustelivat asiaa jatkuvalla muutoksella ja sillä, että toiminnassa ei ole ollut ongelmia.

5.2 Päiväkirjamerkinnät ja tietoturvapoikkeamat

Osastotunteja ja työpaikkakokouksia pidettiin aineistonkeruuaikana yhteensä 15. Tilaisuuksiin osallistui pääsääntöisesti hoitohenkilöstöä ja osastonsihteereitä sekä muutama lääkäri. Eniten keskustelua ja kysymyksiä herätti potilastietojen käsittely. Pohdittiin, missä tilanteissa potilaan tietoja saa käsitellä ja kuinka laajasti (18 mainintaa). Erityisesti psykiatrian tietojen ja yhteisessä potilastietokannassa tapahtuva potilastietojen katselu sekä potilastietojen luovutus sairaanhoitopiirin alueen potilastietorekisterin sisällä ja sen ulkopuolelle aiheutti keskustelua. Tietokoneiden ja tietojärjestelmien auki jääminen ilman valvontaa, kirjaaminen vahingossa toisen tunnuksilla sekä kirjautumisen hitaus ja kömpelyys keskusteluttivat (9 mainintaa). Lisäksi esitettiin kysymyksiä potilastietojärjestelmän käytön seurantamenetelmistä ja väärinkäyttöepäilyihin liittyvästä toimintaprosessista (5 mainintaa). Tietosuoja-, tietoturva-, yhteinen potilastietorekisteri - ja sairaanhoitopiirin potilasrekisteri-käsitteissä oli epäselvyyttä (3 mainintaa). Internetin ja sosiaalisen median palveluiden käyttö työaikana herätti myös jotakin kysymyksiä (3 mainintaa).

Tietoturvapoikkeamia raportoitiin joulukuun 2011 ja lokakuun 2012 välisenä aikana 28 tapahtumaa. Eniten poikkeamia aiheutui inhimillisten syiden seurauksena. Ongelmia oli muun muassa käyttäjätunnusten asianmukaisessa käytössä, säilyttämisessä ja luovuttamisessa. Luottamuksellista tietoa myös joutui väärään paikkaan toimintaprosessien epäselvyyksistä johtuen. Lisäksi raportoitiin tietojärjestelmien toimintahäiriöihin liittyvistä ongelmista.

5.3 Yhteenveto tuloksista

Tulosten perusteella esimiehet ovat kiinnostuneita tietoturvallisen toiminnan kehittämisestä ja valmiita panostamaan siihen. Esimiehillä on varsin kattava kuva oman vastuualueensa tilanteesta ja myös käytännönläheisiä ehdotuksia tietoturvatoiminnan kehittämiseen.

Tietoturvallisuutta ja tietosuojaa pidetään hoitohenkilöstön keskuudessa periaatteellisena asiana ja siihen halutaan sitoutua. Lähiesimiehet korostivat tietoturvallisuuteen liittyvää asennetta ja jokaisen työntekijän vastuuta omasta toiminnastaan. Tietoturvallista toimintaa kuvasivat käsitteet vaitiolovelvollisuus, salassapito, luottamuksellisuus ja omatunto. Esimiehet kertoivat pääsääntöisesti uskovansa siihen, että henkilöstö toimii lain ja ohjeiden mukaisesti. Koulutuksen tarve on kuitenkin jatkuva, ja koulutuksen toivotaan vastaavan käytännön tarpeisiin.

Omaa osaamistaan tietoturvallisuuteen ja tietosuojaan liittyvissä asioissa esimiehet pitivät melko hyvänä. Tuloksissa korostuvat kuitenkin oman osaamisen kehittämisen tarve sekä lainsäädännön, potilastietojen käsittelyyn liittyvien ohjeiden että henkilöstön tukemiseen, ohjaamiseen ja valvontaan liittyvien asioiden osalta. Koulutusta toivottiin erityisesti esimiestyön näkökulmasta; esimiehen vastuista, velvollisuuksista ja oikeuksista tietoturvallisen toiminnan toteuttamisessa, seurannassa ja kehittämisessä. Henkilöstön näkökulmassa korostuivat puolestaan välittömään potilastyöhön ja tietosuojaan liittyvät asiat, kuten potilastietojen käsittely sekä potilastietojen käytön valvonta.

