HOITOHENKILÖSTÖN TIETOSUOJA- JA TIETOTURVATIETÄMYS

Pirjo Jokelainen

Pro gradu -tutkielma

Sosiaali- ja terveydenhuollon tietohallinto

Itä-Suomen yliopisto

Sosiaali- ja terveysjohtamisen laitos

Marraskuu 2011

ITÄ-SUOMEN YLIOPISTO, yhteiskuntatieteiden ja kauppatieteiden tiedekunta
Sosiaali- ja terveysjohtamisen laitos, sosiaali- ja terveydenhuollon tietohallinto

JOKELAINEN PIRJO: Hoitohenkilöstön tietosuoja- ja tietoturvatietämys

Pro gradu -tutkielma, 77 sivua, 1 liite (11 sivua)

Tutkielman ohjaajat: TtT Anneli Ensio, YTM Sirpa Kuusisto-Niemi

Marraskuu 2011

Avainsanat: terveydenhuolto, tietoturva, tietosuoja, tietämys, osaamisen johtaminen (YSA)

Tietoverkkojen välityksellä tapahtuva tietojen reaaliaikainen käyttö ja siirto terveydenhuollon organisaatioissa ovat nykypäivää tietoteknistyneessä terveydenhuollon ympäristössä. Lainsäädännön ja normien määrittämät tietosuojan yleiset vaatimukset ja edellytykset sekä henkilötietojen tietoturvasta huolehtiminen säätelevät tätä tiedonhallintaa. Teknologian nopean kehityksen ohella myös muutokset lainsäädännössä ovat tuoneet uusia haasteita potilasasiakirjojen käsittelylle. Terveydenhuollossa lisääntynyt henkilötietojen turvallinen käsittely on keskeisessä asemassa. Entistä tärkeämmäksi tulee henkilöstön tietoturva- ja tietosuojatietoisuus sekä osaaminen tiedon hallinnan prosessin kaikissa vaiheissa. Tieto henkilöstön osaamisen nykytilasta ja tulevaisuuden osaamisvaatimuksista luo perustan osaamisen suunnitelmalliselle johtamiselle henkilöstön osaamisen hyödyntämiseksi ja kehittämiseksi.

Tutkimus toteutettiin sähköpostikyselynä ja sen kohderyhmänä oli Kainuun maakunta -kuntayhtymän perusterveydenhuollossa sekä erikoissairaanhoidossa työskentelevä hoitohenkilöstö, joka käyttää työssään potilastietojärjestelmiä. Tarkoituksena oli hankkia tietoa organisaation hoitohenkilöstön omasta tämänhetkisestä käsityksestään tietoturva- ja tietosuojatietämyksestä sekä –osaamisesta usealta eri osa-alueelta: yleisen tietosuojan ja tietoturvan, potilastietojen käsittelyn, suostumuksen hallinnan, henkilöstöturvallisuuden sekä käyttöturvallisuuden näkökulmasta. Tavoitteena oli näin saada kokonaiskuva siitä, millaista osaamista organisaatiossa on tällä hetkellä.

Tutkimustulosten mukaan hoitohenkilöstön tietosuoja- ja tietoturvatietämys ja osaaminen olivat pääsääntöisesti hyvät. Eniten epätietoisuutta esiintyi tietojen luovutuskäytäntöjen periaatteista muun muassa viranomaisille ja omaisille. Vaikka henkilöstöllä näyttäisikin olevan hyvät valmiudet tietoturvalliseen tiedon hallintaan, lisäkoulutuksen ja toimintatapojen yhtenäisen ohjeistuksen sekä tiedottamisen tarve on ilmeinen liittyen organisaatiossa paraikaa menossa olevaan potilastietojärjestelmien yhtenäistämishankkeeseen. Tutkimuksessa saatu tieto on hyödynnettävissä muun muassa kartoitettaessa kyseisen toimintaympäristön muutoksen mahdollisesti tuomia uusia tietoturvauhkia ja –vaatimuksia, arvioitaessa henkilöstön koulutuksen tarvetta sekä perehdytettäessä uusia työntekijöitä. Tietoturvallisen toiminnan vaikuttavuuden arvioimiseksi ja tueksi tarvitaan tulevaisuudessakin palautetta henkilöstön tietämyksen tasosta ja koulutuksen vaikuttavuudesta

UNIVERSITY OF EASTERN FINLAND, Faculty of Social Sciences and Business Studies, Department of Health and Social Management, Health and Human Services Informatics

JOKELAINEN, PIRJO: Information data privacy and security awareness of nursing staff

Master's thesis, 77 pages, 1 appendice (11 pages)

Advisors: PhD, Anneli Ensio, M.Sc, Sirpa Kuusisto-Niemi

November 2011

Keywords: health, security, privacy, knowledge, knowledge management (YSA)

The information networks, the use and the transfer of real-time information within healthcare delivery organizations are the modern world in today's computerized healthcare environment. The general requirements and conditions defined by legislation and data protection standards as well as confidentiality and data security, regulate this management of information. The rapid expansion of computer driven technologies, but also changes in legislation have brought new challenges for handling patient records. The increased processing of personal data safely in healthcare plays a key role. Personnel data security and protection awareness and knowledge will become increasingly important in knowledge management process at all stages. The knowledge of nursing staff skills current state and future skills requirements provides the basis for management of knowledge, that allows employees' skills utilization and developing.

This study was conducted by e-mailed questionnairy and the target group consisted of the Joint Authority of Kainuu Region primary healthcare and specialized medical healthcare employees, who use patient information in their work.The purpose of this study was to get information about the nursing staff's own understanding concerning their current data security knowledge and awareness of the data protection from several different areas: from the perspective of the general data protection and data security, patient information handling, consent management, human security as well as operational safety. The aim was thus to obtain an overall picture of what knowledge the organization currently has.

According to the results privacy and data security awareness and knowledge of the nursing staff were generally good. Uncertainty appeared mostly in practices and principles concerning the disclosure of information to other authorities and relatives. Although the nursing staff seems to be well prepared for secure information management, the need for additional education and practice guidelines as well as integrated information is obvious related to the ongoing harmonization of the patient information systems in the organization. The findings of this study can be utilized in, among other things, identifying potential future threats and requirements, assessing the need for nursing staff training and familiarizing new employees. The feedback on the level of staff awareness and training effectiveness is also needed to evaluate the effectiveness of the data security strategy and to support the security policy.

SISÄLTÖ

KUVIOT

TAULUKOT

1 JOHDANTO

Toimintojen ja palveluiden laatu, tehokkuus ja avoimuus sekä kansalaisten etu ja oikeudet edellyttävät hyvän hallinnon periaatteiden mukaista tietoturvallisuuden toteutumista tietojen, niiden käsittelyn, hallinnan ja käytön turvaamiseksi. Muun muassa Valtioneuvoston julkaisemalla periaatepäätöksellä valtionhallinnon tietoturvallisuuden kehittämisestä (Valtiovarainministeriö 2009) pyritään ohjaamaan tietoturvallisuuden kehittämistä osana johtamista, osaamista, riskienhallintaa, hallinnon kehittämistä sekä toimintaa valtionhallinnon ja muiden organisaatioiden kuten kuntien, yritysten ja yhteisöjen välisessä toiminnallisessa sekä tiedon hallinnan yhteistyössä. Viranomaisten tulee taata riittävän hyvän tietoturvallisuuden ja henkilötietojen suojan toteutuminen niin omassa organisaatiossa kuin hankittaessa palveluja organisaation ulkopuolelta. Yhtenä kehittämisperiaatteena vastuullisuuden, laillisuuden, yhteistyön, integroinnin ja kansainvälisen yhteistyön lisäksi periaatepäätöksessä mainitaan osaaminen, henkilöstöllä tulee olla tehtäviensä ja valtion tietoturvavaatimusten edellyttämä osaaminen. (Valtiovarainministeriö 2009.)

Terveydenhuollossa henkilötietojen turvallinen käsittely niiden arkaluonteisuuden ja käyttötarkoituksen vuoksi sekä tiedonhallinta yleensäkin ovat keskeisessä asemassa. Terveydenhuollon toiminta ja päätöksenteko perustuvat tietoon. Tiedonhallinnan tavoitteena on tiedon tuottaminen terveydenhuollon toimintayksiköille tätä tarkoitusta varten. Potilastietojen käsittely on siten osa palvelutapahtumaa, jonka tarkoituksena on potilaan tutkimusten ja hoidon järjestäminen, toteuttaminen ja seuranta. Keskeisiä ovat tiedon tarpeiden tunnistaminen, tiedonhankinta, tiedon organisointi ja varastointi, tietotuotteiden ja –palveluiden kehittäminen tiedonjakeluun sekä tiedon käyttö ja toiminnan mukauttaminen. Lainsäädännön ja normien määrittämät tietosuojan yleiset vaatimukset ja edellytykset sekä henkilötietojen tietoturvasta huolehtiminen säätelevät tätä palvelutapahtuman tiedonhallintaa. (Saranto 2007, 25 – 26; Ylipartanen 2010, 23 – 25.)

Tietotekniikan kehittyessä tieto, tiedon siirto sekä käsittely tapahtuvat yhä useammin sähköisesti. Potilastietojen käsittelyssä on käytössä yhä laajemmin sähköisiä tietojärjestelmiä manuaalijärjestelmien rinnalla. Tietoverkkojen välityksellä tietojen reaaliaikainen käyttö ja siirto sairaaloiden, terveyskeskusten sekä muiden terveydenhuollon toimintayksiköiden sisällä ja välillä ovat nykypäivää. Tiedon lisääntynyt määrä asettaa omat haasteensa oikean tiedon löytämiselle ja käsittelylle. Hyvä tiedonhallintatapa on-

kin noussut entistä keskeisemmäksi periaatteeksi. (Kleemola & Tervo-Pellikka 1998, 3; Ylipartanen 2010, 21,27.)

Terveydenhuollon salassa pidettäville tiedoille asetetut tietosuojan ja tietoturvan erityisvaatimukset tulee huomioida sovellusten ja tiedonsiirron käytössä. Tiedot ja tiedonvälitys tulee suojata ja turvata vaarantamatta tietojen olemassaoloa, oikeellisuutta, käytettävyyttä, luottamuksellisuutta, muuttumattomuutta sekä palveluiden saumattomuutta ja jatkuvuutta. (Kleemola ym. 1998, 16 – 17.) Virheettömyysvaatimuksen sekä luottamuksellisuus- ja huolellisuusvelvoitteen korostuminen terveydenhuollon potilassuhteissa lisäävät tietosuojan ja -turvan merkitystä. Sähköisessä muodossa oleva tieto on myös alttiimpaa erilaisille tietoturvaloukkauksille. Potilaan hoidon kannalta tarpeellisen ja riittävän tiedon saanti ja turvallinen siirto takaavat laadultaan hyvät terveyspalvelut ja parantavat näin myös omalta osaltaan potilasturvallisuutta. (Ylipartanen 2010, 25.)

Teknologian nopean kehityksen ohella muutokset lainsäädännössä ovat myös tuoneet uusia haasteita potilasasiakirjojen käsittelylle. Tästä johtuen sosiaali- ja terveysministeriö on uudistamassa terveydenhuoltohenkilöstölle tarkoitetun vuonna 2001 julkaisemansa Potilasasiakirjojen laatiminen sekä niiden ja muun hoitoon liittyvän materiaalin säilyttäminen –nimisen oppaan (Sosiaali- ja terveysministeriö 2001) sekä siihen liittyvän tarkentavan ohjeistuksen. Kyseiseen oppaaseen on koottu lainsäädännön normit ja yleinen kehys liittyen potilasasiakirjojen käsittelyyn tavoitteena kokonaiskuvan luominen lainsäädännön asettamista vastuista, velvoitteista ja edellytyksistä potilasasiakirjojen käsittelyssä. (Sosiaali- ja terveysministeriö 2010.)

Kainuun maakunta- kuntayhtymässä ollaan siirtymässä kolmesta eri sähköisestä potilastietojärjestelmästä yhteen yhtenäiseen potilastietojärjestelmään tavoitteena järjestelmän kattaminen koskemaan koko maakunnallista organisaatiota – sekä perusterveydenhuoltoa että erikoissairaanhoitoa. Kyseinen käyttöönottohanke on paraikaa menossa. Tavoitteena on ottaa yhtenäinen järjestelmä käyttöön vuoden 2011 aikana. Siirtyminen tulee olemaan suuri haaste ja muutos henkilöstölle. Tarvitaan uudenlaista osaamista, uusien toimintatapojen omaksumista ja ennen kaikkea myönteistä asennetta muutoksia kohtaan. Muutos tuo mukanaan uusia haasteita, vaatimuksia ja rajoitteita erityisesti tietoturvan ja tietosuojan toteutumiselle. Entistä tärkeämmäksi tulee henkilöstön tietoturva- ja tietosuojatietoisuus sekä osaaminen tiedon hallinnan prosessin eri vaiheissa. Miten taa-

taan turvallinen lainsäädännön vaatimusten mukainen tietojen salassapito, käsittely ja luovuttaminen?

Aihealueelta on toistaiseksi vielä olemassa vähän tutkittua tietoa, joten siinäkin mielessä tutkimus on ajankohtainen ja tarpeellinen. Toisaalta kansalliseen sähköiseen arkistoon siirtyminen tuo uusia vaatimuksia henkilöstön tietosuoja- ja tietoturvaosaamiselle organisaatioissa. Toisaalta kansalaisten valveutuneisuus omista oikeuksistaan ja mahdollisuuksistaan omien tietojen tarkasteluun lisää henkilöstön osaamisen ja tietämyksen merkitystä.

Tässä tutkimuksessa tarkoituksena oli hankkia tietoa organisaation hoitohenkilöstön tämänhetkisestä tietoturva- ja tietosuojatietämyksestä ja –osaamisesta ennen uuden yhtenäisen järjestelmän lopullista käyttöönottoa kuvaamalla hoitohenkilöstön tietoturva- ja tietosuojatietämyksen ja –osaamisen taso henkilöstön itsensä arvioimana. Tavoitteena oli saada kokonaiskuva nykyosaamisesta, siitä, millaista osaamista organisaatiossa on tällä hetkellä. Saadut tulokset tullaan esittelemään ja käyttämään oheismateriaalina organisaation järjestämissä henkilöstön tietosuoja- ja tietoturvakoulutuksissa ja lisäksi tulokset julkaistaan organisaation sisäisellä Intranet-sivustolla. Dokumentoidut osaamiskuvaukset tuovat näin tietosuoja- ja tieturvaosaamisen näkyväksi, organisaation yhteiseksi asiaksi. Saatu tieto on hyödynnettävissä muun muassa haluttaessa myöhemmin kartoittaa uuden toimintamallin mukanaan tuomia mahdollisia tietoturvauhkia ja -vaatimuksia ja sen pohjalta arvioitaessa henkilöstön koulutuksen tarvetta tietoturva- ja tietosuojaosaamisen varmistamiseksi uudessa toimintaympäristössä. Tietoa voidaan hyödyntää myös uusien työntekijöiden perehdyttämisessä arvioitaessa heidän tietosuoja- ja tietoturvaosaamistaan ja tietämystään.

2 TERVEYDENHUOLLON TIETOJEN LAINMUKAINEN JA LUOTTAMUKSELLINEN KÄSITTELY

Terveydenhuollossa salassapito liittyy olennaisesti luottamukselliseen asiakas- ja potilassuhteeseen. Osallistuessaan potilaan hoitoon tai ollessaan tekemisessä potilasta koskevien tietojen kanssa terveydenhuollon henkilöstöä koskee salassapitovelvollisuus, joka säilyy ammatinharjoittamisen päättymisen jälkeenkin. Lähtökohtana on, että kaikki potilasta koskevat tiedot ovat salassa pidettäviä. Luottamuksellisuus edellyttää, etteivät potilaalta tai muista tietolähteistä saadut tiedot joudu laittomasti asiaankuulumattomien tietoon. Salassa pidettäviä tietoja voidaan luovuttaa vain potilaan tai tietyissä tapauksissa hänen laillisen edustajan antamalla suostumuksella tai lakiin perustuvalla oikeudella. (Lohiniva-Kerkelä 2007, 159 - 162; Pahlman 2007, 26 – 27; Pahlman 2010, 11, 24. – 25; Ylipartanen 2010, 66 – 67, 70.)

Asiakirjasalaisuus, vaitiolovelvollisuus ja salassa pidettävien tietojen hyväksikäyttökielto sisältyvät salassapitovelvollisuuteen. Asiakirjasalaisuudella käsitetään velvollisuutta pitää salassa pidettävä asiakirja salassa näyttämättä ja luovuttamatta asiakirjaa, sen kopiota tai tulostetta sivulliselle sekä antamatta sitä teknisen käyttöyhteyden tai muun vastaavan avulla sivullisen nähtäväksi tai käytettäväksi. Sivullisella tarkoitetaan kyseisessä terveydenhuollon toimintayksikössä tai sen toimeksiannosta muuta kuin potilaan hoitoon tai siihen liittyvien tehtävien hoitoon osallistuvaa henkilöä (PotL 13.2§). Vaitiolovelvollisuus puolestaan on asiakirjasalaisuutta laajempi velvoite, se koskee myös tallentamattomia, suullisesti saatuja tietoja tai omiin havaintoihin pohjautuvia tietoja. Se, mitä on säädetty asiakirjasalaisuudesta, koskee yleensä myös vaitiolovelvollisuutta. Hyväksikäyttökielto sisältää kiellon käyttää salassa pidettäviä tietoja omaksi tai toisen hyödyksi. (Lohiniva- Kerkelä 2007, 161; Pahlman 2007, 16, 25 – 26; Ylipartanen 2010, 66 - 67, 69.)

Hoitohenkilökunnan käsitellessä potilaiden henkilötietoja potilaan tietosuoja ei ole pelkästään salassapitovelvollisuuden noudattamista. Tarkoituksena ei ole ensisijaisesti niinkään suojata tietoa ja tietoja vaan henkilön, potilaan tai asiakkaan oikeutta yksityisyyteen, luottamukselliseen potilassuhteeseen ja itsemääräämisoikeuteen. Hyvä tietojenkäsittelytapa mahdollistaa potilastietojen suojaamisen hoitosuhteeseen nähden sivul-

lisilta, toisaalta se takaa hoitoon osallistuvien tarvitsemien tietojen saatavuuden. (Ylipartanen 2010, 21, 23 – 24.)

2.1 Tietosuoja terveydenhuollossa

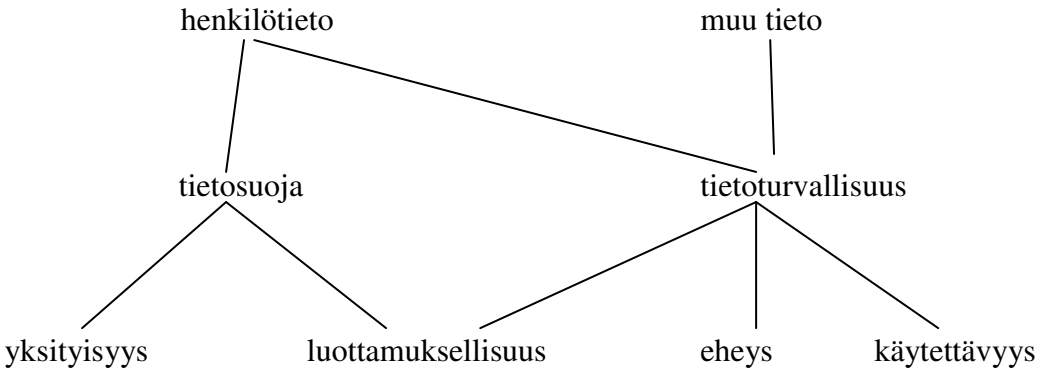
Tietosuojalla tarkoitetaan henkilötietolain (523/1999) vaatimusten huomioon ottamista henkilötietoja käsiteltäessä (muun muassa kerätä, tallettaa, käyttää, siirtää, luovuttaa, säilyttää ja hävittää) tavoitteena varmistaa yksityisten henkilöiden yksityisyys, edut ja oikeusturva. *Henkilötiedoilla* tarkoitetaan kaikkia niitä henkilöä tai hänen ominaisuuksia koskevia merkintöjä, joiden avulla hänet, hänen perheensä tai hänen kanssaan yhteisessä taloudessa elävät voidaan tunnistaa. Käyttötarkoituksensa vuoksi yhteenkuuluvista merkinnöistä muodostuvaa henkilötietoja sisältävää tietojoukkoa kutsutaan puolestaan *henkilörekisteriksi*. (Kerko 2001, 251; Kleemola ym. 1998, 6; Pahlman 2007, 9, 13, 23, 148; Ylipartanen 2010, 18- 19, 23.)

Terveydenhuollossa tietosuojan tavoitteena on hyvän käsittelytavan luominen ja toteuttaminen henkilötietojen käsittelyn kaikissa vaiheissa. Tarkoituksena on potilaiden oikeuksien kunnioittaminen ja toteuttaminen, toisaalta myös oikeusturvan varmistaminen niin rekisteröidyn kuin rekisterinpitäjänkin näkökulmasta. *Rekisteröity* on henkilö, jota henkilötieto koskee ja *rekisterinpitäjällä* tarkoitetaan henkilöä, yhteisöä, laitosta tai säätiötä, jonka käyttöön henkilörekisteri perustetaan ja jonka oikeutena on määrätä kyseisen rekisterin käytöstä. (Ylipartanen 2010, 23 – 24.) Potilasasiakirjojen, kuten muun muassa potilaskertomuksen, ajanvarauspäiväkirjojen ja laboratoriolähetteiden rekisterinpitäjä on terveydenhuollon toimintayksikkö, se voi olla myös itsenäisesti ammattiaan harjoittava terveydenhuollon ammattihenkilö (Pahlman 2010, 15, Ylipartanen 2010, 19 - 20). Potilaiden henkilötietojen lainmukaisen käsittelyn edistämiseksi näiden tietojen käsittelyyn liittyviin rikosoikeudellisiin vastuisiin ja vahingonkorvausvastuuseen kohdistuvia säännöksiä on sisällytetty useisiin lakeihin (Ylipartanen 2010, 167).

2.2 Tietoturva terveydenhuollossa

Tietoturvallisuudella tarkoitetaan yksityisyyden, ennen kaikkea tiedon laadun ja eheyden koskemattomuuden säilyttämiseen ja suojaamiseen kohdistuvia toimenpiteitä (Ylipartanen 2010, 18). Tietoturvallisuus liittyy keskeisesti riskienhallintaan, hallintoon ja

palveluihin, kehittämiseen, resurssien suunnitteluun sekä toiminnan sisäiseen että ulkoiseen tarkastukseen. Nämä edellyttävät hyviin käytäntöihin perustuvaa tietoturvallisuuden jatkuvaa kehittämistä. Kehittämisessä korostuu muun muassa vastuullisuusperiaate, osaamisperiaate ja laillisuusperiaate. Jokaisella toimijalla on vastuu oman toimintansa ja järjestelmiensä tietoturvallisuudesta. Osaamisperiaatteella korostetaan tietoturva- ja varautumisosaamista, tehtävien edellyttämä tietoturvaosaaminen tulee olla koko henkilöstön perustaito. Laillisuusperiaate edellyttää puolestaan toimimaan kansallisen lainsäädännön ja Suomea koskevien kansainvälisten tietoturvavelvoitteiden edellyttämällä tavalla. Viranomaisten tietoturvavelvoitteita sisältävien monien lakien, asetusten ja määräysten mukaisesti tulee huolehtia tietojen luottamuksellisuudesta, eheydestä, käytettävyydestä ja saatavuudesta. (Valtiovarainministeriö 2009, 9, 26.) Tietoturvallisuuden toteuttamisen, siinä käytettävien menetelmien ja teknologioiden tavoitteena on pyrkiä toteuttamaan tietosuojaa (Ylipartanen 2010, 18). Tietoturvaa lisäävät tekniset ja toiminnalliset järjestelyt parantavat samalla myös tietosuojaa. Varmistamalla muun muassa tietojen luottamuksellisuus estetään ulkopuolisia käyttämästä keräämiään tietoja. Tietosuoja ja tietoturva liittyvät näin läheisesti toisiinsa. (Järvinen 2002, 21.) (Kuvio 1).



KUVIO 1. Tietosuoja ja tietoturvallisuus: kohteita ja painopisteitä (Valtiovarainministeriö 2003, 50).

Tietoturvallisuus on kokonaisuus, johon sisältyy tietojen, järjestelmien, palveluiden ja tietoliikenteen suojaaminen hallinnollisilla, teknisillä ja muilla toimenpiteillä. Se ei kuitenkaan koostu pelkästään teknisistä ratkaisuista ja turvatoiminnan yleisistä järjestelyistä vaan siihen sisältyy keskeisesti myös ihmisen toimintaan liittyvät turvallisuustekijät. (Valtiovarainministeriö 2004a, 9, 15.) Tietoturvan tärkeimpiä vaatimuksia ovat tiedon käytön mahdollistaminen ja turvaaminen, suojaamisen kohteena ovat tietoihin liittyvät

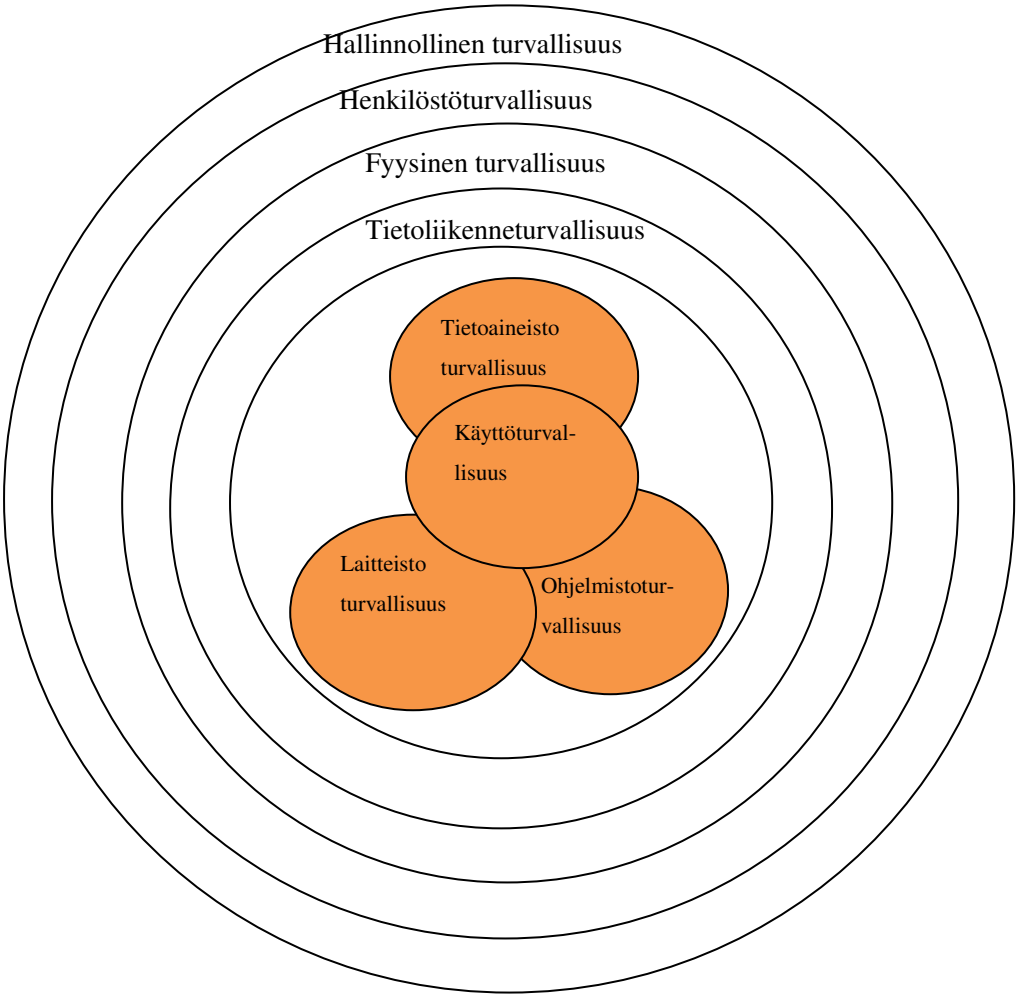
sellaiset ominaisuudet kuten *luottamuksellisuus*, *eheys*, *todentaminen, kiistämättömyys ja käytettävyys* (Järvinen 2002, 22; Paavilainen 1998, 8; Ruohonen 2002, 2; Tammisalo 2005, 7- 8;Valtiovarainministeriö 2004b, 22).