Vaikka henkilöstöön luotetaan, potilastietojen käytön valvontaa tulee tulosten perusteella kehittää. Esimiehet halusivat selkiyttää omaa rooliaan valvontaprosessissa sekä toivoivat tehokkaampia työvälineitä valvonnan toteuttamiseen vastuualueillaan. Henkilöstön osalta valvontaprosessia tulisi kehittää avoimemmaksi ja läpinäkyvämmäksi.

Sairaanhoitopiirin tietoturvallisuuteen ja tietosuojaan liittyviä ohjeistuksia pidettiin melko kattavina. Ohjeita on kuitenkin määrällisesti paljon, ne ovat osittain vaikeaselkoisia ja hankalasti löydettävissä. Lisäksi niissä on jonkin verran päällekkäisyyttä ja ristiriitaisuutta, mikä hankaloittaa käytännön hoitotyötä.

Tuloksissa korostuvat sähköiset tietojärjestelmät, niiden käytettävyys ja käytön haasteet. Haastatteluissa tietojärjestelmien käytettävyysongelmat nähtiin osittain tietoturvallisuutta ja tietosuojaa uhkaavana tekijänä. Toisaalta ongelmat eivät aiheudu yksinomaan järjestelmistä, vaan myös toimintaprosessien selkiyttämiselle on tarvetta esimerkiksi käyttäjätunnusten hallinnan ja kirjautumisratkaisujen osalta.

Internetin ja sosiaalisen median käyttö työaikana yksityisiin tarkoituksiin ei useimmissa yksiköissä aiheuttanut ongelmia. Verkkopalveluihin liittyy kuitenkin sekä tietoturvallisuuteen että muihin työelämän pelisääntöihin kohdistuvia haasteita. Tästä syystä sääntöjen luomista sairaanhoitopiirin tasolla ja niistä keskustelua pidettiin tärkeänä.

Hallinnollisesta näkökulmasta sairaanhoitopiirin johdon koettiin toimivan tietoturvaasioissa pääasiassa johdonmukaisesti ja esimerkillisesti. Lähiesimiehet toivoivat kuitenkin enemmän tukea tietoturvallisuuden johtamiseen omilta esimiehiltään.

Tietoturvapoikkeamia raportoitiin aineistonkeruuaikana organisaation kokoon nähden vähän. Haastatteluissa kävi ilmi, että raportointikäytännöt eivät ole täysin selkeät ja raportointiin tarvitaan uusia, helppokäyttöisiä menetelmiä. Toisaalta ongelmat ratkaistaan usein työyksiköissä, jolloin ilmoittamistarvetta ei välttämättä tunnisteta seurannan ja raportoinnin näkökulmasta.

6 KEHITTÄMISSUOSITUKSET JA AIKATAULUTUS

6.1 Suositukset tietoturvallisuuden ja tietosuojan kehittämiseen

Etelä-Savon sairaanhoitopiirissä on panostettu tietoturvallisuuden ja tietosuojan kehittämiseen vuosien ajan. Kehitystyö näkyy vahvana erityisesti potilastietojen käsittelyssä ja niihin liittyvässä ohjeistuksessa, jotka pääsääntöisesti koskettavat potilaiden hoitoon osallistuvaa henkilöstöä. Vaikka seuraavien suositusten pohjalla ovatkin suurelta osin hoitotyön näkemykset, lähes kaikki toimenpiteet voidaan laajentaa koskemaan koko sairaanhoitopiiriä ja sen henkilöstöä.

Tietoturvallisuuteen ja tietosuojaan liittyvän johtamisen kehittäminen

- Nostetaan tietoturvallisuus ja tietosuoja yhdeksi johtamisen kehittämiskohteeksi. Selkiytetään tietoturvallisuuteen ja tietosuojaan liittyvää johtamista, organisointia ja keskeisten vastuuhenkilöiden rooleja sekä tiedotetaan niistä koko henkilöstölle.

- Päivitetään tietoturvapolitiikka ja täsmennetään sitä erityisesti tietosuojan linjauksissa. Politiikan linjausten tulisi ohjata tiiviimmin toimintaa. Jatketaan jalkautustyötä erityisesti organisaation ylimmässä ja keskijohdossa.
- Kehitetään tiedottamista ja yhteistyötä läpi koko organisaation sekä kiinnitetään huomio erityisesti lähiesimiesten tukemiseen.