Luottamuksellisuuden vaatimus toteutuu silloin, kun tiedot ovat vain niiden käyttöön oikeutettujen henkilöiden ja organisaatioiden käytettävissä. Hyvä luottamuksellisuus edellyttää tietojen luokittelua niiden luottamuksellisuuden mukaisesti, tietojen käyttäjien tunnistamis- ja todentamismahdollisuutta sekä tietojen luovuttamista koskevien sääntöjen määrittelyä. (Kerko 2001, 224; Järvinen 2002, 22; Miettinen 1999, 25; Paavilainen 1998, 8-9; Tammisalo 2005, 8.) Tieto voidaan luokitella julkiseen ja salassa pidettävään tietoon ja nämä edelleen jakaa erittäin salaiseen, salaiseen ja luottamukselliseen tietoon. Tietojärjestelmien käyttäjien tunnistaminen ja todentaminen tapahtuu käytännössä esimerkiksi käyttäjätunnusten ja salasanojen tai toimikorttien avulla. Henkilön asemaan, työtehtäviin tai rooliin perustuvat käyttövaltuudet puolestaan antavat oikeuden muun muassa luoda, muuttaa tai tuhota asiakirja. (Tammisalo 2007, 38 – 69.)

Eheydellä tarkoitetaan tietojen totuudenmukaisuutta. Tiedot eivät synny tai häviä itsestään, ne säilyvät virheettöminä alkuperäisessä muodossaan koko tiedon elinkaaren sekä tietojenkäsittelyn eri vaiheissa. Tietojen eheys on kunnossa, kun niiden alkuperäisyys, koskemattomuus ja kiistämättömyys kyetään varmistamaan. (Kerko 2001, 224; Järvinen 2002, 22 – 23; Miettinen 1999, 26; Paavilainen 1998, 10 – 11; Ruohonen 2002, 3.) Tietojen aitous ja alkuperäisyys voidaan todentaa muun muassa liittämällä tietojen olemassaoloon tekijä ja tekoaika (Järvinen 2002, 28; Tammisalo 2007, 68).

Käytettävyys tarkoittaa tietojen ja niiden muodostamien palvelujen oikea aikaista käytettävyyttä tai saatavuutta niihin oikeutetuille henkilöille. Käytettävyyteen vaikuttavat hyvin monet eri tekijät, kuten tiedon luottamuksellisuus, laitteiston määrä, ohjelmistolisenssit, tietoliikennekapasiteetti, häiriöt laitteistoissa, ohjelmistoissa ja tietoliikenteessä, käyttäjien toiminta, oheismateriaalin saatavuus sekä huolto- ja tukitoimintojen tehokkuus. (Paavilainen 1998, 23 – 25; Tammisalo 2007, 68.) Tietojen tallentaminen yksiselitteisesti luettavaan ja ymmärrettävään muotoon on myös käytettävyyttä (Järvinen 2002, 24; Tammisalo 2005, 7-8).

Tietoturvallisuus on laaja käsite, jota voidaan tarkastella eri osa-alueiden kautta. Kyseinen lähestymistapa auttaa paremmin ymmärtämään, mitä tietoturvallisuudella tarkoitetaan, mistä se koostuu ja miten se vaikuttaa päivittäiseen toimintaan. Tietoturvallisuus voidaan jakaa *hallinnolliseen turvallisuuteen*, *henkilöturvallisuuteen*, *fyysiseen turvallisuuteen*, *tietoliikenneturvallisuuteen*, *tietoaineistoturvallisuuteen*, l*aitteistoturvallisuuteen*, *ohjelmistoturvallisuuteen* sekä *käyttöturvallisuuteen*. (Miettinen 1999, 15 – 16; Paavilainen 1998, 7 – 8, 26; Ruohonen 2002, 4.) (Kuvio 2).



KUVIO 2. Tietoturvallisuuden tasot (Paavilainen 1998, 26).

Hallinnollinen turvallisuus on kokonaisuus, joka muodostuu johtamisesta, tietoturvatoiminnan järjestelyistä, tehtävien ja vastuiden määrittelystä, henkilöstön ohjeistuksesta, koulutuksesta ja valvonnasta (Valtiovarainministeriö 2004a, 15). Lähtökohtana tulisi olla organisaation laatimat ja dokumentoidut tietosuoja- ja tietoturvapolitiikat, joista

ilmenee tietojenkäsittelyn turvaamisen tavoitteet, periaatteet ja käytännön tietoturvatoiminnan menettelytavat. Kun organisaatiossa koko henkilöstön tiedossa ja saatavilla on selkeät säännöt ja hyväksytyt menettelytavat tietoturvaturvallisuuden toteuttamiseen, mahdollistetaan tällöin paremmin myös niiden mukainen toiminta riskien hallitsemiseksi ja niiltä suojautumiseksi. Organisaation on myös jatkuvasti ylläpidettävä osaamistaan henkilöstön tietoturvaosaamisen varmistamiseksi riittävällä koulutuksella ja säännöllisellä tiedottamisella. (Kerko 2001, 234; Paavilainen 1998, 84 – 85; Tammisalo 2005, 20, 25.)

Henkilöstöturvallisuudella on keskeinen merkitys tietojen turvaamisessa, se koskettaa kaikkia työntekijöitä. Sillä tarkoitetaan toimenkuvien, käyttöoikeuksien ja koulutuksen avulla tapahtuvaa henkilöstöön liittyvien tietoturvariskien hallintaa. Se on henkilöstöön liittyvien salassapito- ja käytettävyysriskien hallintaa, jonka haasteena on suojata tietoa ja turvata sen saanti. Henkilöstön on todettu olevan suurin riskitekijä organisaation menettelytapojen ohella, henkilöstöturvallisuuden tavoitteena onkin estää inhimillisestä joko tahattomasta tai tahallisesta toiminnasta aiheutuvat tietoturvavahingot. Toiminta painottuu riskien ennakointiin ja niiden synnyn estämiseen suunnitelmallisesti ja järjestelmällisesti ohjeistamalla, kouluttamalla, kehittämällä työmenetelmiä ja vaikuttamalla asenteisiin. (Paavilainen 1998, 87 -89, 94; Tammisalo 2005, 36; Valtiovarainministeriö 2008a, 11 – 12, 14, 19.)

Fyysinen turvallisuus käsittää tietotekniikan vaatiman fyysisen käyttöympäristön ja muun muassa toimitilojen suojaamisen (Paavilainen 1998, 95; Ruohonen 2002, 4; Valtiovarainministeriö 2004a, 15). Tavoitteena on ehkäistä valtuudettomasta pääsystä organisaation tiloihin, tietoihin ja tietojärjestelmiin tai fyysisestä ympäristöstä aiheutuvia riskejä ja vahinkoja. Valtuudettomasta tietoihin pääsystä aiheutuvien uhkien ennaltaehkäisyn kannalta oleellisia ovat pääsynhallintaan liittyvät määrittelyt ja toimenpiteet, kuinka määritellään tietojen käyttö ja käyttäjät, miten käyttöoikeuksia ja –valtuuksia hallitaan sekä miten käyttäjät tunnistetaan ja miten heidän henkilöllisyytensä todennetaan. (Kerko 2001, 245; Tammisalo 2005, 43; Valtiovarainministeriö 2004b, 47.)

Tietoliikenneturvallisuus sisältää toiminnot, joiden avulla pyritään takaamaan tietoliikenteen turvallisuus (Paavilainen 1998, 108; Ruohonen 2002, 4). Siihen sisältyvät muun muassa käytön valvonta, verkon hallinta, viestinnän salaus ja varmistaminen, tietotur-

vapoikkeaminen hallinta sekä tietoliikenneohjelmien testaus ja hyväksyminen. *Laitteistoturvallisuus* puolestaan koostuu muun muassa laitteistojen suojauksesta, asennuksesta, ylläpidosta sekä niihin liittyvästä hallinnoinnista tavoitteenaan turvata laitteistot ja tukipalvelut koko elinkaaren ajan. (Valtiovarainministeriö 2007,61,63.)

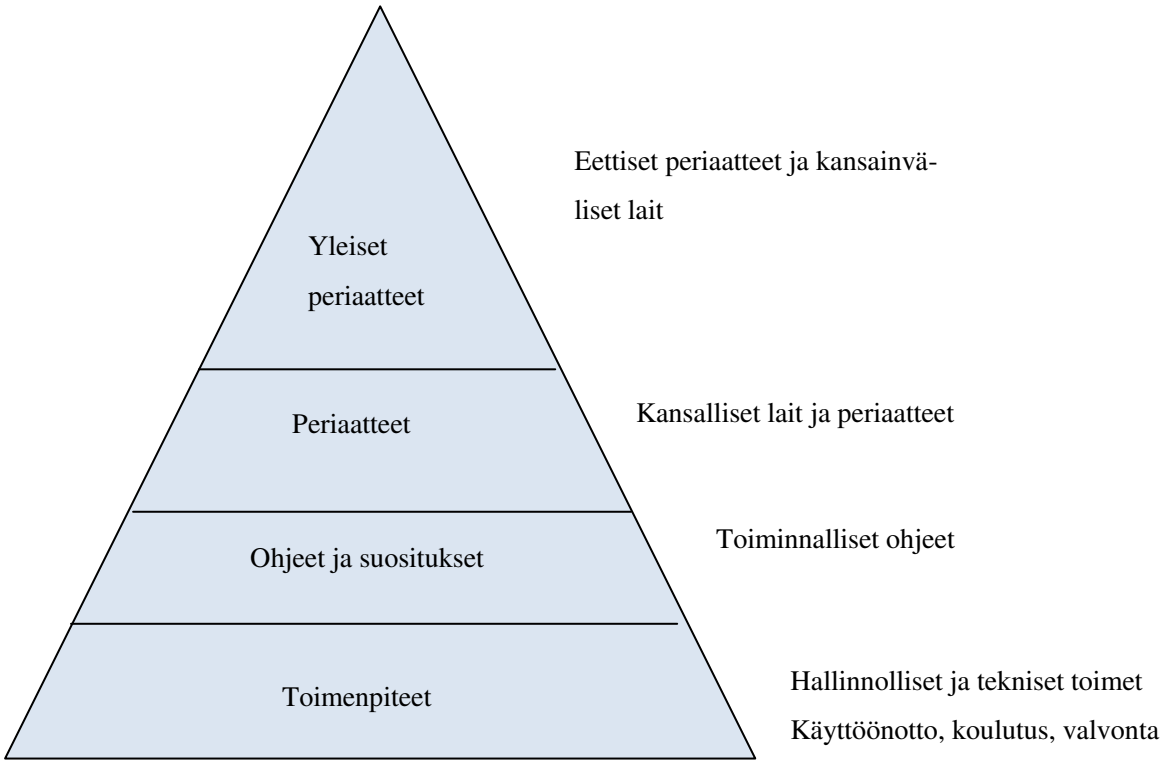
Ohjelmistoturvallisuus käsittää käyttöjärjestelmien ja ohjelmistojen tunnistamis- ja suojausominaisuudet, valvonta- ja lokimenettelyt sekä turvallisuustoimenpiteet kohdistuen ohjelmistojen päivityksiin ja ylläpitoon. Ohjelmistojen turvallisuuteen vaikuttavia tekijöitä ovat muun muassa ohjelmistokehitykseen käytetyt prosessit, ohjelmistojen asetukset sekä käyttäjien saama koulutus ja ohjeistus. (Valtiovarainministeriö 2007, 69.)

Tietoaineistoturvallisuus käsittää asiakirjojen, tietueiden ja tiedostojen tunnistamisen ja turvallisuusluokituksen. Tietoaineistoturvallisuutta on myös tietovälineiden asianmukainen hallinta, säilytys ja käsittely tiedonhallintaprosessin kaikissa vaiheissa. Tämä edellyttää ajantasaista, kaikki tietoaineistot kattavaa arkistonmuodostussuunnitelmaa tietojen käsittelysääntöineen. (Paavilainen 1998, 26 - 27; Valtiovarainministeriö 2007, 56.) Tavoitteena on tiedon tuhoutumisen tai tahattoman muuttumisen sekä sen luottamuksellisuuden menettämisen estäminen. Tiedon varmistaminen, asianmukainen säilytys sekä hävittäminen kuuluvat olennaisena osana tietoaineistoturvallisuuteen. (Paavilainen 1998, 26; Valtiovarainministeriö 2004b, 79.)

Käyttöturvallisuuden perustan muodostavat tunnistamiseen ja säännöstöihin liittyvät vaatimukset. Tietotekniikan turvallisen käytön vaatimat toimintaolosuhteet luodaan ja ylläpidetään huolehtimalla muun muassa käyttöoikeuksien hallinnasta, käytön ja lokien valvonnasta, ohjelmistotuesta, ylläpidosta sekä varmuuskopioinnista. (Paavilainen 1998, 213 – 214; Valtiovarainministeriö 2007, 65.) Varmistamalla organisaatiossa kaikkien henkilöiden oikeanlainen ja turvallinen tehtävien hoito sekä tietojärjestelmien käyttö varmistetaan samalla organisaation toiminta ja toimintakyky. Kaikkien tietojärjestelmien sisältämiä tietoja käsittelevien tulee tuntea oikeanlaiset ja sallitut käsittelytavat ja –säännöt. Käyttäjien on tiedettävä, miten ja mihin tarkoitukseen järjestelmiä saa käyttää ja millainen käyttö puolestaan on kiellettyä. Jokainen tiedon saaja pitää kyetä tunnistamaan ennen arkaluonteisten tietojen luovuttamista. Tietoja luovutettaessa tiedon saanti tulee perustua kunkin henkilön tiedonsaantioikeuksiin. (Tammisalo 2005, 53.)

2.3 Tietosuojan ja –turvallisuuden ohjaus terveydenhuollossa

Sosiaali- ja terveydenhuollon tehtävänä on samanaikaisesti sekä kehittää että hallinnoida tietosuojaa ja tietoturvallisuutta organisaatioiden turvallisten tietojenkäsittelytapojen toteuttamiseksi (Tammisalo 2005, 6, 9). Vaikka salassapitosäännökset muodostavatkin keskeisen perustan ja vaatimustason terveydenhuollon asiakas- ja potilastietojen hallinnoinnille, ei se ole riittävää nykyisessä sähköistyvässä ja verkottuvassa terveydenhuollon tietojen käsittelyssä (Pahlman 2010, 44). Terveydenhuollossa henkilötietojen käsittelyä ohjaavatkin ja määrittelevät monet lait ja asetukset, erilaiset suositukset, ohjeistukset, säännöstöt sekä eettiset periaatteet. Suomessa ei kuitenkaan ole olemassa yhtenäistä tietoturvallisuutta koskevaa lainsäädäntöä vaan tietosuojaan ja tietoturvaan liittyviä säädöksiä on sisällytetty useisiin lakeihin. (Tammisalo 2005, 6; Itälä & Ruotsalainen 2004, 62; Ruotsalainen 2006, 23.)



KUVIO 3. Asiakastiedon lainmukaisen ja luottamuksellisen käsittelyn kehikko (Ruotsalainen 2006, 9).

Ylimmäisenä Ruotsalaisen (2006) yllä esittämässä hierarkiassa (Kuvio 3) ovat *kansainväliset lait* ja *eettiset periaatteet*. Euroopan parlamentin ja neuvoston vuonna 1995 antama terveydenhuollon potilaan yksityisyyttä ja henkilötietojen suojaa koskevan direktiivin (EY:n henkilötietodirektiivi) tavoitteena on muun muassa turvata jäsenvaltioidensa jäsenten henkilötietojen käsittelyssä yksilöiden perusoikeudet ja –vapaus sekä heidän oikeutensa yksityisyyteen. Henkilötietodirektiivi saatettiin Suomessa voimaan henkilötietolailla 1.6.1999. Suomi on myös sitoutunut noudattamaan aiemmin, jo vuodesta 1992 lähtien Euroopan neuvoston yksilöiden suojelua henkilötietojen automaattisessa tietojenkäsittelyssä (tietosuojasopimus) koskevaa sopimusta (28.1.1981), jonka mukaan tiedot tulee kerätä asiallisesti ja laillisesti. (Pahlman 2010, 18 – 19; Ylipartanen 2010, 41.) Kyseinen sopimus sisältää *käyttötarkoitussidonnaisuus*-, *tarpeellisuus*-, *virheettömyys*-, *huolellisuus*- ja *suojaamisvaatimukset*. Laillisiin ja ennalta määriteltyihin tarkoituksiin kerättävä tarpeellinen määrä tietoja tulee olla oikeita ja ajantasaisia. Tietojen suojeleminen edellyttää myös riittäviä turvatoimia. (Pahlman 2010, 18.)

Terveydenhuollon ammattilaisten toimintaa ohjaavat ammattikunnan *eettiset periaatteet*: ihmisarvo, toisen ihmisen kunnioittaminen, inhimillisyys, luottamuksellisuus, oikeudenmukaisuus (Kalkas & Sarvimäki 1996, 205 – 208). *Laissa terveydenhuollon ammattihenkilöistä* (559/1994) määrittelee lainsäätäjä terveydenhuollon ammattihenkilön yleisiksi velvollisuuksiksi muun muassa ammattieettiset velvollisuudet, potilasasiakirjojen laatimisen ja säilyttämisen sekä niihin sisältyvien tietojen salassapitovelvollisuuden sekä salassapitovelvollisuuden. Ammattitoiminnassa tulee huomioida potilaan oikeuksia koskevat määräykset sekä noudattaa yleisesti hyväksyttyjä ja kokemusperäisiä perusteltuja menettelytapoja**.** Ammatinharjoittamisen päättymisen jälkeenkin säilyvä salassapitovelvollisuus puolestaan velvoittaa terveydenhuollon ammattihenkilöä ilmaisemasta luvatta asemansa tai tehtävänsä perusteella saatua yksityistä tai perheen salaisuutta. Potilasasiakirjojen laatiminen ja säilyttäminen sekä näiden tietojen salassa pitäminen tulee tapahtua potilaan asemasta ja oikeuksista annetun lain mukaisesti.

Perustuslaissa (731/1999) on säädetty yksilölle kuuluvia perusoikeuksia, joissa korostetaan yksilöä, yksilöiden tasavertaisuutta, tasa-arvoa sekä yksilöä oikeuksien subjektina. Laki sisältää säännökset yksityiselämän suojasta ja henkilötietojen käsittelyn säätämisestä lain tasoisesti. Julkisuusperiaatteen merkitystä viranomaisomaistoiminnassa on pyritty lisäämään säätämällä perustuslaissa viranomaisten hallussa olevat asiakirjat ja

muut tallenteet julkisiksi, jokaisella on oikeus saada tieto näistä asiakirjoista. (Pahlman 2007, 22; Pahlman 2010, 21; Ylipartanen 2010, 42.)

Kansallisella tasolla terveydenhuollon tietojen käsittelyä ohjaavat *yleislait* sekä *terveydenhuollon erityislait ja säädökset*. Tietosuojaa ja henkilötietoja koskeva tärkein yleislaki on 1.6.1999 voimaan tullut *henkilötietolaki* (523/1999), jonka tavoitteena on yksityiselämän suojan ja yksityisyyttä turvaavien perusoikeuksien toteuttaminen käsiteltäessä henkilötietoja sekä hyvän tietojenkäsittelytavan kehittämisen ja noudattamisen edistäminen. Laissa säädetyt vaatimukset liittyvät henkilötietojen keräämiseen, tallettamiseen, käyttöön, siirtämiseen, luovuttamiseen, säilyttämiseen, muuttamiseen, yhdistämiseen, suojaamiseen, poistamiseen, tuhoamiseen sekä rekisteröidyn oikeuksiin rekisterinpidossa. Lainsäädännön keskeisinä periaatteina ovat *huolellisuusvelvoitteen* ja *suojaamisvelvoitteen* toteutuminen *suunnitelmallisesti* sekä *käyttötarkoitussidonnaisuus* ja *avoimuus.* Henkilötietolakia sovelletaan julkisen ja yksityisen terveydenhuollon potilasrekistereihin sisältyvien henkilötietojen käsittelyssä. (Kleemola ym. 1998, 6; Pahlman 2007, 9, 13,23, 148; Ylipartanen 2010, 18- 19, 23 – 26, 44.)

Terveydenhuollossa potilasasiakirjojen arkaluonteisuuden ja käyttötarkoituksen vuoksi kaikissa käsittelyvaiheissa tulee noudattaa *huolellisuusvelvoitetta* potilassuhteen luottamuksellisuuden ja yksityisyyden suojan turvaamiseksi. Huolellisuusvelvoite edellyttää henkilötietojen käsittelyä laillisesti, huolellisuutta ja hyvää tietojenkäsittelytapaa noudattaen, rajoittamatta kuitenkaan rekisteröidyn yksityiselämän sekä yksityisyyden suojan turvaavia perusoikeuksia. (Kleemola ym. 1998, 6; Pahlman 2007, 76; Valtiovarainministeriö 2008b, 49; Ylipartanen 2010, 25.)

Potilas- ja asiakastietojen *suojaamisvelvoitteen* yhtenä lähtökohtana on estää asiattomilta henkilöiltä pääsy tietoihin sekä tietojen hävittäminen, muuttaminen, luovuttaminen, siirtäminen tai muu laiton käsittely (HetiL 523/1999). Käytettävissä tulee kulloinkin olla vain tehtävien hoidon kannalta tarpeelliset tiedot. Tietojärjestelmien toteutuksessa potilastietojen käyttöä rajataan määrittelemällä sellaiset toimintokohtaiset tietorakenteet, joiden avulla voidaan varmistaa vain hoidon kannalta tarpeellisten ja virheettömien tietojen käyttö sekä toisaalta määrittelemällä tehtävien vaatimusten mukaiset käyttöoikeudet henkilökohtaisine käyttäjätunnuksineen ja salasanoineen. Suojaamisvaatimus edellyttää myös suunnitelmallista järjestelmän käytön seurantaa ja valvontaa. (Pahlman

2007, 160.) *Laissa sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä* (159/2007) henkilötietojen suojaamista koskevissa säännöksissä huomioidaan erityisesti sähköiseen käsittelyyn liittyviä sellaisia erityispiirteitä ja –tarpeita kuten muun muassa jo aiemmin mainitut vaatimukset käytön ja luovutuksen seurannasta, potilasasiakirjojen tietorakenteista, tunnistamisesta sekä asiakirjan sähköisestä allekirjoittamisesta (Pahlman 2010, 53).

Terveydenhuollossa hyvä tietojenkäsittelytapa ja tiedonhallinnan toteuttaminen edellyttävät henkilötietolain mukaisen henkilötietojen käsittelyn *etukäteissuunnittelu* -vaatimuksen huomioon ottamista. Rekisterinpitäjän tulee ennen tietojen keräämistä ja muodostamista henkilöstörekisteriksi suunnitella henkilötietojen laillinen käsittely kaikissa vaiheissa. (Ylipartanen 2010, 20, 31.) Tällöin mahdollistetaan sellaisten lain asettamien vaatimusten kuten esimerkiksi tarkastusoikeuden, tietojen korjaamisen ja tietojen luovutuksen toteuttaminen lainmukaisesti (Pahlman 2010, 53).

Henkilötietolaki edellyttää henkilötietojen käsittelyn tarkoituksen määrittelyä, minkälaisten tehtävien hoitamiseksi henkilötietoja käsitellään. Lisäksi tietojen käsittelyn tulee olla rekisterinpitäjän toiminnan kannalta perusteltua. (Pahlman 2007, 149; Pahlman 2010, 56.) Potilasrekisterin ensisijainen käyttötarkoitus on potilaan hoitaminen. *Käyttötarkoitussidonnaisuus* tarkoittaa tällöin, että potilasrekisterissä olevia tietoja saa käyttää pääsääntöisesti vain potilaan hoitoon eli vain siihen tarkoitukseen, mihin ne on etukäteen määritelty. Käyttötarkoituksella taataan se, että käyttäjät saavat käyttöönsä kaikki tehtävänsä hoitamisen kannalta tarvitsemansa tiedot. (Kleemola ym. 1998, 42, 58, 67; Ylipartanen 2010, 49 - 50.)

Rekisterinpidon *avoimuus* perustuu rekisteröityjen oikeuteen saada tietää tietojensa käsittelystä. Henkilötietojen käsittelyn tulee olla suojattua sivullisilta, mutta avointa potilaan ja asiakkaan näkökulmasta tarkasteltuna. Periaatteena on, että jokaisella on oikeus tietää itseään koskevien tietojen käsittelystä. (Ylipartanen 2010, 130.)

Laki viranomaisen toiminnan julkisuudesta (621/1999) sisältää henkilötietojen käsittelyä koskevia säännöksiä. Lain tavoitteena on toteuttaa avoimuutta ja hyvää tiedonhallintatapaa viranomaisten toiminnassa lisäämällä muun muassa kansalaisten mahdollisuuksia valvoa viranomaisten toimintaa, omia oikeuksiaan ja etujaan. Lähtökohtana on jul-

kisuusperiaate. Poikkeuksen tästä pääsäännöstä muodostavat arkaluonteiset ja salassa pidettävät sosiaali- ja terveydenhuollon asiakirjat, jotka ovat salassa pidettäviä riippumatta siitä, minkä viranomaisen hallussa ne ovat ja miten viranomainen on ne saanut. Siten julkisuuslain säännökset täydentävät sosiaali- ja terveydenhuollon erityislainsäädäntöön sisältyviä salassapitovelvoitteita. (Pahlman 2007, 35 – 36; Ylipartanen 2010, 54 – 55.)

Laki potilaan asemasta ja oikeuksista (785/1998) sisältää perussäännökset potilasasiakirjojen ja potilastietojen käsittelystä täydentäen näin muuta terveydenhuollon lainsäädäntöä (Pahlman 2007, 24). Sen tavoitteena on parantaa potilassuhteen luottamuksellisuutta, potilaan hoidollista itsemääräämisoikeutta sekä potilaan tietosuojaa. Laissa on määräykset liittyen muun muassa potilaan tiedonsaantioikeuksiin sekä potilaan suostumukseen perustuvaan salassa pidettävien potilasasiakirjojen yleisistä luovutusperusteista. Lähtökohtaisesti tietoja tulisi luovuttaa vain potilaan suostumuksella tai tietyissä tilanteissa hänen laillisen edustajansa suostumuksella esimerkiksi silloin, kun kyseessä on vajaavaltainen potilas. Salassapitovelvollisuuden piiriin kuuluvia tietoja saa luovuttaa ilman potilaan suostumusta myös niissä tapauksissa, kun siihen on jokin lakiin perustuva oikeus. Viranomaisten tietojensaantioikeutta säädellään erityislainsäädännöllä. (Ylipartanen 2010, 56, 77 - 79.)

Sosiaali- ja terveysministeriön asetukseen potilasasiakirjoista (289/2009) sisältyvät yleiset periaatteet ja vaatimukset koskevat tietojen eheyden ja käytettävyyden turvaamista laadittaessa ja säilytettäessä potilasasiakirjoja sekä potilasasiakirjoihin sisältyvien tietojen käyttöoikeuksia. Asiakastietojen käyttöoikeudet tulee määritellä yksityiskohtaisesti potilaan hoitoon tai siihen liittyviin tehtäviin osallistuvien työtehtävien ja vastuiden edellyttämässä laajuudessa. Sähköisiä potilastietojärjestelmiä käyttävät tulee pystyä todentamaan yksiselitteisesti. Potilasasiakirjojen merkinnöille asetetaan myös tiettyjä vaatimuksia - merkinnät tulee tehdä yleisesti tunnettuja ja hyväksyttyjä käsitteitä ja lyhenteitä käyttäen.

Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007), muutettu 1.1.2011 voimaan tulleella lailla (1227/2010), sisältää sosiaali- ja terveydenhuollon asiakastietojen sähköisen käsittelyn yleiset vaatimukset tavoitteenaan muun muassa edistää sosiaali- ja terveydenhuollon asiakastietojen tietoturvallista käsittelyä ja

potilaan tiedonsaantimahdollisuuksia omista potilastiedoistaan ja niiden käsittelyyn liittyvistä lokitiedoista. Tämän asiakastietolain säännöksillä pyritään turvaamaan asiakastietojen käytettävyys, eheys, säilyminen sekä asiakkaan yksityisyyden suoja. (Pahlman 2010, 123, 125.)

Asiakastietolaissa on edellä mainittujen vaatimusten toteutumiseksi säädöksiä asiakirjojen yksilöinnistä, säilyttämisestä sekä käyttäjien ja käyttöoikeuksien rekisteröinnistä unohtamatta käytön ja tietojen luovutuksen seurantaa lokirekisterin avulla koskien rekisterinpitäjän omassa toiminnassa tapahtuvaa tietojen käyttämistä. Laki sisältää määräyksiä myös sähköisten potilastietojen käsittelystä, kenellä on oikeus saada ja käsitellä potilastietoja ja missä laajuudessa. Sähköisten potilasta koskevien tietojen luovuttamisesta toiselle terveydenhuollon palvelujen antajalle on omat säännöksensä. Samoin potilaan suostumusta koskevat yleiset vaatimukset on sisällytetty kyseiseen lakiin. (Pahlman 2010, 124 – 127, 129.)

Uusi terveydenhuoltolaki (1326/2010) astui voimaan 1.5.2011. Lain tarkoituksena on muun muassa väestön terveyden, hyvinvoinnin, työ- ja toimintakyvyn sekä sosiaalisen turvallisuuden edistäminen ja ylläpitäminen, terveydenhuollon asiakaskeskeisyyden vahvistaminen ja palvelujen yhdenvertaisen saatavuuden, laadun ja potilasturvallisuuden toteuttaminen. Tietosuojan ja tietoturvan kannalta merkityksellinen lainkohta sisältyy terveydenhuoltolain 9 §:ään, joka sisältää potilastietojen hallintaan liittyviä säännöksiä koskien yhteisen potilastietorekisterin toteutusta ja potilastietojen käsittelyä kuten potilastietojen luovutusta ja käyttöä, potilaan informointia ja potilaan kieltooikeutta.

Potilaita tulee informoida yhteisestä potilastietorekisteristä ja mahdollisuudesta luovuttaa hoitosuhteen yhteydessä potilastietoja muille kyseisessä rekisterissä oleville palvelunantajille ilman potilaan erikseen antamaa suostumusta. Potilasta tulee myös informoida hänen mahdollisuudestaan kieltää tietojensa luovutus toimintayksiköiden välillä. Kieltomahdollisuus koskee kaikkia potilasasiakirjoja niiden tallennusmuodosta riippumatta. Yhteisessä potilastietorekisterissä olevien eri toimintayksiköiden tietojen luovuttaminen ilman potilaan antamaa suostumusta siis edellyttää ensinnäkin potilaan etukäteisinformointia toisaalta olemassa olevaa hoitosuhdetta tietoja tarvitsevaan toimintayk-

sikköön. Edellisten lisäksi potilas ei saa olla myöskään kieltänyt tietojensa käyttöä. (Sosiaali- ja terveysministeriö 2011.)

Lainsäädännön lisäksi erilaiset suositukset, ohjeistukset, säännöstöt säätelevät terveydenhuollon henkilötietojen ja potilasasiakirjojen käyttöä. Erilaisten sosiaali- ja terveysministeriön ja valtionvarainministeriön VAHTI –ohjeistojen lisäksi käytettävissä on myös toimialakohtaisia erillisohjeistuksia. Näistä esimerkkinä mainittakoon Terveydenhuollon ja hyvinvoinnin laitoksen tietoteknologian osaamiskeskuksen (OSKE) antamat suositukset terveydenhuollon tietoturvallisen tiedonvälityksen ohjeistusten laatimiseksi. Lisäksi tietosuojavaltuutetun toimisto yhtenä henkilötietolaissa sekä laissa tietosuojalautakunnasta ja tietosuojavaltuutetusta määriteltynä tehtävänään antaa yleistä ohjeistusta.

2.4 Yleiset vaatimukset potilasasiakirjojen käsittelylle

Kuten jo aiemmin on tullut esille, terveydenhuollon tietojen käsittelyssä tulee noudattaa kansallisia lakeja, asetuksia ja STM:n antamia ohjeita sekä terveysalan eettisiä periaatteita. Terveydenhuollon tietojen lainmukainen ja luottamuksellinen käsittely edellyttää suunnitelmallista tietojen käyttöä, talletusta, ylläpitoa ja luovutusta. Säätelystä johtuvat yleiset vaatimukset potilasasiakirjatietojen ja henkilötietojen käsittelyyn kohdistuvat tietojen eheyden, yksityisyyden, luottamuksellisuuden, tarpeellisuuden ja käyttötarkoitussidonnaisuuden turvaamiseen. (Ruotsalainen 2006,8, 53.) Tietoturvavaatimukset ovat välineriippumattomia, ne kohdistuvat sekä sähköisessä että manuaalisessa muodossa olevan tiedon kaikkeen käsittelyyn (Valtiovarainministeriö 2006,11, 14).

Henkilötietojen käsittelyssä tulee huomioida yksityisyyden ja luottamuksellisen viestinnän suoja. Henkilötietoja käytetään vain siihen tarkoitukseen kuin mihin ne on kerätty ja silloinkin käsitellään vain tarpeellisia tietoja. Hoidon kannalta tarpeellisten tietojen käsittely edellyttää hoitosuhdetta, asiayhteyttä tai tietojen käsittelylle on olemassa joku muu laista johtuva peruste. Tiedot eivät saa myöskään joutua sivullisten käsiin ilman potilaan suostumusta tai laista johtuvaa perustetta. Lainsäädäntö asettaa omat vaatimuksensa myös tietojen luovuttamiselle sekä potilaan oikeuteen määrätä omien terveystietojensa käytöstä ja luovuttamisesta antamansa suostumuksen tai tekemänsä kiellon perusteella. (Ruotsalainen 2006, 8, 53.)

Terveydenhuollon tietoja käsiteltäessä käytössä tulee olla sellaiset järjestelmät, jotka mahdollistavat tietojen alkuperän tunnistamisen sekä niiden käytön ja luovutuksen seurannan. Tietojen käytön tulee olla suunnitelmallista ja tietojen muuttumattomuus käsittelyn, siirron tai säilyttämisen aikana tulee varmistaa. Terveydenhuollon sähköisessä asioinnissa tunnistamisen ja tarvittaessa todentamisen vaatimus kohdistuu asiakkaaseen, ammattihenkilöstöön sekä organisaatioon. Käyttäjien hallinnan ja tunnistamisen, käyttöoikeuksien hallinnan sekä tietojenkäytön hallinnan tietojärjestelmäpalvelut mahdollistavat sähköisten potilasasiakirjojen käsittelylle asetettuihin haasteisiin vastaamiseen. (Ruotsalainen 2006, 53.)

3 TIETOSUOJA- JA TIETOTURVAOSAAMINEN

Jokaisen viranomaisen tulee huolehtia riittävän hyvän tietoturvallisuuden ja henkilötietojen suojan toteutumisesta omassa organisaatiossaan. Tietoturvallisuuden riittävä taso tulee määritellä ja toteuttaa voimassa olevia säädöksiä noudattaen kunkin organisaation toiminnallisten tavoitteiden ja tietosisältöjen arvon ja merkityksen mukaisesti. Yhtenä periaatteena tietoturvallisuuden kehittämisessä on henkilöstön tehtävien ja tietoturvavaatimusten edellyttämän osaamisen varmistaminen arvioimalla osaamista sekä kehittämällä niin tietoturvatietoisuutta kuin -koulutusta. (Valtiovarainministeriö 2009.)

Terveydenhuollon toimintaympäristöissä ja toimintatavoissa tapahtuvat teknologian tuomat muutokset vaikuttavat henkilöstön osaamisvaatimuksiin. Kehittyvä tietoyhteiskunta edellyttää uusien tietojen ja taitojen hankkimista. Osaamisvaatimusten tarkastelussa vahvistuu käsitys tietojen ja taitojen jatkuvan päivittämisen tarpeesta. Työelämässä ei enää selvitä pelkällä ammattikoulutuksessa saavutetulla osaamisella. Osaaminen onkin painottunut uusien toimintatapojen kehittämiseen ja uuden osaamisen tuottamiseen. Informaatiotekniikka sekä tiedon merkityksen lisääntyminen ovat luoneet uusia osaamisvaatimuksia terveydenhuollossa. (Lammintakanen & Kinnunen 2006, 16 – 17; Ylipartanen 2010, 27.) Terveydenhuollon ammattihenkilöiden tietosuoja- ja tietoturvaosaamisen merkitys yhtenä ammatillisena osaamisvaatimuksena onkin korostumassa entisestään; tieto- ja viestintätekniikan käytön tulee kunnioittaa potilaiden päätöksentekoa ja korostaa tietosuojaa ja –turvallisuutta (Jauhiainen 2006, 36). Hoitotyön tietosuoja- ja tietoturvaosaamisen kehittäminen tulee olemaan haaste terveydenhuollon organisaatioille.

3.1 Tietosuoja- ja tietoturvaosaamiseen kohdistuvia vaatimuksia

Henkilöstön on todettu olevan suurin riskitekijä tietoturvatapahtumissa. Henkilöstöstä ja heidän toimintatavoistaan johtuviin tietoturvariskeihin voidaan vaikuttaa muun muassa toimenkuvien, käyttöoikeuksien ja asianmukaisen koulutuksen avulla. Tietosuojan ja -turvallisuuden merkityksen ymmärtäminen, toimintaohjeiden tiedostaminen ja noudattaminen auttavat paremmin hallitsemaan tietoturvauhkia. Terveydenhuollon ammattihenkilöiden tietämyksessä ja asenteissa rekisterinpitoa, yksityisyyden suojaa ja itsemääräämisoikeutta kohtaan onkin todettu tapahtuvan koko ajan muutosta. Tämä muutos luo

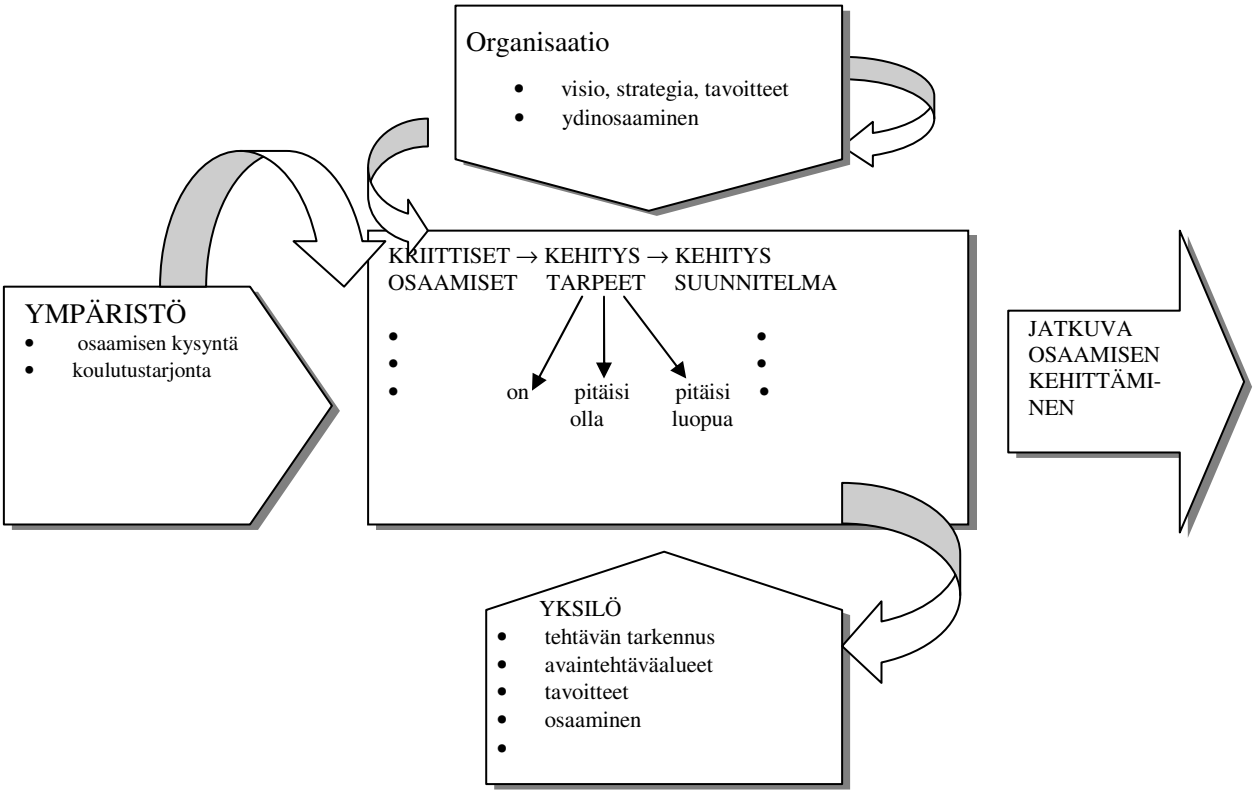
osaltaan entistä enemmän tarvetta työelämän tarpeita vastaavaan tietosuojaan liittyvien asioiden opettamisen järjestämiselle jo aivan peruskoulutuksessa. (Tammisalo 2005, 7; Ylipartanen 2010, 27.) Tulevaisuudessa tietoturvakoulutuksessa näyttäisi painopiste olevankin enemmän tietoturva-asenteeseen ja yksityisyydensuojaan liittyvissä asioissa kuin teknistä osaamista korostavassa koulutuksessa (Valtiovarainministeriö 2008a, 19).

Teknologian kehitys terveydenhuollossa on sekä haaste että mahdollisuus. Tietojärjestelmät helpottavat ja nopeuttavat työskentelyä sekä parantavat hyödynnettävän tiedon saatavuutta. Toisaalta muutos on tuonut mukanaan myös ongelmia: kaikilla ei ole riittävää tietoteknistä osaamista. Lisääntyvän tietoteknologian käyttöönoton ja hyödyntämisen myötä myös tietosuoja ja siihen liittyvät oikeudelliset kysymykset ovat yhä keskeisemmässä asemassa hoitotyössä. Terveydenhuollossa kaikkien potilastietoja käsittelevien tulisikin tuntea oman alansa lainsäädännössä, henkilötietolaissa ja julkisuuslaissa määritellyt tietosuojaa koskevat keskeiset periaatteet ja säännökset. (Hilden 2002, 13; Kleemola & Tervo-Pellikka 1998,1; Ylipartanen 2010, 24.)

Toimintaympäristön ja uusiutuvan lainsäädännön mukanaan tuomat muutokset ovat muuttaneet osaamiseen liittyviä vaatimuksia hoitotyössä. Terveydenhuollon ammattihenkilöiden yhdeksi tärkeäksi ammatilliseksi osaamisvaatimukseksi näyttäisi nousevan tietosuoja- ja tietoturvaosaaminen. (Ylipartanen 2010, 27.) Tämä muutos pakottaa henkilöstöä uusimaan osaamistaan sekä luomaan uutta osaamista. Jokaisen tulisi säännöllisin väliajoin arvioida omaa osaamistaan, vastaako se tämänhetkistä työssä tarvittavaa osaamista. Tieto henkilöstön osaamisen nykytilasta ja tulevaisuuden osaamisvaatimuksista luo perustan osaamisen suunnitelmalliselle johtamiselle, jonka avulla kyetään kehittämään henkilöstön osaamisen tasoa ja hyödyntämään osaamista. Osaamista voidaan mitata muun muassa osaamiskartoituksen avulla laatimalla osaamiskartta tietyn henkilöstöryhmän osaamisista tai vain jostain erikseen valitusta yksittäisestä osaamisesta. (Hilden 2002, 7, 29 – 31; Kujansivu, Lönnqvist, Jääskeläinen & Sillanpää 2007, 113, 117.)

Inhimillinen pääoma (osaaminen, työmotivaatio, sitoutuminen, työkyky) muodostuu työntekijöiden koulutuksen ja kokemuksen tuomasta osaamisesta – tiedoista, taidoista ja asenteista (Viitala 2005, 99). Liiketoiminnassa tämän yritysten aineettoman pääoman ja sen johtamisen tueksi on kehitetty joukko erilaisia malleja pääsääntöisesti yritysten

käyttöön, mutta ne ovat sovellettavissa myös julkisen sektorin organisaatioihin (Kujansivu ym. 2007, 7-8). Tässä tutkimuksessa tutkittavaa ilmiötä lähestytään osaamisen johtamisen viitekehyksen kautta soveltuvin osin. (Kuvio 4).



KUVIO 4. Osaamisen johtamisen viitekehys (Sydänmaalakka 2007, 132).

3.2 Osaamisen johtaminen

Tieto ja osaaminen eli *tietämys* syntyy informaation vastaanottajan tulkinnan kautta osaksi hänen tietorakennettaan muuttaen sitä. Yleisellä tasolla tietämys voidaan määritellä johonkin asiaan liittyväksi inhimilliseksi käsitykseksi, joka sisältää kokemuksia, asiatietoa, mielipiteitä, arvoja, asenteita ja uskomuksia. Uuden tietämyksen aikaansaamiseksi tarvitaan informaation lisäksi myös aiempaa tietämystä. Tietämys liittyy usein asiantuntemukseen, se voi olla asiantuntijoiden tietoa tietyllä erityisalalla. (Huotari, Hurme & Valkonen 2005, 38 – 39; Sydänmaalakka 2007, 189 – 190.)

Organisaatiotasolla osaaminen on *ydinosaamista*, joka jakautuu osaamisalueisiin, jotka puolestaan jakautuvat konkreettisiin osaamisiin eli kompetensseihin (Sydänmaalakka 2007, 146 – 147). Ydinosaamisella tarkoitetaan tietojen, taitojen, prosessien, menetelmien, teknologioiden ja tietojärjestelmien yhdistelmää, pitkällä aikavälillä kehittynyttä organisaatioissa omaksuttua laaja-alaista osaamista. Se on osaamista, jota organisaatio hyödyntää toiminnassaan nyt ja tulevaisuudessa. Jatkuvasti muuttuvissa toimintaympäristöissä se on organisaation tärkeä kilpailutekijä. Ydinosaaminen kehittyy ja muodostuu organisaation oppimisen tuloksena, käsitettä käytetään yleensä vain organisaatiotasolla. (Otala 2000, 206; Sydänmaalakka 2007, 144 – 145; Virtainlahti 2009, 30.)

Yksilön osaamisella tarkoitetaan työn vaatimien tietojen ja taitojen hallintaa, kykyä ja motivaatiota niiden soveltamisessa käytännön työtehtäviin. Osaaminen siis liittyy tiedon käyttöön. (Kujansivu ym. 2007,112.) Kompetenssi eli ammattitaito ymmärretään työtehtävien vaatimiksi valmiuksiksi eli kvalifikaatioksi. Ammattitaito koostuu yleisistä tehtävästä riippumattomista, ammattikohtaisista tiettyyn ammattialaan ja tehtäväkohtaisista tiettyyn tehtäväkuvaan liittyvistä valmiuksista. (Viitala 2005, 113 – 114.)

Yksilön tasolla *osaaminen* on hyvin konkreettista, se koostuu tiedoista, taidoista, asenteista sekä motivaatiosta (Viitala 2005, 113, 115). Suoriutuakseen tehtävistään yksilöltä vaaditaan tiettyä osaamista. Jotta henkilöstön osaamista kyetään kehittämään, tarvitaan tietoa osaamisen nykytilasta sekä tulevaisuuden osaamisvaatimuksista. Tunnistamalla kriittiset osaamiset, mitä osaamista yksilöllä on, mitä pitäisi olla ja mistä mahdollisesti pitäisi luopua, saadaan selville mahdolliset kehittämistarpeet. Määrittelemällä ja kuvaamalla tunnistetut konkreettiset osaamisalueet osaamisluetteloiksi, mahdollistetaan osaamisen arviointi osaamiskartoituksen avulla. Yksilöllisten kehittämistarpeiden pohjalta voidaan edelleen laatia kullekin henkilökohtaiset kehityssuunnitelmat. (Kujansivu ym. 2007, 113; Sydänmaalakka 2007, 133¸ Virtainlahti 2009, 69.) Osaamisen johtaminen mahdollistaa näin tämän osaamiseen ja henkilöstöön liittyvien tulevaisuuden tarpeiden ennakoinnin, organisaation kannalta keskeisten osaamistarpeiden tunnistamisen sekä osaamisen ja koulutuksen kehittämisen organisaatiossa.

Osaamisen johtamisen tarkoituksena on saada organisaation käyttöön paras mahdollinen osaaminen arvioimalla systemaattisesti organisaation ja sen henkilöstön osaamista sekä kehittämistä toiminnan tavoitteista lähtöisin. Osaamisen johtaminen liittyy käsityk-

seen yksilön oppimisesta ja osaamisen ymmärtämisestä, organisaation osaamista ei ole ilman ihmisiä. (Virtainlahti 2009, 68.) Peruslähtökohdan osaamisen johtamiselle muodostavat organisaation strategia, visio, tavoitteet ja ydinosaaminen, osaamistarpeet määräytyvät visiosta ja tavoitteista (Kuvio 4). Osaaminen kehittäminen on siis osa vision toteuttamista, strategiaa. On tiedettävä, mikä organisaation tarkoitus on ja minkälaista osaamista se tarvitsee suoriutuakseen tehtävästään. Osaamisia voidaan tarkastella monesta eri lähtökohdista. Niitä voidaan tunnistaa muun muassa tulevaisuudessa vaadittavien osaamisalueiden näkökulmasta, minkälaista osaamista tulevaisuudessa edellytetään tai toimintaympäristön muutosten tuomien osaamisvaatimusten näkökulmasta, mitä osaamisvaatimuksia lainsäädäntö tai kehittyvä teknologia asettavat. (Hilden 2002,73 – 74; Kujansivu ym. 2007, 117 - 118; Otala 2000, 223 - 225; Sydänmaalakka 2007, 131 – 132, 136, 148.) Käytännössä osaamisen johtamisella usein tarkoitetaan osaamiskartoitusta, osaamisen arviointia ja koulutustoimintaa (Virtainlahti 2009, 68).

Osaamisen ja tietämyksen johtaminen perustuu osaamisen ja tietämyksen *tunnistamiseen*. Osaamisen tunnistaminen itsessään jo antaa hyödyllistä tietoa esimerkiksi määritettäessä työtehtävien sisältöä, tunnistetun osaamisen mittaaminen puolestaan auttaa hyödyntämään ja kehittämään tietämystä osaamisen johtamisen näkökulmasta. (Kujansivu ym. 2007,119.) Osaamista voidaankin mitata useasta eri näkökulmasta. Mitattavina kohteina voivat olla muun muassa opitut tiedot ja taidot, soveltaminen, asenteet ja arvot sekä henkilökohtaisen suorituskyvyn kehittyminen. Usein osaamisen mittarina käytetään pelkkää koulutuksiin osallistumista, jolloin seurannan kohteena ovat esimerkiksi kurssille osallistuneiden määrä tai koulutuspäivien lukumäärä. Tästä näkökulmasta arvioituna todellista osaamisen tasoa on kuitenkin vaikea selvittää. Yksinkertaisia teoriaosaamisia voidaan puolestaan testata muun muassa näyttökokeilla. Yhtenä vaihtoehtona osaamisen mittaamiseen voidaan käyttää myös itsearviointia tai esimerkiksi esimiehen tekemää arviointia. Tämän arvioinnin heikkoutena on kuitenkin sen subjektiivisuus - arviointiin voivat vaikuttaa muutkin tekijät kuin henkilön todellinen osaaminen. (Laamanen 2005, 341.)

3.3 Aikaisempia tutkimuksia

Lehtonen (2002) kartoitti tutkimuksessaan organisaation kilpailukyvyn säilyttämisen kannalta keskeiset osaamisalueet tavoitteenaan mallintaa organisaation tärkeimmät

osaamisresurssit ja – vaatimukset sekä tarkastella näiden hallintaa strategianäkökulmasta organisaatiotason ilmiönä. Tutkimuksen teoreettisena viitekehyksenä toimi osaamisperusteisen johtamisen (competence-based management) tutkimuksen piirissä kehitetty teoria, CBM-teoria. Osaamisalueiden mallinnusta ja hallintaa lähestyttiin yksilön ja organisaation vuorovaikutuksen sekä osaamisen kehitysmekanismien näkökulmasta perustuen kognitiotieteelliseen lähestymistapaan. Kohdeorganisaation asiantuntijoiden todettiin osaavan yleensä kuvata ja arvioida paremmin konkreettisia jo olemassa olevia osaamisia kuin sellaista osaamista, jota organisaatiolla ei ole, mutta jota se tarvitsee. Toimintakäytäntöjen tulisikin vahvistaa muun muassa myös abstraktimpaa osaamista. Osaamisen kehittämisessä ja hallinnassa tulisi keskittyä toiminnan kautta oppimista tukevien toimintatapojen ja –kulttuurin kehittämiseen. Tutkimuksessa kehitetty organisaation osaamisen strategista johtamista tukeva malli ja metodiikka ovat tutkijan mukaan yleistettävissä myös muiden organisaatioiden tutkimuksissa.

Myös Draganidis ja Mentzas (2006) tarkastelivat tutkimuksessaan osaamisen johtamisen (competency management, CM) avainkäsitteitä sekä esittivät menetelmän osaamisen kehittämisen välineeksi. Tutkimus kohdistui 22 kaupallisen CM järjestelmän ja 18 oppimisen johtamisen järjestelmän ominaisuuksiin. Yleisimpiä piirteitä näille järjestelmille olivat muun muassa osaamisen luokittelut, määrittelyt, pätevyysasteikot, tehtäväkuvaukset sekä arviointityökalut. He tunnistivat 4 vaihetta osaamisen elinkaaressa: osaamisen kartoitus, määrittäminen, kehittäminen ja seuranta. Kaikki neljä vaihetta analysoitiin yksityiskohtaisesti ja sen pohjalta kehitettiin algoritmi osaamisen kehittämisen malliksi. Johtopäätöksenä he totesivat CM:n tulevan entistä tärkeämmäksi toiminnaksi niin yksityisissä kuin julkisissakin organisaatioissa auttaen näin osaavan työvoiman rekrytoinnissa, oikeiden henkilöiden kohdentamisessa oikeisiin tehtäviin, koulutuksen suunnittelussa ja muissa inhimillisen pääomaan liittyvissä toiminnoissa.