Tietoturvapoikkeamaraportoinnin kehittäminen

- Systematisoidaan tietoturvapoikkeamailmoituskäytäntöjä kuvaamalla ilmoitusprosessi.
- Kehitetään olemassa olevaa sähköistä turvallisuuspoikkeamailmoitusta siten, että myös tietoturvallisuuteen liittyvät häiriöt voi ilmoittaa sitä kautta.
- Tiedotetaan ilmoittamiskäytännöistä ja ilmoittamisen merkityksestä koko henkilöstölle riittävän laajasti.

Tietoturvallisuuteen ja tietosuojaan liittyvä koulutus

- Tietoturvallisuuteen ja tietosuojaan liittyvää peruskoulutusta järjestetään systemaattisesti koko henkilöstölle. Jokaisen työntekijän edellytetään osallistuvan koulutukseen. Koulutuksissa hyödynnetään olemassa olevia sähköisiä oppimisympäristöjä ja alueellista yhteistyötä.
- Potilastietojen käsittelyyn osallistuvalle henkilöstölle räätälöidään omaa koulutusta tarvelähtöisesti.
- Esimiehille järjestetään omaa koulutusta tarvelähtöisesti. Koulutus keskittyy erityisesti rekisterinpitoon, lainsäädäntöön ja esimiehen rooliin.
- Koulutusten toteutumiselle rakennetaan seurantajärjestelmä ja seurantavastuut määritellään.

Tietoverkon ja tietojärjestelmien kirjautumisratkaisujen kehittäminen

- Selvitetään, miten ja millä aikataululla tietoverkon ja tietojärjestelmien kirjautumisratkaisuja voidaan kehittää nopeammiksi ja käyttäjäystävällisemmiksi.
- Tiedotetaan kirjautumisratkaisujen kehittämisestä henkilöstölle selkeästi ja otetaan henkilöstö mukaan kehitystyöhön.

Potilastietojen käytön seurannan ja valvonnan kehittäminen

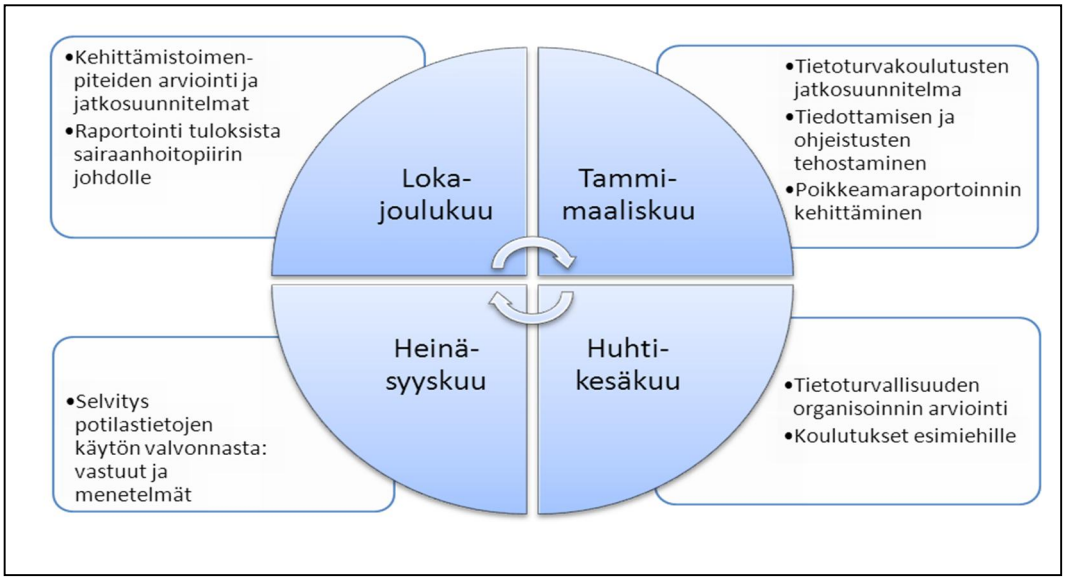
- Pyritään lisäämään potilastietojen käytön seurannan ja valvonnan avoimuutta ja läpinäkyvyyttä jatkamalla asiasta tiedottamista henkilöstölle.
- Käydään läpi potilastietojen käytön seurantaan ja valvontaan liittyvä ohjeistus ja päivitetään se tarvittaessa. Laaditaan tarvittaessa seurantaan osallistuville esimiehille oma ohjeistus.
- Pyritään tehostamaan potilastietojen käytön valvontaa. Tutustutaan tietojärjestelmiin, jolla pystytään automatisoimaan käytönvalvontaa ja poimimaan sieltä poikkeavat tulokset. Harkitaan järjestelmähankintaa alueellisena hankintana.

Tietoturva- ja tietosuojaohjeistusten kehittäminen

- Tarkistetaan tietoturvallisuuteen ja tietosuojaan liittyvät ohjeistukset ja niiden ylläpitovastuut sekä tehdään tarvittavat päivitykset.
- Kartoitetaan mahdollisuudet ohjeiden sähköisen haun tehostamiseen.
- Kiinnitetään erityistä huomiota ohjeiden selkeään ja yhdenmukaiseen ulkoasuun ja kielelliseen ilmaisuun.
- Edellytetään, että sairaanhoitopiirissä on olemassa virallinen linjaus siitä, miten ja missä tilanteissa Internetiä ja siihen liittyviä palveluita voi käyttää.
- Laaditaan/ päivitetään Internetin ja sosiaalisen median käyttöön liittyvä ohjeistus tietoturvallisuuden näkökulmasta yhteistyössä organisaation viestinnän kehittämistyöryhmän kanssa.

6.2 Kehittämisen vuosikello 2013

Esittelin edellä kuvatut kehittämissuositukset Etelä-Savon sairaanhoitopiirin tietoturvatyöryhmässä joulukuussa 2012. Keskustelun pohjalta päädyttiin siihen, että työryhmän jäsenet tutustuvat ehdotuksiin, ja asia otetaan uudelleen esille seuraavassa kokouksessa. Tammikuussa 2013 pidetyssä kokouksessa hyväksyttiin esittämäni kehittämisalueet ja vuosikello vuodelle 2013 pääpiirteittäin (Kuvio 6).



KUVIO 6. Vuosikello: tietoturvallisuuden kehittämisalueet vuodelle 2013

Kehitettävät asiat ovat kuitenkin laajoja ja vaativat jokainen erillisen toimeenpanosuunnitelman, jota työstetään kuluvan vuoden aikana. Vuosikelloon tietoturvatyöryhmä nosti kiireellisimpiä kehittämiskohteita, joille laadittiin ohjeellinen toteutusaikataulu.

7 POHDINTA

7.1 Tulosten luotettavuuden arviointi

Valitsin aineiston keruuseen kolme erilaista menetelmää, koska halusin saada mahdollisimman kattavan näkemyksen tietoturvallisuuteen liittyvistä ilmiöistä. Käytin aineistonkeruussa sekä määrällisiä että laadullisia menetelmiä. Eri menetelmät tukivat toisiaan ja tuottivat tarkentavaa tietoa.

Määrällisessä tutkimuksessa kokonaisluotettavuudella tarkoitetaan sitä, että otos edustaa perusjoukkoa mahdollisimman hyvin ja mittaamisessa on mahdollisimman vähän satunnaisia virheitä. Reliabiliteetilla tarkoitetaan tutkimuksen luotettavuutta, jolloin tutkimuksessa saadaan toistetusti sama tulos riippumatta tutkijasta. Validiteetti puolestaan kuvaa mittarin tai menetelmän kykyä mitata kohdetta ilman systemaattisia virheitä. (Vilkka 2007, 152, 177, 179.) Laadullisen tutkimuksen osalta luotettavuutta voidaan arvioida aineiston laadun ja tutkijan aineistosta tekemän analyysin perusteella. Triangulaation avulla voidaan verrata aineistonkeruumenetelmällä saatujen tulosten

yhdenmukaisuutta muista lähteistä saatuihin tietoihin, jolloin voidaan todeta, onko tulkinta saanut vahvistusta. (Hirsjärvi & Hurme 2004, 184─190.)