Kivinen (2008) puolestaan tarkasteli tutkimuksessaan tiedon ja osaamisen johtamista terveydenhuollon organisaatioiden toimintana tarkoituksena selkeyttää knowledge management -käsitettä, kuvata tiedon ja osaamisen johtamisen toteutumista sekä selittää siihen vaikuttavia tekijöitä. Tulosten mukaan teknologian kehityksellä on ollut lisäävä vaikutus tiedon ja osaamisen johtamisen keskustelun käynnistymiselle sekä tutkimuksen ja käytännön toiminnan edistämisessä. Kuitenkaan kaikissa organisaatioissa ei ollut suunnitelmallisuutta eikä yhtenäisiä käytäntöjä tiedon ja osaamisen johtamisessa.

Osaamisen kehittäminen keskittyy lyhytkestoisiin koulutuksiin ja kehityskeskusteluihin, koko organisaatiotasolla olevat käytännöt olivat vähäisessä käytössä. Tutkimus antaa tietoa tiedon ja osaamisen johtamisen tilanteesta ja siihen vaikuttavista tekijöistä. Tuloksista ilmenee muun muassa, että terveydenhuollossa on käytössä erilaisia tietojärjestelmiä, mutta niiden monipuolinen käyttö on edelleen vähäistä. Tietotekniikan ja tiedonhallinnan osaamispuutteet tulevat esille tässä tutkimuksessa. Vaikka organisaatioissa on käyty tiedon hallintaan liittyvää keskustelua tietotarpeista, tiedon hankinnasta, säilyttämisestä ja käytöstä, kirjalliset suunnitelmat ja sovitut toimintatavat ovat tutkimuksen tulosten mukaan puutteellisia.

Belsis, Kokolakis ja Kiountouzis (2005) myös tarkastelivat tutkimuksessaan tietojärjestelmien turvallisuutta osaamisen johtamisen näkökulmasta. Tietoturvallisuuden hallinta on tietointensiivistä toimintaa, jossa korostuu voimakkaasti alan asiantuntijoiden kokemus. Tästä huolimatta sekä tutkimuksissa että eri ammattialoilla tietämyksen merkitystä tietoturvallisuuden hallinnassa on laiminlyöty. Toiminnan perustuessa nykyään entistä enemmän tietoon ja tiedonvälitykseen tietojärjestelmien turvallisuuden merkitys on kasvanut organisaatioiden toiminnassa. Turvallisuus on ensisijaisesti ihmisten, mutta myös organisaation asia. Tietämyksen luominen on sosiaalinen tapahtuma, osaamisen johtamisen avulla tulisikin tukea kaikkia tietämyksen kehittämiseen osallistuvia kaikilla organisaation tasoilla – strategisella, taktisella sekä toiminnallisella tasolla. Tutkijat totesivatkin menestyvän turvallisuuden hallinnan olevan riippuvainen käyttäjien ja muiden asianomaisten mukanaolosta muun muassa tietoturvallisuuden suunnittelussa, toteutuksessa sekä varmistamisessa.

Tutkimuksensa tuotoksena Belsis ym. (2005) tunnistivat turvallisuutta parantavia toimintoja sekä turvallisuustietämystä hyödyntäviä lähteitä. Lisäksi he esittivät löydöksiensä tukemiseksi organisaation tietojärjestelmien turvallisuuden tietämystä kuvaavan mallin kolmella eri hierarkkisella tasolla: toimintaperiaatteet, suositukset ja mittaaminen. Yhteenvetona Belsis ym. totesivat osaamisen johtamisjärjestelmällä olevan monia suotuisia vaikutuksia tietojärjestelmien turvallisuuteen liittyvissä kysymyksissä. Tietämyksen ja osaamisen kehittämisen tapahtuessa organisaation sisällä, organisaatio ei ole riippuvainen kalliista ulkopuolisista asiantuntijoista. Se mahdollistaa myös käyttäjien osallistumisen tietojärjestelmien turvallisuuden kehittämiseen, hallinnolliset suositukset ovat tehokkaammin käyttäjien tiedossa. Palautejärjestelmää vahvistamalla puolestaan

mahdollistetaan tietojärjestelmien turvallisuuden johtamisjärjestelmän seuranta, arviointi ja parantaminen.

Kirjallisuuskatsauksessaan Hobbs (2002) tarkasteli tietokonetaitoihin liittyvien ominaisuuksien kuten tietämyksen, asenteiden ja käyttötaitojen mittaamista koskevia menetelmiä ja tutkimuksia. Katsauksen perusteella tietämys koostui perustoiminnoista, tietojenkäsittelystä, turvallisuudesta ja hoitajien tietämyksestä terveydenhuollon tietojärjestelmistä. Asenteisiin puolestaan sisältyi tyytyväisyys käytettävään järjestelmään ja uskomus järjestelmän paremmuuteen. Käyttäjien taidot koostuivat muun muassa peruskäyttötaidoista, tietojenkäsittelystä, turvallisuudesta, sähköpostin ja Internetin käyttötaidoista. Vaikka hoitajien tarvitsemista erityistietämyksestä, asenteista ja taidoista ei esiintynytkään täyttä yksimielisyyttä, tutkimusten kokonaisuuden tarkastelussa esille nousivat hoitotyön tiedonhallinnan osaamisvaatimuksiksi tieto- ja viestintätekniikan peruskäyttötaidot, valmiudet käyttää erilaisia tietojärjestelmiä, verkkotietoisuus, tietokoneluku- ja –kirjoitustaito sekä tietosuojan ja –turvan hallinta ja osaaminen.

Staggers, Gassert ja Curran (2001, 2002) toivat artikkeleissaan Hobbsin tavoin esille pätevien ja kattavien hoitotyön tiedonhallintapätevyyksien määrittelyn puutteellisuuden. Aiemmin on enemmänkin keskitytty tietokoneen käyttöön liittyviin taitoihin kuin tiedonhallintaan liittyvien taitojen määrittelyyn. Staggers ym. kehittivät kattavat kuvaukset sairaanhoitajien tiedonhallinnan osaamisvaatimuksista kolmelle eri osa-alueelle - atk-taidot (computer skills), tiedonhallinnan tietämys (informatics knowledge) ja tiedonhallinnan taidot (informatics skills). Edellä mainitut luokittelut sisälsivät myös tietosuoja - ja tietoturva –osaamisen kullekin neljälle eri osaamistasolle, joita olivat aloitteleva sairaanhoitaja, kokenut sairaanhoitaja, tiedonhallinnan asiantuntija ja tiedonhallinnan kehittäjä.

Jo edellisten tutkimusten perusteella voidaan todeta terveydenhuollon eri toimintayksiköissä työskentelevien ammattilaisten tarvitsevan uudenlaisia taitoja ja tietoja omaksuakseen ja hyödyntääkseen tehokkaasti tietotekniikkaa sekä sähköisessä muodossa olevaa informaatiota. Vastauksena tähän lisääntyneeseen tarpeeseen tukea sähköisten potilastietojärjestelmien kanssa työskentelevien koulutusta ja perehdytystä myös AHIMA (the American Health Information Management Association) ja AMIA (the American Medical Informatics Association) ovat vuonna 2008 julkaisemassa artikkelissaan esitel-

leet vuosina 2007 – 2008 toimineen työryhmän työstämän mallin. Malliin on sisällytetty yksityiskohtaiset suositukset muun muassa perusosaamisten määrittelemisestä sähköisten potilastietojärjestelmien käyttäjille, terveydenhuollon tiedonhallinnan koulutusvaatimuksista kaikille alan ammattilaisille sekä terveydenhuollon tiedonhallinnan osaamisista ja taidoista ammatillisena ja henkilökohtaisena pätevyytenä. Mallissa ehdotetut ydinosaamiset on ryhmitelty viiteen eri luokkaan: terveystietojen lukutaidot, sähköisten potilastietojärjestelmien käyttötaidot, terveystietojen yksityisyys ja luottamuksellisuus, terveystietojen tekninen turvallisuus sekä perustekniset atk-taidot. Malli sisältää yksityisyyteen ja luottamuksellisuuteen liittyviä osaamisia (tietosuoja) 21 kpl ja tekniseen turvallisuuteen liittyviä osaamisia (tietoturva) 8 kpl. (American Health Information Management Association & American Medical Informatics Association 2008.)

Myös Kruger ja Kearney (2006) toivat artikkelissaan esille organisaatioiden lisääntyneen tarpeen kohentaa tietoturvallisuutta. Informaatioteknologiaan liittyvien turvallisuusriskien määrän kasvu on lisännyt tietoturvatietoisuuden merkitystä luottamuksellisuuden, eheyden ja tiedon saatavuuden varmistamiseksi. Välinpitämättömyys tietoturvaa kohtaan on suurin tietojärjestelmiin kohdistuva uhka. Parasta tietoturvan toteutumista ei kuitenkaan saavuteta pelkillä teknisillä ratkaisuilla vaan yleistä tietoturvatietämystä parantamalla ja kouluttamalla kaikki käyttäjät järjestämällä kaikille koulutusta tietoturvaan liittyvistä perusasioista. Työntekijöiden tietämyksen lisäämiseksi ja suojaamiseksi tietoturvariskeiltä onkin perustettu erilaisia tietoturvallisuus ohjelmia. Jotta näillä ohjelmilla olisi myös jotain arvoa organisaatioille tietoturvallisen toiminnan tueksi, tarvitaan tutkimusmenetelmiä ja mittareita vaikuttavuuden arvioimiseksi.

Kruger ja Kearney (2006) kehittivät tietoturvatietoisuuden mittaamiseksi mallin, jonka avulla he mittasivat kansainvälisen kaivosyhtiön eri toimipisteiden henkilöstön tietoturvatietoisuutta organisaatiossa käyttöönotetun tietoturvaohjelman vaikuttavuuden arvioimiseksi. Mittarin kehittelyssä hyödynnettiin sosiaalipsykologiasta peräisin olevaa käsitystä tunteiden, käyttäytymisen ja tiedon merkitystä ihmisen opittuun taipumukseen käyttäytyä joko suotuisalla tai epäsuotuisalla tavalla eri asioita kohtaan. Edelliseen pohjautuen tietoturvatietoisuutta mitattiin kolmesta eri näkökulmasta, mitä henkilöt tietävät (tietämys), kuinka he suhtautuvat (asenne) ja kuinka he käyttäytyvät (käyttäytyminen). Kysely sisälsi monivalintakysymyksiä, joista saatujen oikeiden vastausten määrää käytettiin kunkin osa-alueen tietämyksen indikaattorina.

Mittari sisälsi 35 tietämystä, asennetta ja käyttäytymistä kuvaavaa kysymystä kuudelta eri riskialueelta kultakin kolmelta aiemmin mainitulta osa-alueelta. Tietoisuutta ja asenteita mitattiin 3-asteisella asteikolla – tosi, epätosi ja en tiedä. Käyttäytymisen osalta asteikko oli dikotominen - tosi ja epätosi. Saadut tulokset kuvattiin graafisesti ja tietämyskarttoina. Tietämyksen tasojen mittaamiseen käytettiin painotettuja keskiarvoja ja kyseisten tasojen kuvaamiseen 0 – 100 % asteikkoa, jossa tietämyksen tasoa tulkittiin kolmiportaisella asteikolla hyväksi (80 – 100 %), kohtalaiseksi (60 – 79 %) tai heikoksi (alle 60 %). (Kruger & Kearney 2006.)

Krugerin ja Kearneyn (2006) mukaan organisaatioilla on useita syitä tietoturvallisuus tietoisuuden arvioimiseksi ja mittaamiseksi. Ylin johto tarvitsee palautetta henkilöstön tietämyksen tasosta ja koulutuksen vaikuttavuudesta, tietämyksen mittaaminen tukee myös toiminnan valvontaa sekä tietoturvallisuudelle asetettuja strategisia tavoitteita. Jatkokehiteltynä kyseinen mallinnettu kvantitatiivinen mittari tarjoaakin heidän mielestään mahdollisuuksia edellisten tavoitteiden toteuttamiselle.

Appari ja Johnson (2010) selvittivät kirjallisuuskatsauksessaan terveydenhuollon tietoturvaa ja yksityisyyttä koskevan tutkimuksen nykytilaa esittäen kokonaisvaltaisen näkemyksen viimeaikaisista tutkimuksista sekä ehdottivat myös uusia mielenkiinnon kohteita tutkimuksille. Heidän tutkimuksensa taustalla oli lisääntyneestä sääntelystä ja tietojenvälityksen tarpeesta johtuva terveydenhuollon tietoturvallisuuden ja yksityisyyden merkityksen kasvaminen. Tietoturvariskien johtamisen analysoimiseksi sekä päätöksenteon ja tiedon hallinnan kuvailemiseksi tutkijat ovat käyttäneet useita teorioita. Vaikka tietoturvallisuutta onkin jo tutkittu yhä enenevässä määrin, terveydenhuollon alueella tietoturvallisuusriskeistä on kuitenkin olemassa vielä vähän tutkittua tietoa.

Appari ja Johnson (2010) tiivistivät tutkimukset neljään eri terveydenhuollon tietoturvaa ja yksityisyyttä koskevaan tutkimusalueeseen, jotka liittyivät *terveydenhuollon asiakkaisiin* sisältäen muun muassa potilastietojen hallinnan ja web –pohjaiset potilastietojärjestelmät, *palvelun tuottajiin* sisältäen muun muassa riskianalyysin ja arvioinnin, *organisaation sisäisiin* teemoihin, kuten organisaation sisäisten tietoverkkojen suunnittelu ja kehittäminen ja *yleisiin menettelytapoihin*, esimerkiksi kansallisten terveydenhuollon tietoverkkojen kehittäminen. Lopuksi tutkimuksen yhteenvetona esitettiin kultakin edellä mainituilta alueilta olemassa olevia tutkimuksia eriteltynä yhteentoista eri teemaan,

joita olivat tietoturvallisuusuhkat, terveydenhuollon asiakkaiden yksityisyys, palvelun tuottajien näkökulma sääntelyn noudattamisesta, tietoihin pääsyn valvonta, tietojen yhteentoimivuus ja tietoturva, tietoturvallisuusongelmat sähköisessä terveydenhuollon asioinnissa, tietoturvallisuusriskit tiedonvälityksessä, tiedon eheyteen liittyvät haitalliset vaikutukset terveydenhuollossa, taloudelliset riskit ja väärinkäytön valvonta, sääntelyn merkitys terveydenhuollon toiminnassa ja tietoturvallisuusriskien hallinta.

Yhteenvetona voidaan todeta, että tutkimukset olivat kohdistuneet pääasiassa potilaan yksityisyyden varmistamiseen liittyvien teknisten ratkaisujen kehittämiseen potilastietojen käsittelyprosessin eri vaiheissa. Joissakin tutkimuksissa oli myös keskitytty tarkastelemaan terveydenhuollon informaatioteknologian vaikutuksia hoidon laatuun, sen sijaan tietoturvallisuusriskien taloudelliset näkökohdat olivat jääneet vähäiselle huomiolle. Tulevaisuudessa tutkimuksen kohteiksi he ehdottivat muun muassa organisaation sisäisessä ympäristössä olevien uhkien riskien seurannan ja menettelytapojen kehittämisen, organisaation turvallisuuspolitiikan vaikuttavuuden sekä tietoturvallisuuden hallinnassa vaadittavien resurssien tutkimisen.

4 TUTKIMUSTEHTÄVÄT

Henkilöstön osaamisen kehittäminen on osa organisaation strategista toimintaa. Mittaamalla ja kartoittamalla osaamista luodaan perusta henkilöstön suunnitelmalliselle osaamisen jatkuvalle kehittämiselle. Organisaation henkilöstön tietosuoja- ja tietoturvaosaamista tarkastellaan tässä tutkimuksessa organisaation potilasrekisteritietojen käsittelyä ja tietoturvallista toimintaa ohjaavan lainsäädännön, tietoturvaoppaiden ja ohjeistusten, potilastietojen käsittelyohjeiden, yleisten tietoturvallisuusvaatimusten (luottamuksellisuus, eheys, käytettävyys) sekä näiden organisaation tietoturvapolitiikalle asettamien vaatimusten näkökulmasta. Henkilöstön nykyosaamisen ja tietämyksen tason arvioimiseksi muodostettiin edellä mainitut vaatimukset osaamisalueiksi koskien potilastietojen käsittelyä ja luovutusta, suostumuksen hallintaa, yleistä tietoturvaa, käyttöturvallisuutta ja henkilöstöturvallisuutta. Tutkimuksen tavoitteena oli suunnitella näin tunnistettujen osaamisten arvioimiseksi kyselylomake (Liite 1) ja sen avulla arvioida hoitohenkilöstön tämänhetkistä tietosuoja- ja tietoturvatietämyksen tasoa heidän itsensä kuvaamana. Tarkoituksena oli myös tunnistaa mahdollisia kehittämistarpeita liittyen hoitohenkilöstön tietosuoja- ja tietoturvatietämykseen.

Tutkimustehtävät:

1. Millainen hoitohenkilöstön tietosuoja- ja tietoturvatietämystaso on heidän itsensä arvioimana?
2. Mitä kehittämiskohteita hoitohenkilöstön tietosuoja- ja tietoturvatietämyksessä on heidän itsensä arvioimana?

5 TUTKIMUKSEN TOTEUTUS

Tässä tutkimuksessa tutkimusote on kvantitatiivinen eli määrällinen, jonka taustalla on realistinen ontologia – käsitys siitä, että todellisuus rakentuu objektiivisesti todettavista tosiasioista. Luonteeltaan kuvailevan tutkimuksen avulla selvitetään ja kuvataan tutkittavaan ilmiöön liittyviä asioita numeeristen suureiden avulla ja tuloksia havainnollistetaan taulukoin ja kuvioin. (Hirsijärvi, Remes & Sajavaara 2000, 129, 180; Heikkilä 2004, 16.) Kuvailevassa tutkimuksessa haetaan vastauksia kysymyksiin, mitä on tai mitä ovat. Tällaisen tutkimusasetelman pyrkimyksenä on kuvata prosesseja, käsitteitä, ilmiöitä tai jotakin ihmisryhmää. Näin on mahdollista ymmärtää todellisuutta sellaisena kuin se ilmenee. (Eriksson, Isola, Kyngäs, Leino-Kilpi, Lindström, Paavilainen, Pietilä, Salanterä, Vehviläinen-Julkunen & Åstedt-Kurki 2006, 43, 89 – 90.)

5.1 Tutkimusmenetelmä

Tutkimusmenetelmänä käytettiin kysely- eli survey-tutkimusta, jonka tarkoituksena on aineiston hankinta standardoidusti, kysymällä asioita täsmälleen samalla tavalla kaikilta vastaajilta. Kyselylomake koostui valmiita vastausvaihtoehtoja sisältävistä kysymyksistä sekä avoimista kysymyksistä. Mittarin laadinnassa hyödynnettiin jo olemassa olevia valmiita mittareita soveltuvin osin oman tutkimusasetelman näkökulmasta sekä organisaation tietosuojavastaavan asiantuntemusta. Kysymykset johdettiin potilastietojen käsittelyä ja tietoturvallista toimintaa ohjaavan lainsäädännön, tietoturvaoppaiden ja ohjeistusten, potilastietojen käsittelyohjeiden, yleisten tietoturvallisuusvaatimusten sekä näiden organisaation tietoturvapolitiikalle ja hoitohenkilöstön osaamiselle asettamien vaatimusten näkökulmasta.

Kyselylomake muodostui taustatiedoista sekä viidestä eri tietosuoja- ja tietoturvatietämyksen osaamisalueesta: *yleinen tietosuoja ja tietoturva*, *potilastietojen käsittely*, *suostumuksen hallinta*, *henkilöstöturvallisuus*, *käyttöturvallisuus* sekä *avoimista kysymyksistä*. Kysymyksistä 1 – 8 koskivat *taustatietoja*, kysymys 9 sisälsi 9 väittämää ja kysymykset 10 – 13 strukturoituja tai avoimia kysymyksiä koskien *yleistä tietosuoja- ja tietoturvaosaamista*, kysymys 14 sisälsi 14 väittämää ja kysymykset 15 – 24 strukturoituja tai avoimia kysymyksiä koskien *potilastietojen käsittelyyn liittyvää osaamista*, kysymys 25 sisälsi 3 väittämää ja kysymykset 26 – 27 strukturoituja tai avoimia kysymyksiä

suostumuksen hallinnan osaamista, kysymys 28 sisälsi 4 eri väittämää ja kysymykset 29 – 31 olivat strukturoituja kysymyksiä koskien *henkilöstöturvallisuusosaamista* sekä kysymys 32 sisälsi 11 väittämää *käyttöturvallisuuteen liittyvästä osaamisesta.* Väittämät olivat 3-asteisia Likert -asteikollisia väittämiä (samaa mieltä, eri mieltä, en osaa sanoa) lukuun ottamatta kysymyksiä 29 – 31, jotka sisälsivät kaksi vastausvaihtoehtoa (kyllä, en). Viimeisenä lomakkeessa oli 2 avointa kysymystä, kysymykset 33 – 34. (Taulukko 1).

TAULUKKO 1. Kyselylomakkeen sisältämät osiot ja niitä vastaavat kysymykset

Osiot	**Vastaavat kysymykset**
Taustatiedot	1 -8
Yleinen tietosuoja- ja tietoturvaosaaminen	9 - 13
Potilastietojen käsittelyn osaaminen	14 - 24
Suostumuksen hallinnan osaaminen	25 - 27
Henkilöstöturvallisuusosaaminen	28 - 31
Käyttöturvallisuusosaaminen	32
Avoimet kysymykset	33 - 34

5.2 Tutkimusaineisto ja sen hankinta

Tutkimuksen kohderyhmänä oli Kainuun maakunta -kuntayhtymän sekä perusterveydenhuollossa että erikoissairaanhoidossa työskentelevä hoitohenkilöstö, joka käyttää jotain potilastietojärjestelmää työssään. Hoitohenkilöstöllä tarkoitetaan tässä tutkimuksessa sairaanhoitajia, terveydenhoitajia, kätilöitä, perushoitajia, lähihoitajia, mielenterveyshoitajia, lastenhoitajia ja lääkintävahtimestareita. Otanta toteutettiin niin, että se edusti mahdollisimman hyvin perusjoukkoa. Perusjoukkoon kuuluvien henkilöiden kokonaismäärä oli 1517, josta valittiin systemaattisella otannalla otokseksi 500 henkilöä. Otos kattoi näin ollen 33 % perusjoukosta. Otoksen koon harkinnassa otettiin huomioon myös mahdollinen kato.

Systemaattinen otanta soveltuu otantamenetelmäksi silloin, kun perusjoukko on ominaisuuksiensa esimerkiksi mielipiteidensä, käsityksiensä tai uskomuksiensa perusteella

satunnaisessa järjestyksessä eikä joukossa tapahdu jaksoittaista vaihtelua. Tällaisia perusjoukkoja ovat esimerkiksi aakkosjärjestyksessä olevat luettelot. (Heikkilä 2004, 36; Vilkka 2007, 53.) Systemaattinen otanta on soveltuva menetelmä myös silloin, kun havaintoyksiköiden numerointi on hankalaa (Vilkka 2007, 53). Systemaattisessa otannassa poimintaväli lasketaan jakamalla perusjoukon koko otoskoolla. Tämä kokonaisluvuksi pyöristetty luku kertoo, kuinka mones havaintoyksikkö valitaan otokseen. Ensimmäinen valittava havaintoyksikkö arvotaan satunnaisesti ensimmäisestä poimintavälistä ja sen jälkeen otetaan poimintavälin mukaisesti seuraavat havaintoyksiköt mukaan otokseen. (Metsämuuronen 2006, 52; Vilkka 2007, 54.)

Perusjoukko muodostui potilastietojärjestelmiä käyttävän hoitohenkilöstön aakkosellisesta luettelosta, josta valittiin joka 3:s henkilö otokseen. Kyseinen otantaväli saatiin jakamalla perusjoukon määrä otoskoolla pyöristäen saatu luku lähimmäksi kokonaisluvuksi. Varsinainen otanta suoritettiin arpomalla ensin luvuista 1 – 3 eli otantayksikön 3:n ensimmäisen joukosta satunnaisesti yksi ja siitä eteenpäin joka 3:s yksikkö, kunnes otoskoko 500 täyttyi.

Tutkimusaineisto kerättiin 31.3. – 15.4.2011 välisenä aikana puolistrukturoidulla kyselylomakkeella hyödyntäen kohdeorganisaatiossa käytössä olevaa Webropol –ohjelmaa. Kyselyyn vastasi ensimmäisellä kyselykierroksella 94 henkilöä. Koska kyselyn ensimmäisellä kierroksella ei saatu tutkittavan ilmiön kannalta riittävää määrää vastauksia, suoritettiin uusintakyselykierros ajalla 16.4 -25.4.2011. Uusintakyselyn jälkeen vastausten lopulliseksi kokonaismääräksi tuli 124 ja vastausprosentiksi näin ollen 25 %. Näistä palautetuista vastauksista hylättiin 7 puutteellisten vastausten takia. Lisäksi 41 henkilöä oli avannut kyselyn, mutta jättänyt vastaamatta siihen.

Verkkokysely on nopea, joustava, helppo ja taloudellinen tapa kerätä aineistoa suureltakin tutkimusjoukolta. Ongelmaksi voi kuitenkin muodostua riittävän korkean vastausprosentin varmistaminen, kyselyn tekninen toimintavarmuus ja tietoturvallisuus. (Heikkilä, Hupli & Leino-Kilpi 2008.) Näihin haasteisiin varauduttiin muun muassa esitestaamalla varsinainen kyselylomake sekä kyselyn tekninen toimivuus etukäteen tutkimusryhmää vastaavilla 4 henkilöillä. Kyselyn toteuttamisen ajankohdan huolellisella suunnittelulla pyrittiin puolestaan vaikuttamaan vastausprosenttiin parantavasti. Kohdeorganisaatiossa henkilöstöllä on organisaation sähköposti käytettävissään. Kohdejoukol-

la oletettiin olevan myös tarvittavat tietotekniset taidot sekä mahdollisuus tietokoneen käyttöön.

5.3 Aineiston analysointi

Kyseessä oli Webropol –ohjelmalla toteutettu sähköpostikysely, jossa vastaukset tallentuivat suoraan tietokantaan. Näin vältyttiin erilliseltä tallennusvaiheelta, jolloin myös aineiston virheettömyys on parempi. Tietokannasta muodostetut Excel –taulukko muodossa olevat valmiiksi koodatut tiedot tarkastettiin ja tallennettiin tilastollista analyysiä varten havaintomatriisiin SPSS 17 for Windows –ohjelmistoon. Vastakkaisesti esitettyjen väittämien kohdalla kyseiset osiot koodattiin uudelleen kääntämällä ne niin, että skaalat vastaavat toisiaan, mitä positiivisempi ilmaisu, sitä positiivisempi numero. Kääntämällä osiot samansuuntaisiksi vältytään tulkintaongelmilta, osiot mittaavat tällöin samaa ilmiötä samansuuntaisesti.

Yksittäisiä muuttujia on tarkasteltu frekvenssijakaumien, keskiarvojen, prosenttilukujen, ja keskihajonnan avulla. Tulosten havainnollistamisessa on hyödynnetty soveltuvin osin Exceliä. Joidenkin muuttujien välisten yhteyksien tarkastelussa käytettiin Pearsonin korrelaatiokerrointa ja tulosten havainnollistamisessa ristiintaulukointia. Kyseisten muuttujien välisten yhteyksien tilastollista merkitsevyyttä arvioitiin seuraavalla luokituksella:

- tilastollisesti erittäin merkitsevä, kun $p \leq 0.001$
- tilastollisesti merkitsevä, kun $0.001 < p \leq 0.01$
- tilastollisesti melkein merkitsevä, kun $0.01 < p \leq 0.05$
- tilastollisesti suuntaa antava, kun $0.05 < p \leq 0.1$.