Menetelmäksi valitsemani lähiesimiesten haastattelun avulla sain laajemmin ja yksityiskohtaisempaa tietoa toimintayksiköiden tilanteesta kuin esimerkiksi sähköisen tai paperisen kyselylomakkeen avulla. Haastateltavat kommentoivat, etteivät välttämättä olisi vastanneet lomakekyselyyn ja kokivat, että saivat haastattelussa paremmin oman äänensä kuuluviin. Haastattelun otos (n=22) kuvasi hyvin osastonhoitajien perusjoukkoa (N=23). Aineiston keruu tapahtui autenttisessa ympäristössään kohderyhmältä, jonka työn kehittämisestä oli kysymys. Lähiesimiestehtävissä toimivien erityistyöntekijöiden ja vastaavien mukaan ottaminen haastatteluun olisi kuitenkin saattanut tuoda lisäarvoa kehittämistyölle.

Laadin haastattelulomakkeen tämän raportin teoriaosan, aiempien tutkimusten ja kirjallisuuden sekä sairaanhoitopiirin tietoturvapoikkeamaraporttien pohjalta. Muokkasin lomaketta ohjaajien antamien kommenttien ja esitestausten perusteella. Haastattelulomake mittasi melko hyvin sitä, mitä oli tarkoituskin. Yhdessä kysymyksessä (kysymys 20) haastateltavat tulkitsivat asian eri tavoin.

Haastatteluaineiston keruu tapahtui yksilöhaastatteluna etukäteen sovittuna ajankohtana rauhallisessa paikassa. Haastateltavat saivat kysymykset nähtäväkseen, mikä helpotti kysymysten hahmottamista. Vastaukset tallensin käsin haastattelulomakkeelle, mikä sopi menetelmäksi, koska lomakkeessa oli paljon suljettuja kysymyksiä. Toisaalta haastattelun kuluessa käytiin keskustelua myös varsinaisten kysymysten ulkopuolelta, minkä tallentaminen nauhoittamalla olisi tuonut lisäarvoa tulosten analyysiin ja koko kehittämistyöhön. Vastausten siirtäminen käsin Webropol-ohjelmaan auttoi aineiston saamista mitattavaan muotoon, mutta toisaalta menetelmässä on myös mahdollisuus tallennusvirheisiin. Tämän välttämiseksi säilytin paperiset haastattelulomakkeet tarkistamista varten kehittämistehtävän valmistumiseen saakka.

Päiväkirjamerkintöjen kerääminen tapahtui osastotunneilla ja vastaavissa tilanteissa, jolloin itse toimin sekä asiantuntijana että merkintöjen kirjaajana. Merkinnät jäivät tässä tilanteessa pääkäsitteiden tasolle. Myös tulkintavirheitä on saattanut esiintyä. Käytännön kehittämisen näkökulmasta päiväkirjamerkintöjen tarkkuus oli kuitenkin riittävä ja ne tukivat muusta aineistosta nousseita kehittämistarpeita.

Tietoturvapoikkeamat olivat organisaation sisäiseen käyttöön tarkoitettua, valmiiksi kerättyä tietoa. Tässä yhteydessä käytin niitä yleisellä tasolla, mikä riitti käsityksen saamiseen kehittämistarpeista. Laajemmin tietoturvapoikkeamien osalta voidaan kuitenkin pohtia, kuvaako se organisaation todellisuutta eli onko esimerkiksi kaikki poikkeamatilanteet ilmoitettu ja kirjattu asianmukaisesti.

7.2 Kehittämisprosessin arviointi

Kehittämistehtävän toteutus osui ajankohtaan, jossa organisaatiossa tapahtui suuria tietojärjestelmiin liittyviä periaatteellisia ja toiminnallisia muutoksia. Tässä yhteydessä myös tietoturvallisuuteen ja tietosuojaan liittyviä asioita korostettiin entistä voimakkaammin. Aineiston keruu tapahtui siis tilanteessa, jossa tietoturva- ja tietosuojakoulutukset olivat jo meneillään ja muitakin alueeseen liittyviä asioita kehitettiin ja tiedotettiin aktiivisesti. Voikin pohtia, olisivatko tulokset olleet samansuuntaisia, jos kehittämistehtävä olisi suoritettu ennen muutosprosessia. Asioiden ajankohtaisuus ja niihin paneutuminen saattoi tässä vaiheessa tuoda syvällisempää tietoa kuin aiemmin.