Muuttujat koodattiin 1 – 3 siten, että mitä suurempi saatu arvo on, sitä parempi tietämys asiasta vastaajalla on. Saatujen keskiarvojen tulosten tulkinnassa hyödynnettiin soveltuvin osin Kruger & Kerneyn (2006) kehittelemää tietämyksen tason arvioimiseksi seuraavaa kolmiportaista asteikkoa:

- hyvä tietämystaso, kun tulos 80 – 100 %
- kohtalainen tietämystaso, kun tulos on 60 – 79 %
- heikko tietämystaso, kun tulos on alle 60 %,

jolloin keskiarvolukuina tulkittuna tietämyksen tasot ovat vastaavasti seuraavat:

- hyvä tietämystaso, kun keskiarvo 2.4 – 3.0

- kohtalainen tietämystaso, kun keskiarvo 1.8 – 2.39
- heikko tietämystaso, kun keskiarvo alle 1.8.

Keskihajonnan avulla voidaan arvioida yksittäisten havaintoarvojen sijaintia suhteessa havaintoarvojen keskiarvoon. Mitä suurempi keskihajonta, sitä enemmän havaintoarvoissa on vaihtelua. Ne ilmentävät vastaajien mielipiteiden yksimielisyyttä esitettyihin väittämiin. Yksimielisyyden astetta tulkittiin seuraavasti:

- vastaajat lähes täysin tai täysin yksimielisiä, kun keskihajonta < 0.7
- vastaajat melko yksimielisiä, kun keskihajonta 0.7 – 0.99
- vastaajat ovat melko erimielisiä, kun keskihajonta 1 – 1.19
- vastaajat ovat erittäin erimielisiä, kun keskihajonta >1.2.

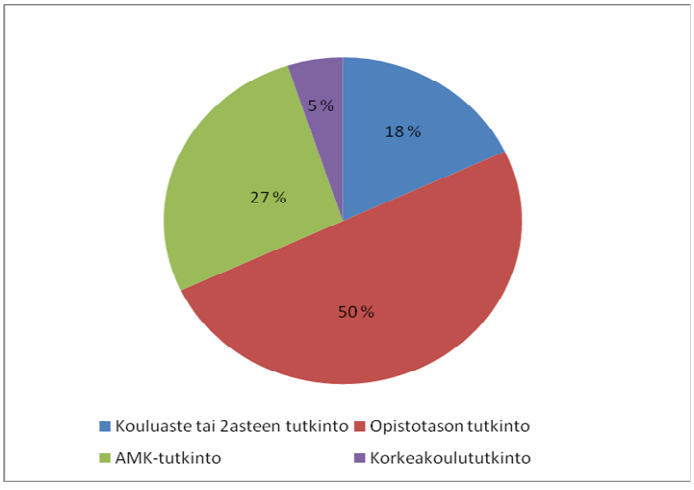
Aineiston täydentämiseksi ja aihepiirin eri ulottuvuuksien kartoittamiseksi kyselylomake sisälsi myös avoimia kysymyksiä, joissa pyydettiin perusteluita mielipiteisiin, esittämään käytännön esimerkkejä sekä kuvaamaan käytännön toimintatapoja. Avointen kysymysten analysoinnissa käytettiin sisällön analyysiä muodostamalla vastauksista käsitteellisiä ja sisällöllisiä kokonaisuuksia, joita rikastutettiin esittämällä tuloksissa suoria lainauksia alkuperäisistä vastauksista.

6 TUTKIMUKSEN TULOKSET

Tässä tutkimuksessa tavoitteena oli saada tietoa hoitohenkilöstön tietosuoja- ja tietoturvaosaamisesta ja tietämyksestä, minkälainen heidän tietosuoja- ja tietoturvaosaamisensa taso oli vastaajien itsensä kokemana ja arvioimana. Näin tietosuoja- tietoturvatietämyksen eri osaamisalueilta saadun tiedon pohjalta mahdollistettiin ennalta määritellyn kolmiportaisen asteikon avulla osaamisen arviointi. Toisaalta tutkimuksen tavoitteena oli myös selvittää, mitä kehittämiskohteita hoitohenkilöstön tietosuoja- ja tietoturvatietämyksessä ilmenee, minkälaisissa osaamisissa on eniten kehittämisen varaa. Tulokset esitellään kyselylomakkeen sisältämien teemojen mukaisessa järjestyksessä.

6.1 Vastaajien taustatiedot

Kyselyyn vastasi hyväksytysti 117 henkilöä, joista 65 (56 %) työskenteli perusterveydenhuollossa ja 52 (44 %) erikoissairaanhoidossa. Heistä suurimmalla osalla oli vakituinen työsuhde (95 %). Koulutuksen suhteen suurimman vastaajaryhmän eli puolet (50 %) muodostivat opistotason tutkinnon suorittaneet. Ammattikorkeakoulututkinnon suorittaneita oli 27 prosenttia, kouluasteen tai 2.asteen tutkinnon suorittaneita 18 sekä korkeakoulututkinnon suorittaneita 5 prosenttia. Kaksi vastaajaa oli ilmoittanut kaksi tutkintoa, näistä huomioitiin vastaukseksi korkeampi tutkinto. (Kuvio 5).



KUVIO 5. Vastaajien ammatillinen koulutus

Kaikki vastaajat käyttivät potilastietojärjestelmiä työssään. Useita kertoja päivässä kyseisiä tietojärjestelmiä käytti 109 (93 %) vastaajaa ja muutaman kerran viikossa tai harvemmin niitä käytti 8 (7 %) kyselyyn vastanneista. Kysyttäessä potilastietojärjestelmien käyttöaikaa, enemmistön muodosti yli 10 vuotta järjestelmiä käyttäneet (37 %). Toiseksi suurimman ryhmän muodosti 6 – 10 vuoden käyttökokemuksen omaava hoitohenkilöstö (32 %). Alle kuusi vuotta potilastietojärjestelmiä työssään käyttäneitä oli 31 prosenttia vastaajista.

Työnantajan organisaatiossa järjestämiin tietosuoja- ja tietoturvakoulutuksiin useammin kuin kerran oli osallistunut neljännes (25 %) vastaajista ja kerran 43 (37 %) vastaajaa. Koulutuksiin osallistumattomia oli suurin ryhmä, 45 henkilöä eli 38 prosenttia kyselyyn vastanneista. Ammatilliseen koulutukseen sisältyviä tietosuojaan ja –turvaan liittyviä opintoja oli ollut runsaasti 3 prosentilla vastaajista. Jonkin verran niitä oli sisältynyt 44 prosentilla koulutukseen ja vastaajista 39 prosenttia ilmoitti niitä olleen vähän. Tietosuoja- ja turvaan liittyvää opetusta koulutuksessaan puolestaan ei ollut saanut lainkaan 14 prosenttia kyselyyn vastanneista.

TAULUKKO 2. Opintoihin sisältyvien tietosuoja- ja tietoturvaopintojen määrän jakautuminen eri ammatillisissa koulutuksissa (n=117)

	Tietosuoja ja tietoturvaopinnot				Yhteensä
	Ei lainkaan (%)	Vähän (%)	Jonkin verran (%)	Runsaasti (%)	(%)
Kouluaste tai 2.asteen tutkinto	19	43	38	0	18
Opistotason tutkinto	19	43	38	0	50
AMK -tutkinto	3	28	60	9	27
Korkeakoulututkinto	0	50	50	0	5
Yhteensä	14	39	44	3	100

Sekä kouluasteen tai 2.asteen tutkinnon että opistotason tutkinnon suorittaneista 62 prosenttia ilmoitti tietosuoja- ja tietoturvaopintoja olleen vähän tai ei lainkaan. Sen sijaan AMK -tutkinnon suorittaneista vain 31 prosentilla ja 50 prosentilla korkeakoulututkinnon suorittaneista niitä oli ollut vähän tai ei lainkaan. Eniten kyseisiä opintoja oli sisältynyt AMK -koulutukseen, jopa 69 prosenttia ammattikorkeakoulututkinnon suorittaneista ilmoitti niitä ollen jonkin verran tai runsaasti. (Taulukko 2).

Enemmistö (67 %) arvioi oman tietosuoja- ja tietoturvatietämyksensä hyväksi. Erittäin hyvänä sitä piti 5 prosenttia vastaajista ja huono se oli 17 prosentin mielestä. Erittäin huonona tietämystään ei pitänyt kukaan, 11 prosenttia ei vastaavasti osannut arvioida tietosuoja- ja tietoturvatietämystään lainkaan. (Taulukko 3).

TAULUKKO 3. Osaamisen taso vastaajien itsensä arvioimana

Osaamisen taso	**Frek-venssi**	**%**
Erittäin hyvä	6	5
Hyvä	78	67
Huono	20	17
En osaa sanoa	13	11
Yhteensä	117	100

Tarkasteltaessa ammatilliseen koulutukseen sisältyvien tietosuoja- ja tietoturvaopintojen määrän yhteyttä osaamisen tasoon Pearsonin korrelaation avulla, opintojen määrän ja arvioidun osaamisen tason välinen yhteys oli tilastollisesti merkitsevä ($p< 0.05$). Mitä enemmän opintoja sisältyi ammatilliseen koulutukseen, sitä paremmaksi vastaajat arvioivat oman osaamisen tasonsa. Sen sijaan osaamisen tasolla ja organisaation järjestämiin koulutuksiin osallistumisen välillä ei ilmennyt yhteyttä ($p=0.138$).

6.2 Yleinen tietosuoja- ja tietoturvaosaaminen

Vastaajien yleistä tietosuoja- ja tietoturvatietämystä kysyttiin väittämillä, jotka koskivat potilasasiakirjojen käsittelyyn ja merkintöjen tekemiseen liittyviä lainsäädännöstä johdettuja yleisiä periaatteita sekä potilaan informointivelvoitetta. Potilasasiakirjojen tietoja pidettiinkin lähes täysin yksimielisesti (99 %) salassa pidettävinä. Vastaajista 95 pro-

senttia oli samaa mieltä myös siitä, että salassapitovelvollisuus jatkuu palvelusuhteen tai tehtävän päättymisen jälkeenkin. Loput 5 prosenttia olivat sitä mieltä, että salassapitovelvollisuus päättyy silloin, kun palvelusuhde tai tehtäväkin päättyy.(Kuvio 6).

Potilasasiakirjoissa olevia tietoja piti arkaluonteisina suurin osa vastaajista (84 %) ja kolme neljästä vastaajasta (74 %) oli samaa mieltä siitä, että niihin merkitään vain potilaan hoidon kannalta välttämättömiä arkaluonteisia tietoja. Enemmistön (86 %) mielestä potilasasiakirjoihin saa merkitä vain potilasta itseään koskevia tietoja. Eri mieltä oli joka kymmenes vastaaja ja 3 prosenttia puolestaan ei osannut sanoa mielipidettään. Potilasasiakirjoihin tehtävien vain käyttötarkoituksensa kannalta tarpeellisia tietoja koskevien merkintöjen tekemisestä yleisesti hyväksyttyjä käsitteitä ja lyhenteitä käyttäen enemmistö (92 %) vastaajista oli samaa mieltä. Loput vajaa 10 prosenttia olivat eri mieltä tai eivät osanneet sanoa mielipidettään.

Merkintöjen teko-oikeutta potilasasiakirjoihin koskevat väittämät kohdistuivat yleisesti oikeuteen tehdä merkintöjä sekä terveydenhuollon opiskelijoiden merkintöjen teko-oikeuteen. Lähtökohtaisesti potilasasiakirjamerkintöjä saavat tehdä potilaan osallistuvat terveydenhuollon ammattihenkilöt. Heidän ohella merkintöjä saavat tehdä myös muut potilaan hoitoon osallistuvat henkilöt terveydenhuollon ammattihenkilön antamien ohjeiden mukaisesti. Merkittävä osa kyselyyn vastanneista (91 %) oli sitä mieltä, että potilasasiakirjoihin saa tehdä merkintöjä vain potilaan hoitoon osallistuvat terveydenhuollon ammattihenkilöt. Eri mieltä oli 8 prosenttia ja vain 1 prosentti ei osannut sanoa. Vastaavasti terveydenhuollon opiskelijoita koskevan väittämän kohdalla lähes kaikkien (96 %) vastaajien mielestä opiskelijoiden tekemät merkinnät hyväksyy työyksikössä hänen ohjaajansa tai tämän valtuuttama henkilö.

Kysyttäessä vastaajien tietoisuutta potilasasiakirjoihin tehtävien merkintöjen oikeellisuuteen liittyvistä vaatimuksista, suurimman osan (96 %) mielestä tehdyistä potilasasiakirjamerkinnöistä ja niiden oikeellisuudesta vastaa käyttäjätunnuksen mukainen henkilö. Perusteluina nämä vastaajat useimmiten esittivät sen, että käyttäjätunnukset ovat henkilökohtaisia ja siten jokainen on vastuussa niiden käyttämisestä.

”Käyttäjätunnus on henkilökohtainen eli jokainen vastaa omista merkinnöistä”

”Jokainen kirjaa vain omilla tunnuksillaan”

Toisaalta vastaajien mukaan tietojen oikeellisuus ja merkintöjen tekijä tulee voida jäljittää.

”Muuten tietojen oikeellisuutta ei voi varmistaa eikä jäljittää tarvittaessa”

”Muuten ei voi olla varma merkintöjen tekijästä”

Muita esille tulleita perusteluja olivat muun muassa kirjaajan oman oikeusturvan toteutuminen sekä olemassa olevan kirjallisen ohjeen noudattaminen.

Laissa määritellyn rekisterinpitäjän informointivelvoitteen mukaisesti potilaalle tulee antaa tietoa siitä, miten hänen henkilötietojaan käsitellään kulloinkin hoitavassa yksikössä. Enemmistön (83 %) mielestä potilaan tullessa sairaalaan potilaalle tulee kertoa hänen henkilötietojensa käsittelystä. Vastaajista kuitenkin 14 prosenttia oli eri mieltä ja 3 prosenttia ei osannut sanoa, tarvitseeko potilasta informoida hänen henkilötietojensa käsittelystä.

Perusteluina potilaan informoinnille ilmoitettiin pääsääntöisesti potilaan tiedonsaantioikeus ja lain edellyttämä velvoite. Perusteluissa tuotiin esille myös se, että ilman potilaan lupaa tietoja ei saa luovuttaa.

”Potilaalla on oikeus tietää omien henkilötietojensa käsittelystä ja niin halutessaan myös oikeus nähdä hänen hoitoonsa liittyvät kirjaukset”

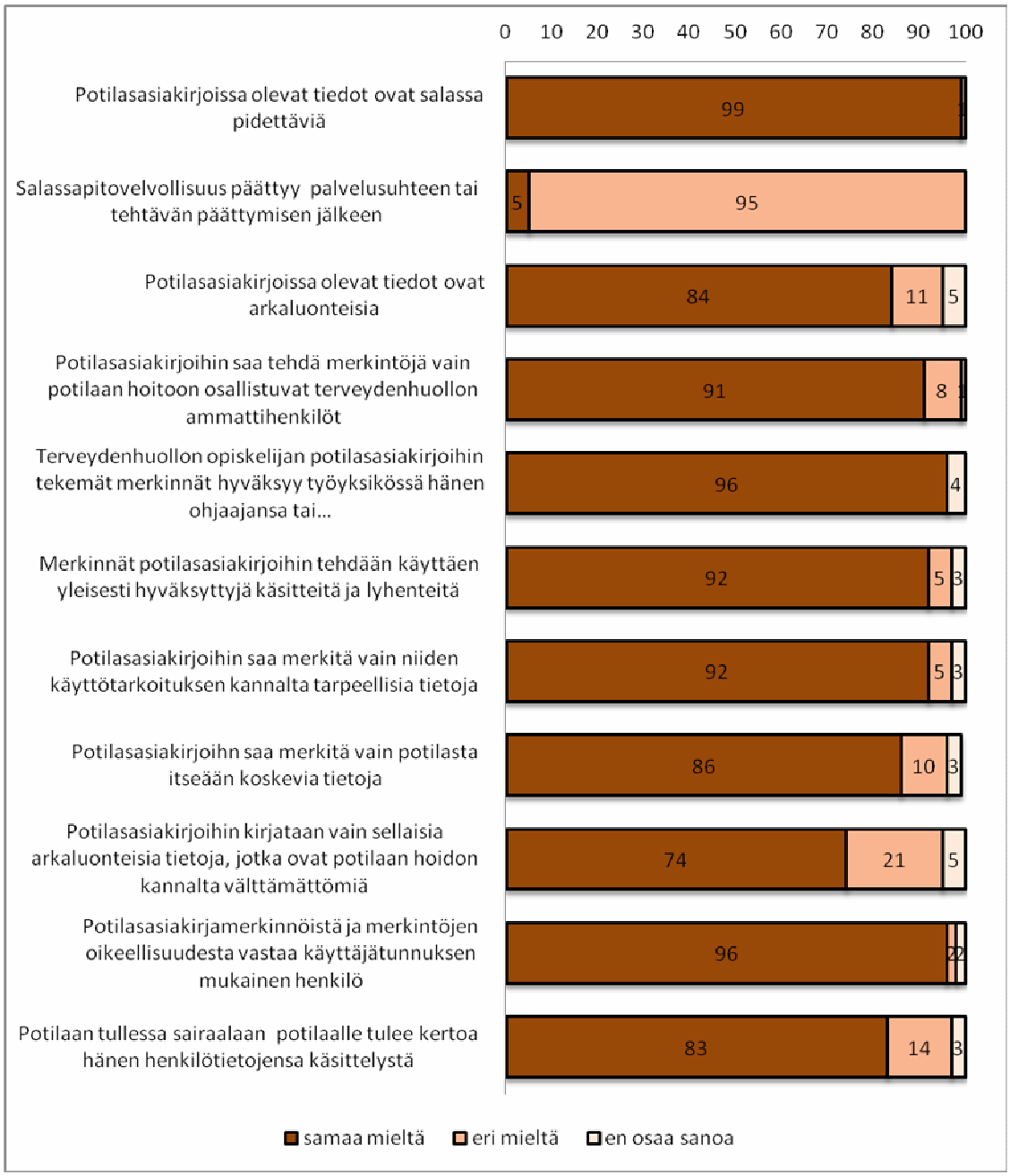
”Laki velvoittaa”

”Potilaalta tulee kysyä mm. kenelle hänen tietojaan saa luovuttaa”

Vastaavasti ne loput 17 prosenttia vastaajista, jotka olivat väittämästä eri mieltä tai eivät osanneet kertoa mielipidettään, perustelivat vastauksiaan muun muassa seuraavasti:

”Ei taida olla aikaa tommoseen. Mikäli potilas kysyy henkilötietojen käsittelystä, silloin tulee kertoa”

”En muista määräystä asiasta”



KUVIO 6. Yleistä tietosuojaa ja tietoturvaa koskevien vastausten prosentuaalinen jakauma

Tarkasteltaessa yleiseen tietosuojaan ja tietoturvaan liittyviä tunnuslukuja (Taulukko 4) voidaan todeta, että vastaajat olivat kaikkein yksimielisimpiä potilasasiakirjojen tietojen salassa pidettävyydessä (s=0.09). Eniten hajontaa oli mielipiteissä potilaan henkilötietojen informoinnista (s=0.70). Vastausten keskiarvot vaihtelivat välillä 2.69 – 2.99, joten tietämyksen tasoa voidaan pitää hyvänä (ka > 2.39) yleisen tietosuojan ja tietoturvan osalta, kokonaiskeskiarvon ollessa 2.86.

TAULUKKO 4. Yleistä tietosuoja- ja tietoturvaosaamista koskevien vastausten tunnuslukuja

Yleinen tietosuoja ja tietoturvaosaaminen	N	Keskiarvo	Keskihajonta
Potilasasiakirjoissa olevat tiedot ovat salassa pidettäviä	117	2,99	0,09
Salassapitovelvollisuus päättyy palvelusuhteen tai tehtävän päättymisen jälkeen	117	2,95	0,22
Potilasasiakirjoissa olevat tiedot ovat arkaluonteisia	117	2,79	0,52
Potilasasiakirjoihin saa tehdä merkintöjä vain potilaan hoitoon osallistuvat terveydenhuollon ammattihenkilöt	117	2,91	0,32
Terveydenhuollon opiskelijan potilasasiakirjoihin tekemät merkinnät hyväksyy työyksikössä hänen ohjaajansa tai tämän valtuuttama henkilö	117	2,91	0,41
Merkinnät potilasasiakirjoihin tehdään käyttäen yleisesti tunnettuja ja hyväksyttyjä käsitteitä ja lyhenteitä	117	2,90	0,38
Potilasasiakirjoihin saa merkitä vain niiden käyttötarkoituksen kannalta tarpeellisia tietoja	117	2,88	0,42
Potilasasiakirjoihin saa merkitä vain potilasta itseään koskevia tietoja	117	2,83	0,46
Potilasasiakirjoihin kirjataan vain sellaisia arkaluonteisia tietoja, jotka ovat potilaan hoidon kannalta välttämättömiä	117	2,69	0,56
Potilasasiakirjamerkinöistä ja merkintöjen oikeellisuudesta vastaa käyttäjätunnuksen mukainen henkilö	117	2,95	0,29
Potilaan tullessa sairaalaan potilaalle tulee kertoa hänen henkilötietojensa käsittelystä	117	2,69	0,70

6.3 Potilastietojen käsittelyn osaaminen

Potilastietojen käsittelyä koskevat väittämät kohdistuivat potilastietojen käyttöön, luovuttamiseen, katseluun sekä korjaamiseen liittyviin periaatteisiin. Enemmistön (87 %) mielestä potilastietoja saa käsitellä ilman potilaan suostumusta vain työtehtävien tai vastuun edellyttämässä laajuudessa, 13 prosenttia vastaajista ei osannut sanoa tai oli eri mieltä asiasta. Kolme neljästä vastaajasta (74 %) oli sitä mieltä, että potilastietoja voi käsitellä ilman potilaan suostumusta vain osallistuessaan potilaan hoitoon tai siihen liittyviin tehtäviin, mutta jopa neljäsosa vastaajista (26 %) oli väittämästä eri mieltä tai ei osannut ottaa kantaa siihen. (Kuvio 7).

Merkittävän suuren osan (86 %) kyselyyn vastanneen mielestä potilasasiakirjamerkinnät tulee tehdä aina viivytyksettä. Lähes kaikkien vastaajien (98 %) mielestä virheelliset tiedot tulee korjata, enemmistö (94 %) oli tietoinen myös virheellisten tietojen korjaamisesta jäävästä merkinnästä potilasasiakirjojen taustatiedostoon. Virheellisten tietojen

poistamisen kannalla oli puolestaan vain 11 prosenttia vastaajista ja yhtä moni (11 %) oli epätietoinen menettelytavasta. Suurin osa (78 %) oli kuitenkin sitä mieltä, että virheellisiä tietoja ei saa poistaa.

Lähes kolmanneksen (29 %) mielestä potilaalla on oikeus kieltää hoidon kannalta tarpeellisten tietojen kirjaaminen potilasasiakirjoihin. Merkittävä enemmistö (60 %) oli kuitenkin eri mieltä väittämästä – potilas ei voi kieltää hoitonsa kannalta tarpeellisten tietojen kirjaamista potilasasiakirjoihin. Sen sijaan melkein kaikki vastaajat (97 %) olivat samaa mieltä potilaan oikeudesta tarkastaa omia potilasasiakirjojaan.

Hoitohenkilöstön tietoisuutta potilasasiakirjojen tietoihin liittyvästä katseluoikeudesta mitattiin kahdella väittämällä. Omien potilastietojen katselu potilastietojärjestelmästä ei ollut enemmistön (91 %) mielestä sallittua. Kuitenkin 7 prosenttia vastaajista sallisi hoitohenkilökunnan katsella omia potilastietojaan ja 2 prosenttia ei osannut kertoa mielipidettään. Sen sijaan vastaajat olivat melkein täysin yksimielisiä (98 %) siitä, että hoitohenkilöstö ei saa katsella sellaisten potilaiden tietoja, joihin heillä ei ole hoitosuhdetta. Mielipiteeseen kysyttiin perustelua avoimena kysymyksenä. Perusteluina pääsääntöisesti esitettiin muun muassa lainsäädännön asettama vaatimus - ainoastaan niiden potilaiden tietoja saa katsella, joiden hoitoon osallistuu.

”Saa katsella vain hoitamansa potilaan sen hetkisen hoidon kannalta tarpeellisia tietoja”

”Laki kieltää katsomasta”

”Tiedot on tarkoitettu oikeanlaisen hoidon saamisen turvaamiseksi eikä uteliaiden tiedonhalun täyttämiseksi”

Potilasasiakirjoihin sisältyvien tietojen luovutusperiaatteita mitattiin useasta eri näkökulmasta. Väittämät koskivat tietojen luovutusta yleisesti koskevia periaatteita, tietojen luovuttamista alaikäisen potilaan huoltajalle, omaisille sekä viranomaisille. Potilastietoja luovutettaessa suurin osa (92 %) kyselyyn vastanneista tarkastaisi tietojen vastaanottajan oikeuden saada tietoja. Samoin lähes yhtä monen (93 %) mielestä tietojen luovuttamisesta tulee tehdä asianmukaiset merkinnät potilasasiakirjoihin. Vastaajista vajaan neljänneksen (23 %) mielestä potilaalta ei tarvita erillistä suostumusta silloin, kun potilastietoja luovutetaan häneen hoitosuhteessa olevalle. Sen sijaan 74 prosenttia oli sitä mieltä, että potilaalta tulee pyytää erillinen suostumus kyseisessä tilanteessa.

Potilastietojen luovuttajan vastuu luovutuksen laillisuudesta oli erittäin hyvin ja tietosuojan varmistamisesta hyvin vastaajien tiedossa. Enemmistön (95 %) mielestä tietojen luovutusta koskeva laillisuus tulee varmistaa, lähes yhtä suuri enemmistö (88 %) oli tietoinen myös tietoja koskevan tietosuojan varmistamisvelvollisuudesta. Käytännön menettelytapoja tietojen luovutuksen laillisuuden ja tietosuojan toteutumisen varmistamiseksi kysyttiin kummassakin tapauksessa avoimilla kysymyksillä. Tietojen laillinen luovuttaminen varmistettaisiin tarvittaessa kysymällä neuvoa usealta eri taholta esimerkiksi lääkäriltä, esimieheltä, arkistohenkilökunnalta, tietosuojasta tietävältä henkilöltä tai työtovereilta.

”Kysyn varmistuksen usealta taholta”

”Lääkärin tai esimiehen kanssa keskustellaan ja mietitään”

”Otan selvää, mitä laki sanoo asiasta”

Yhtenä menettelytapana esitettiin myös tietojen luovuttamista koskevan luvan tarkistaminen potilaspapereista tai kysymällä potilaalta itseltään. Toisaalta myös vastaajien mielestä tulee varmistaa kenelle luovuttaa ja mihin tarkoitukseen tietoja tarvitaan.

”Varmistan potilaalta tai potilaspapereista kenelle potilas on antanut luvan luovuttaa tietojaan”

”Tarkistaa kyseisen henkilön henkilöllisyys ja oikeus tietojen saamiseen. Tarkistaa kenellä oikeus nähdä potilastiedot”

”Selvittämällä luovutuksen syy ja riittävät perusteet, lähinnä kyselemällä”

Tietosuojan toteutuminen varmistetaan vastaajien mielestä tarkastamalla olemassa oleva potilaan antama suostumus tietojen luovuttamiseen sekä ottamalla selville lainsäädännön mukaiset vaatimukset tietojen luovuttamiselle. Tiedot lähetetään suljetussa kirjekuoressa käyttäen ensisijaisesti sisäistä postia tai vaihtoehtoisesti luovuttamalla tiedot potilaalle itselleen edelleen toimitettavaksi.