Kehittämistehtävän suunnittelu ja toteutus tapahtui osittain yhtä aikaa esitettyjen toimenpidesuositusten suunnittelun ja toimeenpanon kanssa, muun muassa tietosuoja- ja tietoturvakoulutukset ja tiedottamisen organisointi aloitettiin jo kehittämistehtävän suunnitteluvaiheessa. Käytännön työskentelyn, teoreettisen taustan ja aineistosta nousseiden tulosten vuoropuhelu rikasti kehittämisprosessia, joskin kehittämistehtävän luotettavuutta ajatellen minun oli kehittämistyön tekijänä tärkeää erottaa tutkimusaineisto ja muualla työtilanteissa syntynyt informaatio toisistaan.

Kehittämistehtävän tulokset tukevat ja syventävät sitä kuvaa, mikä sairaanhoitopiirin tietoturvallisuudesta oli aiemmin tiedossa. Tulosten ja suositusten perusteella käytännön kehittämistoimenpiteitä voidaan kohdentaa tehokkaammin. Vaikka aineisto on kerätty pääosin hoitohenkilöstöltä, suurin osa toimenpiteistä voidaan laajentaa koskemaan myös muita henkilöstöryhmiä.

Kehittämissuositusten realistisuuden arviointi ja niiden nopea vieminen käytäntöön oli mahdollista, kun kehittäminen tapahtui kiinteänä osana organisaation toimintaa. Vuoden 2013 alussa on jo otettu käyttöön uusi tietoturvapoikkeamien raportointikäytäntö.

Verkossa Kanta-sivuilla (www.kanta.fi) suoritettava tietoturva- ja tietosuojakoulutus tuli pakolliseksi potilaiden hoitoon osallistuvalle henkilöstölle syksyllä 2012. Koulutus laajenee koskemaan muita henkilöstöryhmiä vuoden 2013 aikana. Esimiehille järjestetään räätälöityä tietoturva- ja tietosuojakoulutusta kesäkuussa 2013 alueellisena koulutuksena. Myös tietoturvallisuuden ja tietosuojan organisoinnin sekä potilastietojen käytön seurannan jatkokehittämisen suunnittelu on aloitettu.

Tietoturvallisuuden ja tietosuojan tulee nivoutua tiiviisti muuhun organisaation toimintaan, ja sen vuoksi myös kehittämistoimenpiteiden tulee kulkea käsi kädessä toiminnan kehittämisen kanssa. Tämän vuoksi kehittämistehtävän tuloksissa merkittäväksi kehittämiskohteeksi nousseen tietoverkon ja tietojärjestelmien kirjautumisratkaisujen kehittämistarve on tiedostettu, mutta kehittämistoimenpiteiden aloitus riippuu muista tietohallintoon ja tietojärjestelmiin liittyvistä ratkaisuista.

Tietoturvallisuus ja tietosuoja ovat aina olleet tärkeä osa terveydenhuollon toimintaa. Laajat kansalliset ja alueelliset palvelurakenne- ja tietojärjestelmämuutokset ovat tuoneet kuitenkin uusia paineita alueen kehittämiseen. Paineet heijastuvat myös tämän kehittämistehtävän tuloksissa. Tarvitaan uutta ohjeistusta ja osaamista, toimintaprosessien kehittämistä sekä uusia tietoteknologisia mahdollisuuksia toiminnan tueksi.

Tietoturvallisuuden ja tietosuojan tulee olla kiinteä osa organisaation päivittäistä toimintaa. Jokaisen työntekijän tehtävä on pohtia, miten perustehtävä, esimerkiksi potilaiden hoitaminen toteutetaan sujuvasti ja tietoturvallisesti. Tämän vuoksi tietoturvallisuuden ja tietosuojan seurannan ja kehittämisen tulee olla hyvin organisoitua ja perustehtävää tukevaa. Jatkossa olisikin hyvä kiinnittää huomio tietoturvallisuuteen organisaation yhtenä laatutekijänä ja kehittää sitä turvallisuuden osa-alueena laadunhallinnan periaatteiden mukaisesti.

LÄHTEET

Aarnio, Reijo 2013. Lukijalle. Teoksessa Andreasson, Ari, Koivisto, Juha & Ylipartanen, Arto. Tietosuojavastaavan käsikirja. Helsinki: Tietosanoma.