”Tiedot lähetetään sovittuun osoitteeseen suljetussa kirjekuoressa, kun asiakkaalta on ensin saatu lupa tietojen siirtoon”

”Tarkistan laista”

”Pääsääntöisesti pyrin antamaan potilastiedot suoraan asiakkaalle ja hän saa itse ne toimittaa eteenpäin”

Viranomaisille luovutettavia tietoja koskeva erityislainsäädännön olemassaolo oli yleisesti hyvin tiedossa vastaajien keskuudessa, 84 prosenttia tiesi olemassa olevasta tietojen luovuttamiseen liittyvästä lainsäädännöstä. Kuitenkin silti jopa kolmannes (34 %) joko ei osannut sanoa mielipidettään tai luovuttaisi tietoja viranomaisille aina niitä pyydettäessä. Loput 66 prosenttia vastaajista luovuttaisi potilastietoja viranomaisille joitakin poikkeustapauksia lukuun ottamatta vain potilaan suostumuksella.

”Viranomaisia on monenlaisia ja potilastietojen luovuttamisen lupa on aina selvitettävä ennen kuin niitä kenellekään antaa. Ei edes poliisille”

”Kirjallinen selvitys, kuka pyytää ja mitä varten”

”Viranomaisella pitää olla peruste potilastietojen pyytämisessä”

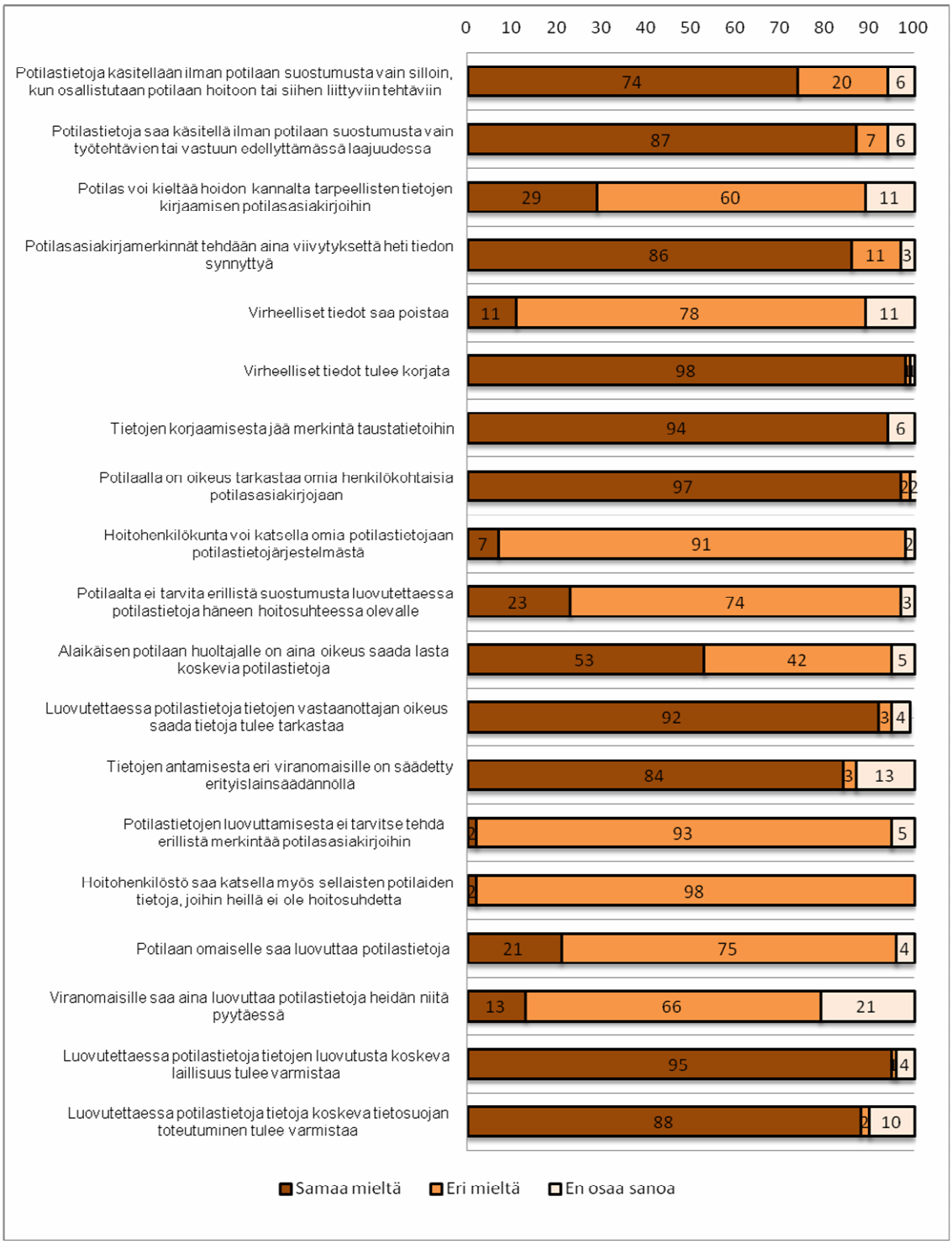
”Jos potilas antaa luvan”

Alaikäisen potilaan huoltajan oikeudesta saada aina lasta koskevia tietoja jakoi mielipiteitä tasaisemmin. Vajaa puolet vastaajista (42 %) oli eri mieltä omaisten tietojen saantioikeudesta ja 5 prosenttia ei osannut ilmaista kantaansa. Loput kyselyyn osallistujista (53 %) oli sitä mieltä, että alaikäisen potilaan huoltajalla on aina oikeus saada lasta koskevia potilastietoja. Potilaan omaiselle ei luovuttaisi potilastietoja kolme vastaajaa neljästä (75 %), mutta loppu neljännes (25 %) joko luovuttaisi tietoja tai ei osannut sanoa kantaansa. Perusteluna mielipiteelleen eri mieltä väittämän kanssa olleet (75 %) esittivät lähes yksimielisesti sen, että tietoja saa antaa vain potilaan luvalla.

”Potilaalta tulee olla suostumus tietojen antamiseen”

Toisaalta myös potilastietoja omaisille luovuttavat perustelivat kantaansa samoilla asioilla.

”Mikäli potilas on myöntänyt luvan”



KUVIO 7. Potilastietojen käsittelyä koskevien vastausten prosentuaalinen jakauma

Potilastietojen käsittelyä koskevien lähes kaikkien väittämien kohdalla vastaajat olivat olleet yksimielisiä (s=0.13 – 0.39), eniten hajontaa (s=0.82) (Taulukko 5) esiintyi vastauksessa kysymykseen, jossa kysyttiin mielipiteitä potilastietojen luovuttamisesta viranomaisille. Kaikkien vastausten keskiarvot vaihtelivat puolestaan välillä 2.20 – 2.98 ja

kahden väittämän kohdalla keskiarvot ovat alle 2.4. Kyseiset väittämät koskivat erillisen suostumuksen tarvetta luovutettaessa potilastietoja hoitosuhteessa olevalle sekä alaikäisen huoltajan oikeutta saada lasta koskevia tietoja. Näiden väittämien osalta tietämyksen tasoa voidaankin pitää kohtalaisena. Muilta osin tietämystä voidaan pitää hyvänä, keskiarvot > 2.39, osion kokonaiskeskiarvon ollessa 2.71.

TAULUKKO 5. Potilastietojen käsittelyn osaamista koskevia tunnuslukuja

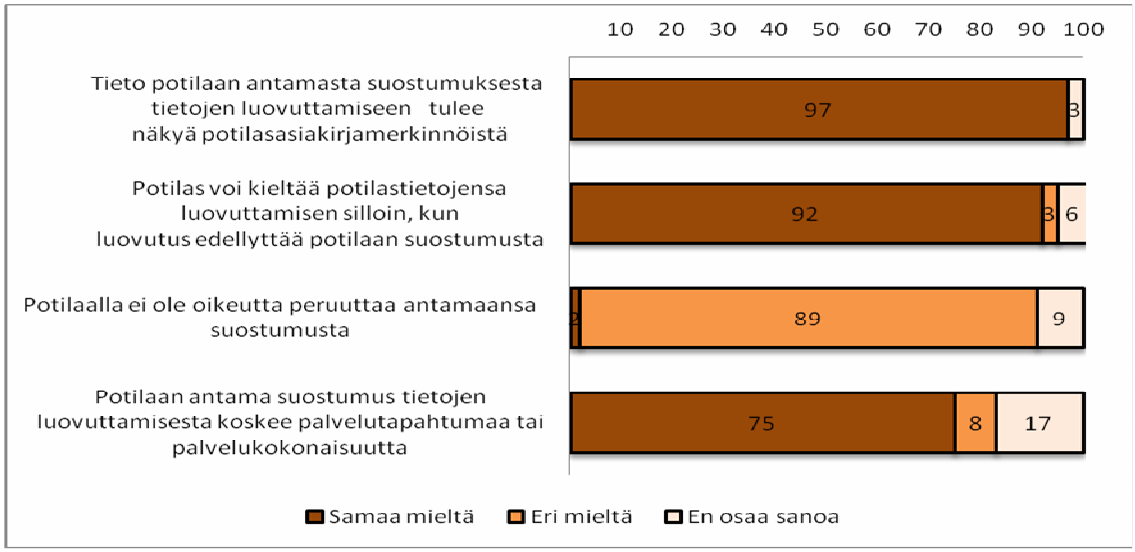
Potilastietojen käsittelyn osaaminen	N	Keskiarvo	Keskihajonta
Potilastietoja käsitellään ilman potilaan suostumusta vain silloin, kun osallistutaan potilaan hoitoon tai siihen liittyviin tehtäviin	117	2,68	0,58
Potilastietoja saa käsitellä ilman potilaan suostumusta vain työtehtävien tai vastuun edellyttämässä laajuudessa	117	2,81	0,52
Potilas voi kieltää hoidon kannalta tarpeellisten tietojen kirjaamisen potilasasiakirjoihin	117	2,49	0,69
Potilasasiakirjamerkinnät tehdään aina viivytyksettä heti tiedon synnyttyä	117	2,84	0,43
Virheelliset tiedot saa poistaa	117	2,67	0,67
Virheelliset tiedot tulee korjata	117	2,97	0,22
Tietojen korjaamisesta jää merkintä taustatietoihin	117	2,88	0,48
Potilaalla on oikeus tarkastaa omia henkilökohtaisia potilasasiakirjojaan	117	2,95	0,29
Hoitohenkilökunta voi katsella omia potilastietojaan potilastietojärjestelmästä	117	2,90	0,36
Potilaalta ei tarvita erillistä suostumusta luovutettaessa potilastietoja häneen hoitosuhteessa olevalle	117	2,20	0,46
Alaikäisen potilaan huoltajalla on aina oikeus saada lasta koskevia potilastietoja	117	2,37	0,58
Luovutettaessa potilastietoja tietojen vastanottajan oikeus saada tietoja tulee tarkastaa	117	2,88	0,44
Tietojen antamisesta eri viranomaisille on säädetty erityislainsäädännössä	117	2,71	0,68
Potilastietojen luovuttamisesta ei tarvitse tehdä erillistä merkintää potilasasiakirjoihin	117	2,88	0,46
Hoitohenkilöstö saa katsella myös sellaisten potilaiden tietoja, joihin heillä ei ole hoitosuhdetta	117	2,98	0,13
Potilaan omaiselle saa luovuttaa potilastietoja	117	2,71	0,54
Viranomaiselle saa aina luovuttaa potilastietoja heidän niitä pyytäessä	117	2,46	0,82
Luovutettaessa potilastietoja tietojen luovutusta koskeva laillisuus tulee varmistaa	117	2,91	0,41
Luovutettaessa potilastietoja tietoja koskeva tietosuojan toteutuminen tulee varmistaa	117	2,78	0,62

6.4 Suostumuksen hallinnan osaaminen

Suostumuksen hallintaan liittyvien väittämien avulla tarkasteltiin vastaajien tietämystä terveydenhuollon potilasasiakirjatietoja koskevista lainsäädännön asettamista luovutussäännöistä. Lähes kaikki vastaajat (97 %) olivat samaa mieltä siitä, että potilasasiakirjamerkinnöistä tulee ilmetä potilaan antama suostumus tietojen luovuttamiseen. Melkein yhtä monen vastaajan (92 %) mielestä potilaalla on oikeus kieltää potilastietojensa luovuttaminen silloin, kun tietojen luovuttaminen edellyttää potilaan suostumusta. Enemmistö (89 %) vastaajista oli myös tietoisia potilaan oikeudesta peruuttaa antamansa suostumus. Kolme neljästä kyselyyn vastanneesta oli tietoisia siitä, että tietojen luovuttamista koskeva suostumus koskee palvelutapahtumaa tai palvelukokonaisuutta.(Kuvio 8). Näiden vastaajien perustelut pohjautuivat potilaiden itsemääräämisoikeuteen ja tarpeellisuusvaatimukseen.

”Potilas saa itse päättää, annetaanko tietoja vain esim. johonkin sairauteen liittyvät asiat, vai kaikki tiedot”

”Kaikkia tietoja ei automaattisesti anneta, vaan kussakin tilanteessa tarpeelliset rajatut tiedot”



KUVIO 8. Suostumuksen hallintaan liittyvien vastausten prosentuaalinen jakauma

Suostumuksen hallintaan liittyvien väittämien kohdalla vastaajat olivat kolmesta ensimmäisestä väittämästä yksimielisempiä (s=0.32 – 0.60) (Taulukko 6), eniten hajontaa

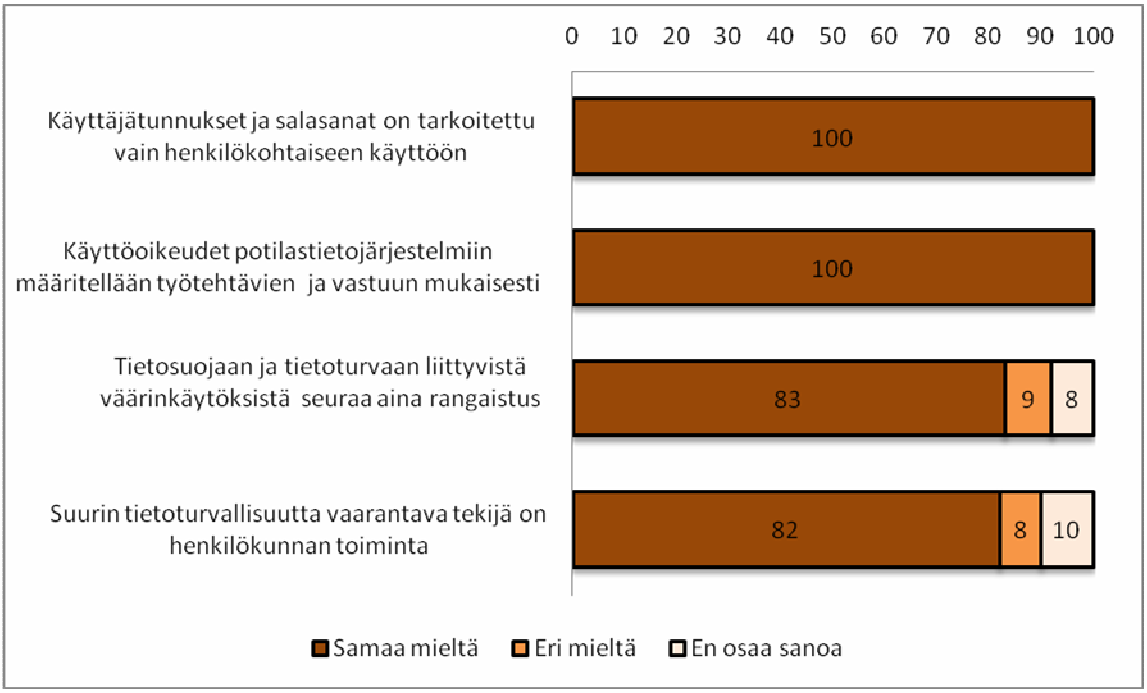
vastauksissa esiintyi potilaan antaman suostumuksen laajuutta koskevan väittämän kohdalla (s=0.77). Kaikkien havaintojen kohdalla keskiarvojen vaihteluväli oli 2.59 – 2.95, kokonaiskeskiarvon ollessa 2.79. Suostumuksen hallintaan liittyvää tietämyksen tasoa voidaankin pitää hyvänä (keskiarvot > 2.39).

TAULUKKKO 6. Suostumuksen hallinnan osaamista koskevien vastausten tunnusluvut

Suostumuksen hallinnan osaaminen	N	Keskiarvo	Keskihajonta
Tieto potilaan antamasta suostumuksesta tietojen luovuttamiseen tulee näkyä potilasasiakirjamerkinnöistä	117	2,95	0,32
Potilas voi kieltää potilastietojensa luovuttamisen silloin, kun luovutus edellyttää potilaan suostumusta	117	2,85	0,50
Potilaalla ei ole oikeutta peruuttaa antamaansa suostumusta	117	2,80	0,60
Potilaan antama suostumus tietojen luovuttamisesta koskee palvelutapahtumaa tai palvelukokonaisuutta	117	2,59	0,77

6.5 Henkilöstöturvallisuusosaaminen

Henkilöstöturvallisuutta koskevat väittämät kohdistuivat henkilöstöön liittyviin tietoriskien hallintaan. Kaikki vastaajat olivat täysin yksimielisiä (100 %) käyttäjätunnusten ja salasanojen henkilökohtaisuudesta sekä potilastietojärjestelmien käyttöoikeuksien määrittymisestä työtehtävien ja vastuun mukaisesti. Suuren enemmistön (82 %) mielestä henkilökunnan toiminta on suurin tietoturvallisuutta vaarantava tekijä ja yhtä monen (83 %) mielestä tietosuojaan ja tietoturvaan liittyvistä väärinkäytöksistä on seurauksena aina rangaistus. (Kuvio 9).



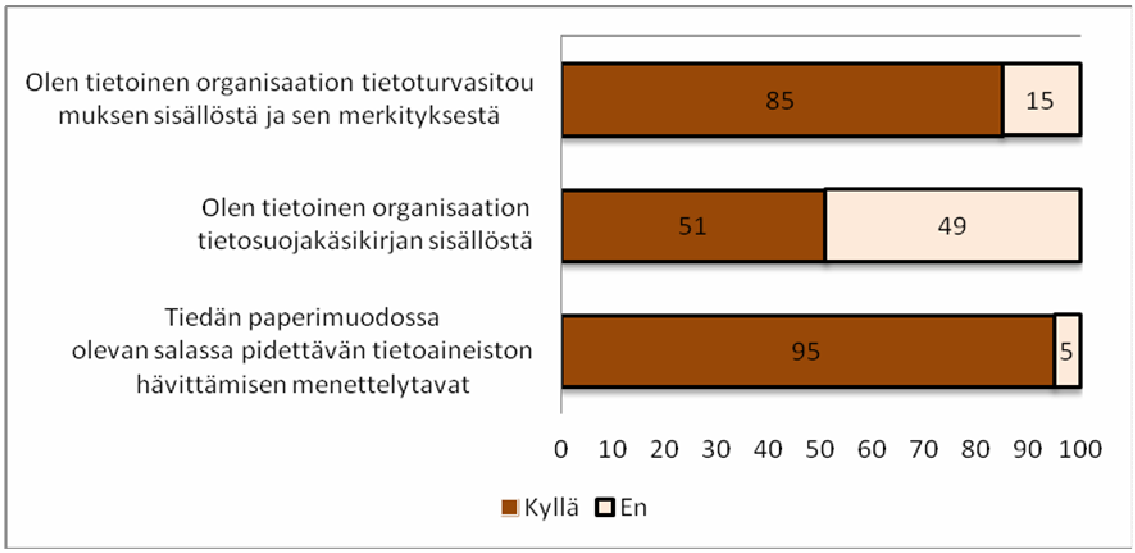
KUVIO 9. Henkilöstöturvallisuutta koskevien vastausten prosentuaalinen jakauma

Käyttäjäoikeuksiin ja käyttäjätunnuksiin liittyvien väittämien kohdalla vastaajat olivat täysin yksimielisiä (s= 0.00) ja väärinkäytöksiin sekä henkilökunnan toiminnan osuuteen tietoturvallisuutta vaarantavana tekijänä liittyvien mielipiteiden kohdalla keskihajonta oli myös pieni (s= 0.59 -0.64) (Taulukko 7). Kaikkien muuttujan keskiarvot olivat yli 2.72, joten myös henkilöstöturvallisuuteen liittyvää tietämyksen tasoa voidaan pitää hyvänä (kokonaiskeskiarvo 2.87).

TAULUKKO 7. Henkilöstöturvallisuusosaamiseen liittyvien väittämien tunnuslukuja

Henkilöstöturvallisuusosaaminen	N	Keskiarvo	Keskihajonta
Käyttäjätunnukset ja salasanat on tarkoitettu vain henkilökohtaiseen käyttöön	117	3,00	0,00
Käyttöoikeudet potilastietojärjestelmiin määritellään työtehtävien ja vastuun mukaisesti	117	3,00	0,00
Tietosuojaan ja tietoturvaan liittyvästä väärinkäytöstä seuraa aina rangaistus	117	2,75	0,59
Suurin tietoturvallisuutta vaarantava tekijä on henkilökunnan toiminta	117	2,72	0,64

Vastaajista suurin osa (85 %) tiesi organisaation tietoturvasitoumuksen sisällöstä ja sen merkityksestä. Kuitenkin huomattavaa on se, että 15 prosenttia oli sellaisia, joilla ei ollut tietoa tietoturvasitoumuksesta. Melkein kaikki (95 %) kyselyyn osallistuneista olivat tietoisia, miten paperimuodossa oleva salassa pidettävä tietoaineisto tulee hävittää. Kaikkein vähiten oltiin tietoisia organisaatiossa olevan tietosuojakäsikirjan sisällöstä, vain noin puolet (51 %) vastaajista ilmoitti tietävänsä, mitä tietosuojakäsikirja sisältää. (Kuvio 10).



KUVIO 10. Henkilöstöturvallisuutta koskevien vastausten prosentuaalinen jakauma

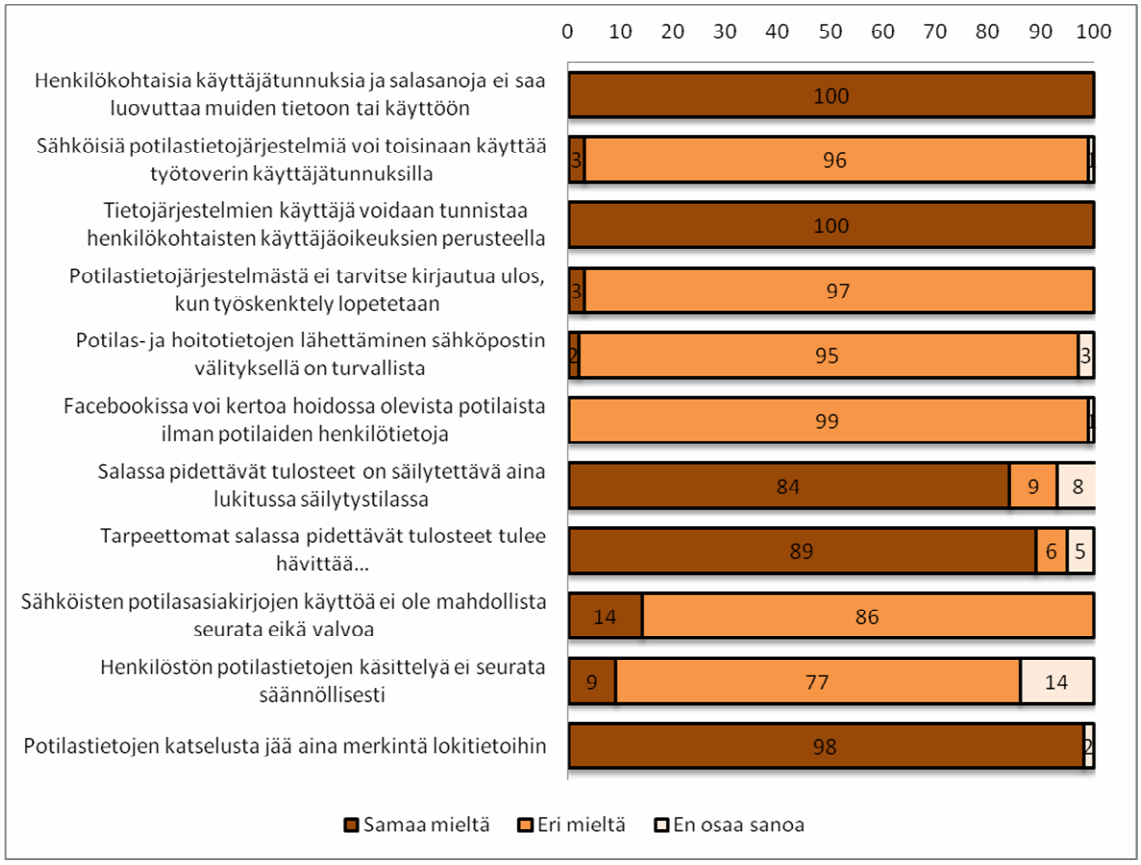
6.6 Käyttöturvallisuusosaaminen

Samoin kuin henkilöstöturvallisuutta, käyttöturvallisuutta koskevaa tietämystä tarkasteltiin henkilöstöön liittyvien tietoriskien hallinnan näkökulmasta. Vastaajien keskuudessa vallitsi täysi yksimielisyys (100 %) siitä, että järjestelmien käyttäjät ovat tunnistettavissa henkilökohtaisten käyttäjäoikeuksien perusteella. Kaikki vastaajat olivat yksimielisiä (100 %) myös siitä, että henkilökohtaisia käyttäjätunnuksia ja salasanoja ei saa luovuttaa muille, kuitenkin 3:n prosentin mielestä sähköisiä potilastietojärjestelmiä voi toisinaan käyttää työtoverin käyttäjätunnuksilla. Enemmistö (97 %) puolestaan oli samaa mieltä siitä, että potilastietojärjestelmistä tulee kirjautua ulos, kun työskentely lopetetaan. (Kuvio 11).

Potilastietojen lähettäminen sähköpostin välityksellä ei ole turvallista suurimman osan (95 %) mielestä, 5 prosenttia vastaajista piti sitä kuitenkin turvallisena tai ei osannut sanoa mielipidettään. Lähes kaikki (99 %) olivat tietoisia myös siitä, että Facebookissa ei voi kertoa hoidossa olevista potilaista edes ilman heidän henkilötietojaan, mutta 1 prosentti vastaajista oli epätietoisia oikeasta menettelytavasta.

Salassa pidettävien tulosteiden säilyttämiseen ja hävittämiseen liittyviä käytäntöjä mitattiin kahdella eri väittämällä. Vastaajista 84 prosentin mielestä salassa pidettävät tulosteet tulee säilyttää aina lukitussa säilytystilassa, 9 prosenttia oli eri mieltä ja loput 8 prosenttia ei osannut sanoa mielipidettään toimintatavasta. Vastaavasti tulosteiden hävittämistä koskevan käytännön kohdalla suurin osa vastaajista (89 %) oli samaa mieltä siitä, että tarpeettomat salassa pidettävät tulosteet tulee hävittää aina välittömästi.

Osion kolme viimeistä väittämää liittyivät tietojärjestelmien käytön valvontaan osana käyttöturvallisuutta. Lähes kaikki vastaajat (98 %) olivat tietoisia potilastietojen katselusta lokitietoihin jäävästä merkinnästä. Silti kyselyyn osallistuneista vähemmistön (14 %) mielestä sähköisten potilasasiakirjojen käyttöä ei voida seurata eikä valvoa, loput 86 prosenttia olivat tietoisia tästä mahdollisuudesta. Melkein neljännes (23 %) vastaajista oli sitä mieltä, että henkilöstön potilastietojen käsittelyä ei seurata säännöllisesti tai he eivät osanneet sanoa mielipidettään. Sen sijaan 77 prosenttia oli tietoisia seurannan säännöllisyydestä.