Andreasson, Ari, Koivisto, Juha & Ylipartanen, Arto 2013. Tietosuojavastaavan käsikirja. Helsinki: Tietosanoma.

Arkistolaki 831/1994. WWW-dokumentti.
http://www.finlex.fi/fi/laki/ajantasa/1994/19940831. Ei päivitystietoa. Luettu 16.5.2012.

Ensio, Anneli & Reponen, Kirsi 2005. Sähköisten työvälineiden juurruttaminen käytännön hoitoprosesseihin sekä näihin liittyvä tietoturva. Loppuraportti 27.1.2005. Kuopion yliopisto, Terveyshallinnon ja -talouden laitos. Shiftec-tutkimusyksikkö. Pdf-dokumentti. http://his.uku.fi/avointa/julkaisut/LoppuraporttiFINAL.pdf. Ei päivitystietoa. Luettu 2.3.2012.

Etelä-Savon sairaanhoitopiirin tietoturvapolitiikka 2012. Etelä-Savon sairaanhoitopiirin intranet. Päivitetty 27.6.2012. Luettu 24.10.2012.

Henkilötietolaki 523/1999. WWW-dokumentti.
http://www.finlex.fi/fi/laki/ajantasa/1999/19990523. Ei päivitystietoa. Luettu 16.5.2012.

Hirsjärvi, Sirkka & Hurme Helena 2004. Tutkimushaastattelu. Teemahaastattelun teoria ja käytäntö. Helsinki: Gaudeamus.

Jokinen, Yrjö 1999. Tietoturvallisuus. Teoksessa Saranto, Kaija & Korpela, Mikko (toim.) Tietotekniikka ja tiedonhallinta sosiaali- ja terveydenhuollossa. Helsinki: WSOY.

Kairamo, Ville 2008. Tampereen teknillinen yliopisto. Tietoturvallisuuden jatkokurssi. Tutkielma. WWW-dokumentti.
https://jop.cs.tut.fi/twiki/bin/view/Tietoturva/Tutkielmat/2008-30. Ei päivitystietoa. Luettu 2.3.2012.

Kansallinen terveysarkisto 2009. Lainsäädäntö. WWW-dokumentti.
https://www.kanta.fi/fi/lainsaadanto. Päivitetty 8.10.2009. Luettu 8.4.2012.

Kansallinen terveysarkisto 2012. Tietoturvallisuus. WWW-dokumentti.
https://www.kanta.fi/fi/tietoturvallisuus. Päivitetty 14.2.2012. Luettu 8.4.2012.

Kelan KanTa-palvelujen tietoturvapolitiikka 2011. WWW-dokumentti.
https://www.kanta.fi/c/document_library/get_file?uuid=25efb0ee-fd88-4d8d-870a-ae8a40ef10af&groupId=10206. Päivitetty 1.1.2011. Luettu 4.4.2011.

Kotisaari, Marja-Liisa & Kukkola, Sirkka 2012. Potilaan oikeudet hoitotyössä. Porvoo: Fioca Oy.

Kulppi, Marja-Leena & Lohi, Sirpa 2011. Tietoturvakulttuuri ja tietoturvan johtaminen terveydenhuollon organisaatiossa: ”Salassapidosta tietoturvaan”. Lapin yliopisto. Hallintotiede. Pro gradu -tutkielma. Tiivistelmä. WWW-dokumentti. http://doria17-kk.lib.helsinki.fi/handle/10024/69918. Päivitetty 4.7.2011. Luettu 14.2.2013.

Laki viranomaisten toiminnan julkisuudesta 621/1999. WWW-dokumentti. http://www.finlex.fi/fi/laki/ajantasa/1999/19990621. Ei päivitystietoa. Luettu 5.4.2012.

Nykänen, Kari 2011. Tietoturvakoulutuksen vaikuttavuuden arviointi yksilön ja organisaation tietoturvakäyttäytymiseen. Oulun yliopisto. Luonnontieteellinen tiedekunta. Tietojenkäsittelytieteen laitos. Väitöskirja. Pdf-dokumentti. http://herkules.oulu.fi/isbn9789514295713/isbn9789514295713.pdf. Päivitetty 2.11.2011. Luettu 25.3.2013.