KUVIO 11. Käyttöturvallisuutta koskevien vastausten prosentuaalinen jakauma

Vastaajat olivat täysin yksimielisiä henkilökohtaisten käyttäjätunnuksien ja salasanojen käytön menettelytavoista sekä tietojärjestelmän käyttäjien tunnistamisesta (s=0.00) (Taulukko 8). Eniten hajontaa oli potilastietojen käsittelyn seurannan säännöllisyyttä koskevan väittämän kohdalla (s=0.71). Keskiarvolukujen perusteella arvioitaessa käyttöturvallisuuteen liittyvää tietämyksen tasoa, voidaan sen todeta olevan hyvä, kokonaiskeskiarvon ollessa 2.90 keskiarvojen vaihdellessa välillä 2.63 – 3.00.

TAULUKKO 8. Käyttöturvallisuusosaamiseen liittyvien väittämien tunnuslukuja

Käyttöturvallisuusosaaminen	N	Keskiarvo	Keskihajonta
Henkilökohtaisia käyttäjätunnuksia ja salasanoja ei saa luovuttaa muiden tietoon tai käyttöön	117	3,00	0,00
Sähköisiä potilastietojärjestelmiä voi toisinaan käyttää työtoverin käyttäjätunnuksella	117	2,96	0,24
Tietojärjestelmän käyttäjä voidaan tunnistaa henkilökohtaisten käyttäjäoikeuksien perusteella	117	3,00	0,00
Potilastietojärjestelmästä ei tarvitse kirjautua ulos, kun työskentely lopetetaan	117	2,97	0,18
Potilas- ja hoitotietojen lähettäminen sähköpostin välityksellä on turvallista	117	2,91	0,38
Facebookissa voi kertoa hoidossa olevista potilaista ilman potilaiden henkilötietoja	117	2,98	0,18
Salassa pidettävät tulosteet on säilytettävä aina lukitussa säilytystilassa	117	2,76	0,58
Tarpeettomat salassa pidettävät tulosteet tulee hävittää aina välittömästi	117	2,84	0,49
Sähköisten potilasasiakirjojen käyttöä ei ole mahdollista seurata eikä valvoa	117	2,86	0,35
Henkilöstön potilastietojen käsittelyä ei seurata säännöllisesti	117	2,63	0,71
Potilastietojen katselusta jää aina merkintä lokitietoihin	117	2,97	0,26

6.7 Tietosuoja- ja tietoturvamääräyksiin liittyviä mahdollisuuksia ja haasteita

Kyselylomakkeen lopussa oli kaksi avointa kysymystä. Näistä ensimmäisessä kysymyksessä pyydettiin vastaajia esittämään käytännön esimerkkien avulla mielipiteitään siitä, miten nykyiset tietosuoja- ja tietoturvamääräykset mahdollistavat joustavan toiminnan. Toisessa kysymyksessä vastaajilta kysyttiin vapaamuotoisia kommentteja liittyen tietosuojaan ja tietoturvaan. Ensimmäiseen kysymykseen saatiin 44 ja toiseen 38 vastausta.

Vastaajien mielestä kaikille olemassa olevat yhtenäiset ohjeet, säännöt ja menettelytavat parantavat toiminnan joustavuutta ja sujuvuutta, kun jokainen on selvillä, miten missäkin tilanteessa toimitaan. Työtehtävien ja vastuiden mukaisesti määritellyt henkilökohtaiset käyttäjätunnukset ja salasanat mahdollistavat puolestaan potilastietojen luottamuksellisen ja turvallisen käsittelyn. Edellytyksenä tietenkin, että toimitaan annettujen ohjeiden ja lainsäädännön vaatimusten mukaisesti. Tiedon saannin reaaliaikaisuus ja tiedonsiirron saumattomuus eri toimintayksiköiden välillä vähentävät tietojen kirjaami-

sen päällekkäisyyttä ja mahdollistavat näin omalta osaltaan joustavan päivittäisen toiminnan. Vastaajat esittivät mielipiteitään seuraavasti:

”Jos henkilöstö tietää tietosuoja- ja turvamääräykset hyvin, niin toiminta on joustavaa”

”Selkeä yhtenäinen käytäntö mahdollistaa rutiinin”

”Jokaisella työntekijällä on henkilökohtaiset käyttäjätunnukset ja salasanat, jolloin myös ns. väärinkäytökset saadaan selville.”

”Tieto siirtyy aina seuraavaan hoitopaikkaan tarvittaessa, päällekkäisyys vähenee”

Kaikissa vastauksissa joustavan toiminnan ei kuitenkaan koettu aina olevan täysin ongelmatonta. Salasanojen määrän runsautta, ohjelmien paljoutta, tietokoneiden hitautta sekä tietojen saannin vaikeuksia kuvattiin seuraavasti:

”Ainut ongelma on tietokoneiden hitaus uudelleen kirjautumisessa käyttäjävaihdon jälkeen ja ohjelmien paljous”

”Jokaisiin ohjelmiin on omat salasanansa ja kirjautuminen vie aikaa”

”Ei ole aina mahdollista, esim. emme näe erikoissh:n tietoja ja as. ehtii tulla vo:lle”

Tietosuojaan ja tietoturvaan liittyen nousi selkeästi esille kolme asiaa – tietojen päivittämisen ja koulutuksen lisätarve kaikille ammattiryhmille, tietoturvariskien lisääntynyt mahdollisuus sekä henkilöstön käyttäytyminen työasemilla muun muassa seuraavasti:

”Lisää asiasta koulutusta ja tieto kulkemaan käytännön työhön”

”Sekä vanhoille että etenkin uusille työntekijöille tulisi olla ns. päivityskoulutusta ko. asiaan liittyen”

”Sähköisellä potilaskertomuksella omat vaaransa. Helppo katsella omaisten papereita, jääkö kiinni?”

”Tietoturva rikkoutuu helposti. Tietokoneen ruudulta voi nähdä toisen asiakkaan tietoja, niitä voi kuulla sairaalassa esim. potilashuoneessa kierrolla. Henkilökunta saattaa tahattomasti rikkoa tietoturvaa puhuessaan esim. kansliassa potilaiden asioista”

”Henkilökunta luottaa liikaa toisiinsa ja ei lukitse työpistettään vaan jättää tunnuksillaan potilaskertomukset auki”

7 TUTKIMUKSEN LUOTETTAVUUS JA EETTISET NÄKÖKOHDAT

Tutkimuksen luotettavuutta voidaan tarkastella useasta eri näkökulmasta. Toisaalta sitä voidaan arvioida mittaamisen ja aineiston keruun kannalta, mutta myös tulosten luotettavuutena. Käytettävissä on useita erilaisia mittaus- ja tutkimustapoja. Määrällisen tutkimuksen mittarin ja mittaamisen luotettavuutta voidaan tarkastella arvioimalla reliabiliteettia (luotettavuus) ja validiteettia (pätevyys). Reliabiliteetilla tarkoitetaan mittaustulosten toistettavuutta. Mitattaessa samaa ilmiötä samalla mittarilla toistuvasti, saatujen vastausten tulee olla samansuuntaisia. Validiteetillä puolestaan tarkoitetaan mittarin kykyä mitata sitä, mitä on tarkoituskin mitata. (Hirsjärvi ym. 2001, 213; Metsämuuronen 2006, 64, 115; Vehviläinen-Julkunen & Paunonen 1998, 206 – 207, 209.)

Mittarin reliabiliteettia voidaan arvioida sen vastaavuutena, pysyvyytenä sekä sisäisenä johdonmukaisuutena käyttäen erilaisia tilastollisia menetelmiä (Metsämuuronen 2006, 65 – 66). Tässä tutkimuksessa mittarin sisäistä johdonmukaisuutta, mittarin eri osioiden kykyä mitata samaa asiaa, arvioitiin käyttämällä Cronbachin alfaa. Yksittäisistä mittarin osioista muodostettiin summamuuttujat teemoittain lukuun ottamatta henkilöstöturvallisuutta koskevia muuttujia. Tämän muuttujaryhmän muuttujista puolella muuttujista keskihajonta oli tasan nolla. Joten oli oletettavaa, että ei olisi tarkoituksenmukaista muodostaa niistä summamuuttujaa. Muuttujaryhmittäin lasketut Cronbachin alfakertoimet muiden kohdalla vaihtelivat 0.33 – 0.71 välillä. Kahden muuttujaryhmän arvoiksi saatiin yli 0.60. Cronbachin alfakertoimien tasoa voitaneen pitää kohtuullisena näiden kahden ryhmän kohdalla.

Tässä tutkimuksessa mittarissa käytettiin suppeaa skaalaa (3-portainen Likert), joka on voinut osaltaan vaikuttaa muuttujien arvojen vähäiseen vaihteluun ja sitä kautta summamuuttujien pieniin variansseihin laskien siten reliabiliteettia. Kyseiset kysymykset eivät ole tällöin olleet riittävästi vastaajia erottelevia, kaikki vastaajat ovat esimerkiksi vastanneet samalla tavalla. Pitkän mittarin on todettu yleensä olevan luotettavampi kuin lyhyt mittari (Metsämuuronen 2006, 69). Tätä puoltaa myös yllä laskettujen Cronbachin alfakertoimien arvot – mitä useampi osio summamuuttujassa, sitä korkeampi alfakerroin ja reliabiliteetti.

Käytetty mittari laadittiin perustuen potilasrekisteritietojen käsittelyä ja tietoturvallista toimintaa ohjaavan lainsäädännön, tietoturvaoppaiden ja ohjeistusten, potilastietojen käsittelyohjeiden, yleisten tietoturvallisuusvaatimusten ja organisaation tietoturvapolitiikan hoitohenkilöstön osaamiselle sekä tietämykselle asettamiin vaatimuksiin. Nämä vaatimukset muokattiin edelleen yksittäisten väittämien muotoon koskien potilastietojen käsittelyä ja luovutusta, suostumuksen hallintaa, yleistä tietoturvaa, käyttöturvallisuutta ja henkilöstöturvallisuutta. Kysymysten edustavuuden ja oikeellisuuden arvioinnissa hyödynnettiin organisaation tietosuojavastaavan asiantuntemusta. Mittarin käytettävyys ja kyselyn tekninen toimivuus testattiin etukäteen tutkimusryhmää vastaavalla 4 henkilöllä. Mittariin ei tarvinnut testauksen jälkeen tehdä muutoksia.

Mittarin kysymysten laatiminen oli haasteellista. Vastaajat eivät välttämättä ole ymmärtäneet kysymyksiä samalla tavalla kuin tutkija. Tämä ilmeni muun muassa sellaisten väittämien kohdalla, jotka sisälsivät avoimia kysymyksiä perusteluineen. Vastaajat olivat olleet eri mieltä vastausvaihtoehdoista, mutta perustelut vastauksiin olivat samansuuntaisia päinvastoin vastanneiden kanssa. Pohdittavaksi jää myös, kattoiko mittaus oikealla tavalla kaikki tutkimuksen kannalta oleelliset tietosuoja- ja tietoturvatietämykseen ja osaamiseen liittyvät osa-alueet.

Tutkimuksen luotettavuuden parantamiseksi kyselyyn osallistujat valittiin systemaattisella satunnaisotannalla, jolloin kaikilla perusjoukossa olevilla oli mahdollisuudet valikoitua otokseen. Suosimalla otosaineistoja määrällisessä tutkimuksessa pystytään paremmin tekemään myös tilastollisia yleistyksiä perusjoukkoon. Vaikka otanta oli satunnainen ja edusti hyvin perusjoukkoa, tämän tutkimuksen tuloksia ei voida yleistää alhaisen vastausprosentin ja kadon määrän vuoksi. Tässä tutkimuksessa kato oli 75 prosenttia. Kadon suuruuteen on voinut olla vaikuttamassa aineistonkeruun ajankohta. Aineistonkeruu tapahtui huhtikuussa, jolloin vuosilomat ovat mahdollisesti alentaneet vastausaktiivisuutta. Henkilöstöä ei ehkä myöskään tavoitettukaan työsähköpostilla tai tilannetekijät työpaikalla esimerkiksi kiire ovat olleet vaikuttamassa mahdollisuuteen vastata kyselyyn. Mittarin laajuudella useine avoimine kysymyksineen on todennäköisesti myös ollut vaikutusta vastausprosenttiin. Toisaalta väittämiin vastaaminen on voinut olla helpompaa ja nopeampaa käytetyn 3-asteisen Likertin johdosta, vastaajien ei ole tarvinnut miettiä erilaisia vivahde eroja. Avoimiin kysymyksiin saatiin runsaasti vastauksia niiden osalta, jotka kyselyyn osallistuivat.

Tutkimuksessa noudatettiin yleisesti hyväksyttyjä eettisiä käytäntöjä. Tutkimukselle haettiin kohteena olevan organisaation käytäntöjen mukaiset tutkimusluvat. Tutkimukseen osallistuminen perustui vapaaehtoisuuteen ja luottamuksellisuuteen. Aineiston keruu toteutettiin anonyymisti, jolloin vastaukset eivät ole yhdistettävissä yksittäisiin vastaajiin. Saadut tulokset olivat vain tutkijan käytössä ja vastausten tallentumisella salasanalla suojattuun tietokantaan sekä ehkäisemällä muiden kuin tutkijan pääsyn tietokantaan mahdollistettiin tietojen turvallisuus. Tutkimuksen päättymisen jälkeen kyselyn aineisto poistetaan tietokannasta ja hävitetään. Kyselyn saatekirjeessä tiedotettiin vastaajille edellä mainittujen eettisten seikkojen huomioiminen tutkimuksessa.

8 JOHTOPÄÄTÖKSET TUTKIMUKSEN TULOKSISTA

Tässä tutkimuksessa tarkoituksena oli kuvata Kainuun maakunta –kuntayhtymän hoitohenkilöstön tämänhetkistä tietosuoja- ja tietoturvatietämyksen ja osaamisen tasoa heidän itsensä arvioimana. Toisaalta haluttiin myös selvittää mahdollisia kehittämiskohteita ja puutteita tietämyksessä ja siten antaa lisätietoa organisaation osaamisen kehittämiseksi riittävän tietosuojan ja tietoturvallisuuden perustason varmistamiseksi koko kuntayhtymässä.

Kyselyyn osallistuneista kaikki vastaajat käyttivät potilastietojärjestelmiä työssään, suuri enemmistö useita kertoja päivässä. Suurimmalla osalla vastaajista oli myös pitkä (yli 6 vuotta) käyttökokemus sähköisten potilastietojen käsittelystä. Nämä toisaalta osin kuvastavat tietoteknologian ja tietojärjestelmien kehittymisen mukanaan tuomaa henkilöstön osaamistarpeita lisäävää muutosta terveydenhuollon toimintaympäristöissä, sähköisten potilastietojärjestelmien ollessa näin todellisuutta hoitohenkilöstön jokapäiväisessä työssä. Toisaalta käyttökokemukseen liittyen vastaajilla olettaisi myös olevan jo käytännön tuomaa kokemusta ja tietämystä sähköisessä muodossa olevien potilastietojen käsittelyä koskevista toimintaohjeista ja vaatimuksista.

Tulosten perusteella henkilöstö näyttäisi arvioineen oman tietämyksensä tason todellisuutta alhaisemmaksi. Vastaajista neljäsosa piti osaamistaan huonona tai ei osannut arvioida sitä, kuitenkin tutkimuksen tulosten perusteella hoitohenkilöstön kokonaistietämystä voitaneen pitää hyvänä. Tämä hyvä tulos on sinällään huomionarvoinen, koska tietosuojaan ja tietoturvaan liittyviä opintoja oli sisältynyt ammatillisiin opintoihin jonkin verran tai vähemmän melkein kaikilla vastaajista (97 %) ja työnantajan järjestämiin koulutuksiinkin osallistumattomia oli reilu kolmannes vastaajista. Näyttäisikin siltä, että toiminnan kautta oppimisella ja sitä mahdollisesti tukevien toimintatapojen ja –kulttuurin kehittämisellä on ollut myös merkitystä henkilöstön osaamisen kehittymisessä ja ylläpitämisessä. Ammatilliseen koulutukseen sisältyvien tietosuoja- ja tietoturvaopintojen määrällä myös näyttäisi olevan positiivinen vaikutus henkilöstön hyvään osaamisen tasoon. Tämä puoltaakin työelämän tarpeita vastaavan opetuksen sisällyttämistä jo ammatilliseen peruskoulutukseen ennen työelämään siirtymistä.

Tutkimuksessa hoitohenkilöstön tietosuoja- ja tietoturvatietämyksen tasoa tarkasteltiin viiden eri osaamisalueen kautta – yleisestä tietosuojaa ja tietoturvaa, potilastietojen käsittelyä, suostumuksen hallintaa, henkilöstöturvallisuutta sekä käyttöturvallisuutta koskevan tietämyksen näkökulmasta. Tarkasteltaessa saatuja tuloksia kokonaisuutena voidaan havaita henkilöstön tietämyksen olevan hyvällä tasolla kaikilla edellä mainituilla osa-alueilla. Vastaajat olivat hyvin tietoisia käsiteltävien potilasasiakirjojen merkintöjen tarpeellisuuteen, oikeellisuuteen, merkintöjen teko-oikeuteen ja vastuisiin liittyvistä vaatimuksista. Sen sijaan kirjattavien tietojen sisällöstä, arkaluonteisuudesta ja arkaluonteisten tietojen kirjaamisesta esiintyi vastaajien keskuudessa eniten epätietoisuutta. Vaikka potilastietoja yksimielisesti pidettiin salassa pidettävinä, niiden arkaluonteisuudesta eivät vastaajat olleetkaan yhtä lailla yksimielisiä. Toisaalla huomio kiinnittyi myös salassapitovelvollisuuden sitovuuden ymmärtämiseen palvelusuhteen tai tehtävän päättymisen jälkeen. Vastoin muun muassa terveydenhuollon ammattihenkilöistä annetun lain mukaisia säännöksiä salassapitovelvollisuuden säilymisestä ammatinharjoittamisen päättymisen jälkeenkin, ihan kaikilla ei ollut tämä velvoite tiedossa.

Henkilötietolaissa ja terveydenhuoltolaissa säädetään rekisterinpitäjää informoimaan asiakasta ja potilasta heidän henkilötietojensa käsittelystä. Tämän velvoitteen noudattamisessa hoitohenkilöstön roolia ei vajaan viidenneksen vastaajan osalta oltu täysin ymmärretty, velvoitteen laiminlyönnin perusteluina esitettiin muun muassa olettamus potilaslähtöisestä aktiivisuudesta pyytää tietoja ja toisaalta myös henkilökunnan ajan puute. Eniten puutteita yleiseen tietosuojaan ja tietoturvaan liittyvässä tietämyksessä näyttäisi esiintyvän koskien potilaan tietojen arkaluonteisuutta, arkaluonteisten tietojen kirjaamista sekä laista johtuvaa potilaan informointivelvollisuutta ja suurin vaihtelu tietämyksen määrässä ilmeni juuri informointivelvollisuuden kohdalla. Kokonaistarkastelussa kuitenkin yleiseen tietosuojaan ja tietoturvaan liittyvä tietämystä voitaneen pitää hyvänä.

Potilastietojen käsittelyn osalta eniten vaihteluja vastaajien tietämyksessä esiintyi potilaan henkilötietojen tietojen luovuttamisessa eri tahoille (omaiselle, alaikäisen huoltajalle ja viranomaiselle), virheellisten tietojen poistamiskäytännöissä, potilaan kieltooikeudesta tarpeellisten tietojen kirjaamisessa sekä tietosuojan toteutumisen varmistamisessa luovutettaessa potilastietoja. Suurimpia puutteita tietämyksessä puolestaan ilmeni tietojen luovuttamisesta viranomaiselle ja alaikäisen potilaan huoltajalle, potilaan

kielto-oikeudesta hoidon kannalta tarpeellisten tietojen kirjaamisessa sekä potilaalta tarvittavan erillisen suostumuksen tarpeellisuudesta luovutettaessa potilastietoja häneen hoitosuhteessa olevalle. Viranomaisille tietojen luovuttamista koskevasta erityislainsäädännöstä oltiin hyvin selvillä, mutta tietämyksessä tietojen luovuttamisesta viranomaisille esiintyi selvästi eroavaisuuksia. Näyttäisikin siltä, että säännösten sisällön tuntemus oli riittämätöntä, vaikka kyselyyn osallistujat olivatkin hyvin tietoisia olemassa olevasta lainsäädännöstä. Tietojen luovuttamisperiaatteista alaikäisen potilaan huoltajalle ja yleensäkin omaiselle ilmeni myös vaihtelua vastauksissa. Noin puolet vastaajista piti selviönä alaikäisen potilaan huoltajan tiedonsaantioikeutta, omaisten kohdalla vastaavasti neljäsosan mielestä omaiselle saa luovuttaa tietoja. Tulosten perusteella vaikuttaakin siltä, että salassa pidettävien potilastietojen luovuttamissäännökset eivät ole riittävän hyvin hoitohenkilöstön tiedossa. Potilasasiakirjojen käsittelyyn ja merkintöjen tekemiseen, potilastietojen käsittelyyn liittyvät yleiset periaatteet sekä sähköpostin ja Facebookin käyttöön liittyvät periaatteet näyttäisivät sen sijaan olevan hyvin vastaajien tiedossa. Myös potilaan tietojen luovuttamista koskeva suostumuksen hallintaan liittyvät toimintatavat hallittiin kokonaisuutena hyvin, ainoastaan potilaan antaman suostumuksen laajuus jakoi mielipiteitä kaikkein eniten ja sen osalta tietämyskin oli heikointa.

Vastaajilla oli yksimielisesti selkeä käsitys käyttäjätunnusten ja salasanojen henkilökohtaisuudesta ja niiden perusteella tapahtuvasta käyttäjien tunnistamisesta. Kaikki vastaajat tiesivät, että käyttäjätunnukset ja salasanat ovat henkilökohtaisia ja että ne määräytyvät kunkin työtehtävien ja vastuun mukaisesti eikä niitä myöskään saa luovuttaa muiden käyttöön. Kuitenkin tuloksista ilmeni myös tätä tietämystä kumoavia mielipiteitä, työasemilta ei tarvitse aina kirjauduta ulos työskentelyn loputtua tai että potilastietojärjestelmiä voidaan joskus käyttää työtoverin käyttäjätunnuksilla. Tämä on hieman ristiriidassa osalla vastaajista olevan käsityksen kanssa, että henkilökunnan toiminnalla ei olisi merkityksestä tietoturvallisuutta vaarantavana tekijänä. Henkilöstön liiallinen luottamus toisiinsa lisää näin tietoturvariskien mahdollisuutta ja mahdollistaa siten asiattomien pääsyn potilastietoihin vaarantaen samalla potilastietojen luottamuksellisuuden. Jos henkilöstö ei itse tiedosta omaa mahdollista osuuttaan tietoturvauhkana, muodostuu siitä todellinen ja huomioonotettava riski.

Rekisterinpitäjällä on henkilötietojen käsittelyn lainmukaisuuden seuranta- ja valvontavelvollisuus esimerkiksi lokiseurannan avulla. Vastaajien keskuudessa ilmeni jonkin

verran epätietoisuutta tästä henkilöstön potilastietojen käsittelyn seurannan säännöllisyydestä ja yleensäkin mahdollisuudesta valvoa ja seurata potilasasiakirjojen käyttöä. Sen sijaan melkein kaikki olivat tietoisia potilastietojen katselusta jäävästä merkinnästä lokitietoihin, kaikki tiesivät myös henkilökohtaisten käyttäjäoikeuksien perusteella tapahtuvasta käyttäjän jäljitettävyydestä. Tämä taas on ristiriitainen joidenkin käyttäjien mielipiteen kanssa, ettei käyttöä olisi mahdollista seurata. Onko syynä tietämyksen puute näiden asioiden keskinäisestä suhteesta vai yleinen käsitys siitä, ettei käyttöä seurata säännöllisesti. Nämä hoitohenkilöstön olettamukset voivat ylläpitää liiallista turvallisuudentunnetta käyttäjien keskuudessa lisäten siten kiinnostusta katsella muun muassa sellaisten potilaiden asiakirjoja, joihin heillä ei ole lainmukaista oikeutta tai potilaan antamaa suostumusta. Henkilörekisteririkoksen ja –rikkomuksen rangaistavuuden osalta väärinkäytösten seuraamuksien toteutumisesta vastaajat eivät myöskään olleet täysin tietoisia, jopa joka 7. vastaaja joko ei osannut sanoa tai ei tiennyt potilastietojen väärinkäytöksiin liittyvästä rikosoikeudellisesta vastuusta.

Lähes kaikki vastaajat ilmoittivat tietävänsä salassa pidettävän paperimuotoisen tietoaineiston hävittämisen menettelytavat, kuitenkaan noin joka kymmenes ei hävittäisi tarpeettomia tulosteita välittömästi ja joka seitsemäs puolestaan ei katsonut tarpeelliseksi salassa pidettävien tulosteiden säilyttämistä lukitussa säilytystilassa. Näyttäisikin siltä, että vaikka menettelytavat tunnetaan hyvin, ei tämä tietämys välttämättä aina kuitenkaan ohjaa käytännön toimintaa. Myös tietoturvasitoumuksen sisältö ja sen merkitys tunnettiin hyvin vastaajien keskuudessa, sen sijaan organisaation tietosuojakäsikirjan sisältö oli tuntematon puolelle vastaajista. Vastauksissaan henkilöstö toi esille yhtenäisten ohjeiden, sääntöjen ja menettelytapojen sekä koulutuksen merkityksen tietojen päivittämisessä. Tämä tukeekin käsitystä tiedottamisen, koulutuksen ja ohjeistuksen tärkeästä roolista hoitohenkilöstön tietosuoja- ja tietoturvatietämyksen lisäämisessä, asenteiden muokkaamisessa ja siten tietoturvariskien ennaltaehkäisyssä ja minimoimisessa.

Yhteenvetona voitaneen todeta hoitohenkilöstön tietosuoja- ja tieturvaosaamisen ja tietämyksen tason olevan hyvä kaikilla tietosuoja- ja tietoturvatietämyksen osa-alueilla Krugerin ja Kearneyn (2006) kehittämällä mittarilla mitattuna tässä tutkimuksessa. Tulosten perusteella ei esille noussut selviä suuria osaamisvajeita, mutta eri tahoille, kuten viranomaisille ja omaisille tapahtuvan tietojen luovuttamisperiaatteiden sekä organisaation tietosuojakäsikirjan ym. ohjeistuksen tuntemuksen lisääminen näyttäisi olevan tar-

peellista käyttäjien tietojen päivittämiseksi ja ylläpitämiseksi. Erityisesti huomiota tulisi kiinnittää niihin yksittäisiin tietämyksen kohteisiin, joissa esiintyi eniten hajontaa vastaajien mielipiteissä. Mielipiteiden jakautuminen voi olla osoitus muun muassa puutteellisesta käytössä olevan ohjeistuksen tuntemuksesta. Avointen kysymysten kohdalla vastaajat nostivatkin esille yhtenäisten ohjeiden, sääntöjen ja menettelytapojen merkityksen jokaisen ollessa tällöin selvillä, miten missäkin tilanteessa tulee toimia. Samoin tietojen päivittämistä ja lisäkoulutusta toivottiin kaikille ammattiryhmille henkilöstön tiedostettua tietoturvariskien lisääntyneet mahdollisuudet. Kuten tuloksissakin tuli joidenkin osa-alueiden kohdalla esille osaaminen ja tietämys ei kuitenkaan yksistään riitä, henkilöstöllä tulee olla myös halu sekä mahdollisuus käyttää osaamistaan työssään, jotta olemassa oleva tietämys parhaiten ohjaisi lainmukaista potilastietojen käsittelyä käytännön työskentelyssä.