Reponen, Kirsi 2006. Terveydenhuollon organisaation tietoturvallisuus henkilöstön arvioimana. Kuopion yliopisto. Terveyshallinnon ja –talouden laitos. Terveyshallintotiede. Sosiaali- ja terveydenhuollon tietohallinto. Pro gradu -tutkielma.

Sosiaali- ja terveysalan lupa- ja valvontavirasto 2012. Hyvä tiedonhallintatapa ja tietosuoja. WWW-dokumentti. http://www.valvira.fi/ohjaus_ja_valvonta/terveydenhuolto/salassapito/hyva_tiedonhallintatapa_ja_tietosuoja. Ei päivitystietoa. Luettu 5.4.2012.

Sosiaali- ja terveysministeriö 2010. Tietoturvapolitiikan malli terveydenhuollon organisaatioille. WWW-dokumentti. https://www.kanta.fi/c/document_library/get_file?uuid=52c6d712-145d-4d61-b7d4-91ff054efa8b&groupId=10206. Ei päivitystietoa. Luettu 4.4.2012.

Tammisalo, Tero 2005. Sosiaali- ja terveydenhuollon tietojärjestelmien tietoturvan ja tietosuojan hallinnan periaatteet ja hyvät käytännöt. Ohje sosiaali- ja terveydenhuollon organisaatioille ja toimintayksiköille tietojärjestelmien tietoturvan ja tietosuojan kehittämiseksi. Stakes. Raportteja 5/2005. Helsinki: Stakes.

Tilastokeskus 2006. Virsta – virtual statistics. Verkko-oppimateriaali opettajille. WWW-dokumentti. http://www.stat.fi/virsta/tkeruu/04/02/. Päivitetty 27.1.2006. Luettu 12.10.2012.

Tuomi, Jouni & Sarajärvi, Anneli 2009. Laadullinen tutkimus ja sisällönanalyysi. Helsinki: Tammi.

Valtionhallinnon tietoturvallisuuden johtoryhmä 2003. Opas julkishallinnon tietoturvakoulutuksen järjestämisestä 6/2003. Pdf- dokumentti. http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/53763/53760_fi.pdf. Päivitetty 29.12.2003. Luettu 9.3.2012.

Valtionhallinnon tietoturvallisuuden johtoryhmä 2008. Tietoturvallisuus on asenne. Selvitys julkishallinnon tietoturvakoulutustarpeista 6/2008. Pdf- dokumentti. http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20081211Tietot/vahti6_taitto_NETTI_%2b_KANNET.pdf. Päivitetty 11.12.2008. Luettu 9.3.2012.

Valtiovarainministeriö 2007. Tietoturvallisuudella tuloksia. Yleisohje tietoturvallisuuden johtamiseen ja hallintaan. Vahti 3/2007. Pdf-dokumentti. http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20071128Tietot/vahti3_07_netti.pdf. Päivitetty 29.11.2007. Luettu 28.3.2013.

Valtiovarainministeriö 2008. Tärkein tekijä on ihminen - henkilöstöturvallisuus osana tietoturvallisuutta. WWW-dokumentti. https://www.vahtiohje.fi/c/document_library/get_file?uuid=af5614a4-fa44-482c-9886-0af9e6a13929&groupId=10128&groupId=10229. Päivitetty 17.2.2008. Luettu 4.4.2012.

Vilkka, Hanna 2005. Tutki ja kehitä. Helsinki: Tammi.

Winblad, Ilkka, Reponen, Jarmo & Hämäläinen, Päivi 2012. Tieto- ja viestintäteknologian käyttö terveydenhuollossa vuonna 2011. Tilanne ja kehityksen suunta. Terveyden ja hyvinvoinnin laitoksen raportti 3/2012. Pdf-dokumentti. http://www.thl.fi/thl-client/pdfs/825d0af8-f97c-4192-bf5b-ba5e1bf773aa. Päivitetty 16.3.2012. Luettu 23.3.2013.

Ylipartanen, Antero 2010. Tietosuoja terveydenhuollossa. Potilaan asema ja oikeudet henkilötietojen käsittelyssä. Helsinki: Tietosanoma.

LIITE 1. Kehittämisprosessi ja aikataulu