9 POHDINTA

Terveydenhuollossa tietoteknologian ja tietojärjestelmien käytön lisääntymisellä on ollut merkittäviä vaikutuksia hoitohenkilöstön päivittäiseen työskentelyyn. Potilastietojen reaaliaikainen siirto organisaation eri toimintayksiköiden välillä parhaimmillaan parantavat potilasturvallisuutta ja hoidon laatua sekä helpottavat ja nopeuttavat henkilöstön työskentelyä tiedon ollessa kaikkien niitä tarvitsevien saatavilla. Terveydenhuollon toimintaympäristöissä tapahtuneiden muutosten lisäksi muutokset terveydenhuollon toimintaa säätelevässä lainsäädännössä ovat myös omalta osaltaan luoneet uusia haasteita henkilöstön osaamiselle, erityisesti tietosuoja- ja tietoturvavaatimusten ja edellytysten huomioimiselle potilastietojen käsittelyssä. Yhä enenevässä määrin sähköisessä muodossa olevat arkaluontoiset ja salassa pidettävät asiakas- ja potilastiedot asettavat nekin lisävaatimuksia tietojen turvalliselle käsittelylle.

Terveydenhuollon palvelujen entistä suurempi riippuvaisuus tiedon saatavuudesta ja luotettavuudesta korostaa rekisterinpitäjän velvoitteita tietojen laadusta ja niiden suojaamisesta. Terveydenhuollossa organisaation yhtenä tehtävänä onkin tietoturvallisuuden ja tietosuojan kehittäminen ja hallinnointi. Toiminnan tavoitteena on saavuttaa asiakkaiden ja potilaiden luottamus siitä, että heidän tietojaan käytetään vain olemassa olevien oikeutuksien perusteella. Tämä edellyttää organisaatiossa muun muassa sellaisten hyväksyttyjen toimintaperiaatteiden ja käytäntöjen, kuten tietoturvapolitiikan, tietoturvallisuustavoitteiden, potilastietojen lainmukaisen ja tietoturvallisen käsittelyn yhteisten toimintatapojen määrittelyä organisaation toiminnallisiin tavoitteisiin ja voimassa olevaan lainsäädäntöön, normistoon ja ohjeistukseen perustuen. Toimintaperiaatteiden ja käytäntöjen pelkkä olemassaolo ei yksistään riitä vaan koko henkilöstöllä on oltava myös riittävä tietämys erityisesti lainsäädännön asettamista potilastietojen käsittelyn ja käytön tietosuoja- ja tietoturvavaatimuksista.

Kainuun maakunta -kuntayhtymässä siirtyminen kolmesta eri sähköisestä potilastietojärjestelmästä yhteen yhtenäiseen potilastietojärjestelmään sekä erikoissairaanhoidon että perusterveydenhuollon osalta vuoden 2011 aikana tuo uudenlaisia haasteita muun muassa tietosuojan ja –turvan toteutumiselle sekä toimintatapojen ja -kulttuurin muutokselle. Siirryttäessä yhteiseen potilastietojärjestelmään näinkin laajassa organisaatiossa korostuu entisestään tietosuojan ja -turvan toteutumisen kannalta potilaan hoidossa

tarvittavien tietojen eheyden, saatavuuden, luottamuksellisuuden sekä potilaiden yksityisyyden turvaaminen sekä turvallisuus ja huolellisuus tietojen käsittelyssä. Kaikkien käyttäjien on tunnettava oikeanlaiset tietojen käsittelytavat ja käsittelysäännöt sekä miten ja mihin tarkoitukseen järjestelmää saa käyttää, toisaalta käyttäjien on myös tiedettävä, mikä on kiellettyä. Hoidon jatkuvuuden ja tiedonvälityksen varmistamiseksi käyttäjien on oltava tietoisia riittävien, virheettömien ja tarpeellisten potilasasiakirjamerkintöjen tekemisestä, lisäksi myös hoitosuhteeseen perustuvasta tietojen asianmukaisesta käytöstä. Kunkin käyttäjän on tiedettävä käyttöoikeuksien hallinnan yleiset periaatteet, kuten esimerkiksi tehtävien mukaisesti käyttäjille määriteltyjen käyttöoikeuksien, henkilökohtaisten käyttäjätunnusten ja salasanojen perusteella tapahtuvasta todentamisesta, tietojen käytön säännöllisestä seurannasta ja todetuista väärinkäytön seuraamuksista.

Tietoturvallisuuden ja tietosuojan toteutuminen osana johtamisen ja osaamisen kehittämistä edellyttää organisaation toiminnan kannalta keskeisen tarvittavan osaamisen määrittelyä, nykyisen osaamisen arviointia ja näiden pohjalta tapahtuvaa osaamisen kehittämistä. Tietosuoja- ja tietoturvaosaaminen voidaankin nähdä organisaation yhtenä ydinosaamisena, jonka ylläpitoa ja kehittämistä säätelee voimassa oleva lainsäädäntö, normit, ohjeistus ja organisaation tietoturvapolitiikka. Ydinosaaminen puolestaan muodostuu useista eri konkreettisista osaamisen osa-alueista. Mittaamalla ja arvioimalla henkilöstön nykyosaamista saatiin selville heidän tietämyksensä taso ja mahdolliset kehittämiskohteet riittävän osaamisen varmistamiseksi. Tietosuojan toteutuminen ja tietoturvallisuuden ylläpito ja kehittäminen on täten osa prosessia, jonka tavoitteena on potilastietojen lainmukainen käsittely niin, että tietojen luottamuksellisuus, eheys, saatavuus ja käytettävyys on varmistettu ja turvattu, yksityisyyden suojaa unohtamatta.

Osaamisen johtamisen kannalta haasteellisena voidaan pitää jo itsessään osaamista, ongelmaksi voi muodostua kriittisten osaamisten määrittely. Mikä on organisaation kannalta oleellista osaamista, jonka avulla tietosuojalle ja tietoturvalle asetetut velvoitteet toteutuvat. Osa olemassa olevasta osaamisesta on tulevaisuudessakin tarpeellista ns. perusosaamista, mutta osa osaamisesta on vasta ennakoitavissa. Tässä työssä tietosuoja- ja tietoturvaosaamisen eri osaamiset määriteltiin perustuen tämänhetkisiin lainsäädännön asettamiin vaatimuksiin. Sosiaali- ja terveydenhuollon jatkuva kehittyminen ja muuttuminen lisäävät henkilöstön osaamistarpeita. Osaamisen johtamisessa keskeistä onkin tunnistaa muutokset organisaation toiminnassa, niiden edellyttämät osaamiset ja

tulevaisuuden haasteet ja siten ennakoida tulevat muutokset riittävän ajoissa - vain sitä voidaan kehittää, mikä tunnistetaan.

Vaikka tarvittavat osaamiset kyetäänkin tunnistamaan, niiden mittaaminen voi olla myös haasteellista. Saatujen tulosten tarkastelua vaikeuttavat osaamisen arviointiin usein liittyvät erilaiset subjektiiviset tulkinnat, saadut tulokset ja todellisuus eivät aina vastaa toisiaan tai mittari ei ole riittävän erottelukykyinen tulosten tulkinnan kannalta. Tässä tutkimuksessa käytetty suppea skaala (3-portainen Likert) osaamisen arvioimiseksi on voinut omalta osaltaan vaikuttaa mittarin erottelukykyyn tulosten tulkinnassa. Osaamisen- ja tietämyksenhallinta moniulotteisena ja –alaisena käsitteenä kuvastaa osaamista organisatorisena, yksilöön kohdistuvana ja organisaatiokulttuurisena ilmiönä. Toisaalta kysymysten kohdentuessa näihin moniselitteisiin ilmiöihin ja niiden taustoihin, laajallakin skaalalla olisi voinut olla vaikeaa tavoittaa kaikkia kyseisiin ilmiöihin liittyviä käsityksiä ja mielipiteitä.

Ottaen huomioon terveydenhuollon toiminnan erityislaatuisuus – arkaluonteisten ja salassa pidettävien tietojen käsittely sekä lainsäädännön voimakkaasti terveydenhuollon toimintaa ohjaava vaikutus, yhtenä haasteena voitaneen pitää tietosuoja- ja tietoturvatietämyksen riittävän ja hyväksyttävän osaamisen perustason määrittelyä. Mikä on rekisterinpitäjän velvoitteiden ja potilastietojen suojauksen kannalta riittävä henkilöstön osaamisen ja tietämyksen taso? Pohdittavaksi jääkin, onko tässä tutkimuksessa käytetyn Krugerin ja Kerneyn (2006) kehittelemä tietämyksen tason arvioinnin kolmiportainen asteikko raja-arvoineen ollut riittävän erottelukykyinen osaamistason tulkinnassa.

Oman haasteensa tietosuoja- ja tietoturvaosaamisen ylläpitämiselle ja kehittämiselle yhtenäistä potilastietotietojärjestelmää käyttöönotettaessa Kainuun maakunta – kuntayhtymässä tuo suuri potilastietojen ja käsittelijöiden määrä uudessa toimintamallissa. Toisaalta myös potilastietojen käsittely-ympäristön muuttuminen laajentuessaan sekä perusterveydenhuollon ja erikoissairaanhoidon potilastietojen käsittelyyn Kainuun maakunta -kuntayhtymässä, myöhemmin myös valtakunnalliseen keskitettyihin sähköisiin potilastietojärjestelmiin, johtaa eittämättä entistä enemmän käytönvalvonnan tehostamisen ja uskottavuuden parantamisen vaatimusten huomioimiseen toiminnan muuttuessa läpinäkyväksi niin henkilöstön kuin asiakkaidenkin näkökulmasta. Edellisten lisäksi terveydenhuollossa pitkät tietojen säilytysajat edellyttävät hyvää tietojen suojaamista

niiden luottamuksellisuuden, eheyden ja käytettävyyden varmistamiseksi myös tulevaisuuden tarpeita varten. Kaikkien mainittujen muutosten myötä terveydenhuollossa tietosuojariskien mahdollisuus tulee kasvamaan, jolla puolestaan on vaikutuksia terveydenhuollon ammattihenkilöiden osaamisvaatimuksiin.

Toistaiseksi tietosuoja- ja tietoturvakoulutuksissa sekä alan tutkimuksissa painopiste on ollut enemmänkin teknistä osaamista korostavaa kuin tietoturva-asenteisiin ja yksityisyyden varmistamiseen liittyvissä asioissa. Terveydenhuollon osalta myös tietoturvallisuusriskeistä on vielä vähän tutkittua tietoa olemassa (Appari & Johnson 2010). Kuitenkin henkilöstön suuri merkitys joko tahattomissa tai tahallisissa tietoturvatapahtumissa lisää heidän tietämyksensä ja osaamisensa tärkeyttä tietosuojaa ja tietoturvaa koskevista keskeisistä periaatteista ja säännöksistä. Tässä tutkimuksessa tietosuoja- ja tietoturvatietämykseen liittyvinä tarkastelun kohteina olivat yleinen tietosuoja ja tietoturva, potilastietojen käsittely, suostumuksen hallinta, henkilöstöturvallisuus ja käyttöturvallisuus. Näin hoitohenkilöstön itsearviointina toteutettu osaamisen nykytilan kartoittaminen antaa tietoa heidän tietosuoja- ja tietoturvatietämyksen nykytasosta ja sitä kautta myös tietoa mahdollisista kehittämiskohteista auttaen täten suuntaamaan henkilöstön osaamisen suunnitelmallista kehittämistä oikein.

Henkilöstön osaaminen on todettu olevan yksi tärkeimmistä tietosuoja- ja tietoturvariskeistä, kuinka hyvin oikeanlaiset toimintatavat tiedetään ja kuinka niiden noudattamiseen suhtaudutaan. Tutkimustulosten mukaan hoitohenkilöstön tietämyksen tasoa eri osa-alueilta kokonaisuutena voidaan pitää käytetyn mittarin asteikolla arvioituna hyvänä. Huomioitavaa kuitenkin on, että muutaman kysymyksen kohdalla taso jäi alle määritellyn hyvän tason tai juuri sen yläpuolelle. Toisaalta huomio kiinnittyy myös vastaajien eriäviin mielipiteisiin koskien muun muassa henkilökunnan informointivelvollisuutta, potilaan kielto-oikeutta tarpeellisten tietojen kirjaamisessa, tietojen luovuttamista viranomaisille, potilaan antaman suostumuksen laajuutta ja potilastietojen käytön seurannan säännöllisyyttä. Tämän perusteella voisi olettaa tietämyksen olevan juuri näillä osa-alueilla kaikkein epävarminta ja siten pitää niitä mahdollisina kehittämiskohteina.

Osaamisen ylläpito ja henkilöstön osallistuminen organisaatiossa järjestettäviin koulutuksiin varmistaa parhaiten organisaation tietoturvallisen toiminnan. Tehokkain keino estää väärinkäytöksiä lieneekin henkilöstön jatkuva koulutus ja tiedottaminen muutok-

sista. Tämän tutkimuksen mukaan organisaation järjestämiin koulutuksiin osallistuminen oli vähäistä, 38 % ei ollut koskaan osallistunut niihin. Ehkä tämä on osaltaan ollut vaikuttamassa siihen, ettei ohjeistus ollut kaikkien niitä tarvitsevien tiedossa. Tärkeää olisikin miettiä syitä henkilöstön koulutuksiin osallistumattomuuteen, pitäisikö tietosuojaan ja tietoturvaan liittyvien asioiden koulutuksen ja erilaisten tietopakettien kuulua esimerkiksi pakollisena osana uusien työntekijöiden perehdyttämiseen ennen kuin oikeudet tietojärjestelmiin annetaan. Belsin ym. (2005) mukaan menestyksellisen tietoturvallisuuden hallinnan edellytyksenä on niin ylemmän johdon kuin suorittavan portaankin tukeminen tietämyksen kehittämisessä. Pohdittavaksi jääkin, miten henkilökuntaa saadaan motivoitua paremmin osallistumaan organisaatiossa järjestettäviin koulutuksiin ja miten työyhteisöissä tällaisena henkilöstöresurssipulan ja kiireen aikana kyetään järjestäminen mahdollisuus kaikille halukkaille osallistua näihin koulutuksiin. Jotta järjestetyillä koulutuksilla olisi myös jotain arvoa organisaatiolle tietoturvallisen toiminnan vaikuttavuuden arvioimiseksi ja tueksi tarvitaan, kuten Kruger ja Kearney (2006) sekä Appari ja Johnson (2010) totesivat tutkimuksissaan, tulevaisuudessakin palautetta henkilöstön tietämyksen tasosta ja koulutuksen vaikuttavuudesta, tietämyksen mittaaminen tukee näin myös toiminnan valvontaa ja osaamisen kehittämistä.

Organisaatiotasolla tässä tutkimuksessa saadut tulokset ovat käytettävissä hoitohenkilöstön tietosuoja- ja tietoturvaosaamista kuvaavana yhteenvetona, joka auttaa niin johtoa kuin henkilöstöäkin tunnistamaan ne kohdat, joissa on eniten kehittämisen varaa ja toisaalta näkemään myös vahvuudet osaamisessa. Tulosten julkistamisella ja käyttämisellä oheismateriaalina organisaation koulutuksissa saadaan tietosuoja- ja tietoturvaosaaminen näkyväksi, organisaation yhteiseksi asiaksi. Saatuja tuloksia voidaan myös hyödyntää näiden koulutusten sisällön suunnittelussa kohdentamalla päähuomio todettuihin puutteellisuuksiin henkilöstön tietämyksessä ja muun muassa mahdollisten tietosuoja- ja tietoturvaosaamisen kehittämissuunnitelmien laatimisessa ja toteuttamisessa koko organisaatiotasolla. Nyt käytettyä mittaria, kokemuksen tuomalla tietämyksellä jatko kehittelemällä paremmin organisaation tarpeita vastaavaksi, voitaneen myös hyödyntää tietosuoja- ja tietoturvatietämyksen arvioimisessa myöhemminkin esimerkiksi uusien työntekijöiden lähtötason selvittämiseksi. Hyvä osaaminen ja tietämys ei kuitenkaan yksistään riitä takaamaan lainmukaista potilastietojen käsittelyä, henkilöstöllä tulee olla myös motivaatio ja oikea asenne käyttää osaamistaan työssään. Tästä näkökul-

masta tulisikin organisaatiossa hankkia myös tietoa siitä, miten hoitohenkilöstön tietämys tietosuojaan ja tietoturvaan liittyvissä asioissa ohjaa heidän toimintaansa.

Terveydenhuollon alueella on toistaiseksi keskitytty enimmäkseen vielä tietoteknistä osaamista korostaviin tutkimuksiin. Tietoturvallisuuden ja yksityisyyden merkityksen lisääntyminen terveydenhuollossa ovat kuitenkin johtamassa myös koulutuksen painopisteen kohdistumiseen entistä enemmän tietoturva-asenteisiin ja yksityisyydensuojan toteutumisen varmistamiseen. Tästä näkökulmasta tarkasteltuna tulevaisuuden tutkimuksissa näyttäisikin olevan tarvetta hankkia uutta tietoa tietoturvallisuusriskeistä päätöksenteon, tietoturvallisuuden hallinnan sekä johtamisen tueksi. Tässä tutkimuksessa hankittiin tietoa Kainuun maakunta –kuntayhtymän hoitohenkilöstön tietosuoja- ja tietoturvatietämyksen tasosta ennen yhteen yhtenäiseen potilastietojärjestelmään siirtymistä. Organisaation tietosuoja- ja tietoturvaosaamisen kokonaiskuvan luomiseksi olisi myös hyödyllistä jatkotutkimuksen avulla selvittää, miten henkilöstön hallitsema tietämys ja osaaminen todellisuudessa ohjaa ja vaikuttaa heidän toimintaansa ja käyttäytymiseensä uudessa toimintaympäristössä. Toisaalta jatkotutkimusten kannalta myös käytettävissä olevien tietämyksen ja osaamisen tason arviointimenetelmiä tulisi pyrkiä kehittämään terveydenhuollon erityispiirteitä paremmin vastaaviksi muun muassa hyödyntämällä jo olemassa olevaa Krugerin ja Kearneyn (2006) arviointiasteikkoa.

LÄHTEET

American Health Information Management Association & American Medical Informatics Association. 2008. Joint Work Force Task Force. Health Information Management and Informatics Core Competencies for Individuals Working With Electronic Health Records. Saatavissa: http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_040723.pdf (Luettu 7.4.2011).

Appari, A. & Johnson, E. 2010. Ingformation security and privacy in healhtcare: current state of research. Int.J.Internet and Enterprise Management 6 (4), 279 – 314.

Belsis, P. , Kokolakis, S. & Kiountorouzis, E. 2005. Information systems security from a knowledge management perspective. Information Management & Computer Security 13 (3), 189 – 202.

Draganidis, F. & Mentaz, G. 2006. Competency based management: a review of systems and approaches. Information Management & Computer Security 14 (1), 51 – 64.

Eriksson, K. , Isola, A., Kyngäs, H., Leino-Kilpi, H., Lindström, U.Å., Paavilainen, E., Pietiä, A-M., Salanterä, S., Vehviläinen-Julkunen, K. & Åstedt-Kurki, P. 2007. Hoitotiede. WSOY oppimateriaalit Oy, Helsinki.

Finlex. Ajantasainen lainsäädäntö. Henkilötietolaki 22.4.1999/523. Saatavissa: http://www.finlex.fi/fi/laki/ajantasa/1999/19990523 (Luettu 8.4.2011).

Finlex. Ajantasainen lainsäädäntö. Laki potilaan asemasta ja oikeuksista 17.8.1998/785. Saaatavissa: http://www.finlex.fi/fi/laki/ajantasa/1992/19920785 (Luettu 8.4.2011).

Finlex. Ajantasainen lainsäädäntö. Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä 9.2.2007/159. Saatavissa: http://www.finlex.fi/fi/laki/ajantasa/2007/20070159 (Luettu 8.4.2011).

Finlex. Ajantasainen lainsäädäntö. Laki terveydenhuollon ammattihenkilöistä 28.6.1994/559. Saatavissa: http://www.finlex.fi/fi/laki/ajantasa/1994/19940559 (Luettu 8.4.2011).

Finlex. Ajantasainen lainsäädäntö. Laki viranomaisen toiminnan julkisuudesta 21.5.1999/621. Saatavissa: http://www.finlex.fi/fi/laki/ajantasa/1999/19990621 (Luettu 1.4.2011).

Finlex. Ajantasainen lainsäädäntö. Suomen perustuslaki 731/1999. Saatavissa: http://www.finlex.fi/fi/laki/ajantasa/1999/19990731 (Luettu 8.4.2011).

Finlex. Ajantasainen lainsäädäntö. Sosiaali- ja terveysministeriön asetus potilasasiakirjoista 298/2009. Saatavissa: http://www.finlex.fi/fi/laki/alkup/2009/20090298 (Luettu 8.4.2011).

Finlex. Ajantasainen lainsäädäntö. Terveydenhuoltolaki 30.12.2010/1326. Saatavissa: http://www.finlex.fi/fi/laki/alkup/2010/20101326?search%5Btype%5D=pika&search%5Bpika%5D=terveydenhuoltolaki (Luettu 8.8.2011).

Heikkilä, A., Hupli, M. & Leino-Kilpi, H. 2008. Verkkokysely tutkimusaineiston keruumenetelmänä. Hoitotiede – lehti 20 (2), 101 – 110.

Heikkilä, T. 2004. Tilastollinen tutkimus. Edita Prima Oy, Helsinki.

Hilden, R. 2002. Ammatillinen osaaminen hoitotyössä. Tammer-Paino Oy, Tampere.

Hirsijärvi, S., Remes, P. & Sajavaara, P. 2000. Tutki ja kirjoita. Tummavuoren kirjapaino Oy, Vantaa.

Hobbs, S. 2002. Measuring nurses' computer competency: an analysis of published instruments. CIN; Computers, Informatics Nursing 20 (2), 63 – 73.

Huotari, M-L., Hurme, P. & Valkonen, T. 2005. Viestinnästä tietoon. Tiedonluominen työyhteisössä. WSOY, Porvoo.

Itälä, T. & Ruotsalainen, P. 2004. Tietoturvallinen kommunikaatioalusta ja luovutuslokin hallinnan suositukset. Osaavien keskusten verkoston julkaisuja 6/2004. Stakesin monistamo, Helsinki.

Jauhiainen, A. 2006. Kolme skenaariota tulevaisuuden hoitotyöhön – uusia mahdollisuuksia tieto- ja viestintätekniikalla. Teoksessa Hoitotyön vuosikirja 2006. Inhimillisten voimavarojen johtaminen. Sairaanhoitajaliitto. Gummerus Kirjapaino Oy, Helsinki.

Järvinen, P. 2002. Tietoturva & yksityisyys. WS Bookwell, Porvoo.

Kalkas, H. & Sarvimäki, A. 1996. Hoitotyön etiikan perusteet. WSOY, Juva.

Kerko, P. 2001. Turvallisuusjohtaminen. WS Bookwell Oy, Porvoo.

Kivinen, T. 2008. Tiedon ja osaamisen johtaminen terveydenhuollon organisaatioissa. Knowledge Management in Health Care Organisations. Väitöskirja. Yhteiskuntatieteellinen tiedekunta. Terveyshallinnon ja talouden laitos. Kuopion yliopiston julkaisuja E. Yhteiskuntatieteet 158. Kuopion yliopisto, Kuopio.

Kleemola, M. & Tervo-Pellikka, R. 1998. Tietosuoja. Vaatimukset verkottuvassa tietojärjestelmässä. Gummerus Kirjapaino Oy, Jyväskylä.

Kujansivu, P., Lönnqvist, A., Jääskeläinen, A. & Sillanpää, V. 2007. Liiketoiminnan aineettomat menestystekijät. Mittaa, kehitä ja johda. Gummerus Kirjapaino Oy, Helsinki.

Kruger, H., A. & Kearney, W.D. 2006. A prototype for assessing information security awareness. Computer & security 25, 289 - 296.

Laamanen, K. 2005. Johda suorituskykyä tiedon avulla – ilmiöstä tulkintaan. Tammer-Paino Oy, Tampere.

Lammintakanen, J. & Kinnunen, J. 2006. Hoitotyön osaamisvaatimukset ja merkitys tulevaisuuden terveyspalveluissa. Teoksessa Hoitotyön vuosikirja 2006. Inhimillisten voimavarojen johtaminen. Sairaanhoitajaliitto. Gummerus Kirjapaino Oy, Helsinki.

Lehtonen, T.,J. 2002. Organisaation osaamisen strateginen hallinta. Akateeminen väitöskirja. Kasvatustieteellinen laitos. Acta Universitatis Tamperensis 867. Tampereen yliopisto, Tampere.

Lohiniva-Kerkelä, M. 2007. Terveydenhuollon juridiikka. Talentum, Helsinki.

Metsämuuronen, J. 2006. Tutkimuksen tekemisen perusteet ihmistieteissä. Gummerus kirjapaino Oy, Vaajakoski.

Otala, L. 2000. Oppimisen etu – kilpailukykyä muutoksessa. WSOY, Porvoo.

Paavilainen, J. 1998. Tietoturva. Gummerus Kirjapaino Oy, Jyväskylä.

Pahlman , I. 2007. Asiakirjajulkisuus ja tietosuoja sosiaali- ja terveydenhuollossa. Edita Prima Oy, Helsinki.

Pahlman, I. 2010. Asiakastietojen käsittely, salassapito ja asiakkaan tiedonsaantioikeus sosiaali- ja terveydenhuollossa. Edita Prima Oy, Helsinki.

Vehviläinen-Julkunen, K. & Paunonen, M. 1998. Kvantitatiivisen tutkimuksen luotettavuus. Teoksessa Paunonen, M. & Vehviläinen-Julkunen, K. (toim.). Hoitotieteen tutkimusmetodiikka. WSOY, Juva, s. 206 – 207, 209.

Ruohonen, M. 2002. Tietoturva. WS Bookwell, Porvoo.

Ruotsalainen, P. 2006. Suositukset terveydenhuollon asiakastietojen tietoturvalliselle sähköiselle arkistoinnille. Usean toimintayksikön yhteinen käyttäjän ja käyttöoikeuksien hallinta – periaatteet ja suositukset. Stakes, Helsinki. Saatavissa: http://www.stakes.fi/verkkojulkaisut/raportit/R4-2006-VERKKO.pdf (Luettu 2.4.2011).

Saranto, K. 2007. Tiedon muodostuminen hoitoprosessissa. Teoksessa Saranto, K., Ensio, A., Tanttu, K. & Sonninen, A-L. (toim.). Hoitotietojen systemaattinen kirjaaminen. WSOY, Porvoo, s. 25 – 26.

Sosiaali- ja terveysministeriö. 2001. Potilasasiakirjojen laatiminen sekä niiden ja muun hoitoon liittyvän materiaalin säilyttäminen. Opas terveydenhuollon henkilöstölle. Sosiaali- ja terveysministeriö, Helsinki. Saatavissa: http://www.stm.fi/c/document_library/get_file?folderId=39503&name=DLFE-8444.pdf (Luettu 26.11.2010).

Sosiaali- ja terveysministeriö. 2010. Potilasasiakirjaluonnos. Sosiaali- ja terveysministeriö, Helsinki.

Sosiaali- ja terveysministeriö. 2011. Potilastietojen käsittely. Ohje terveydenhuoltolain 9 §:n ja asiakastietolain muutosten toteuttamiseksi. Sosiaali- ja terveysministeriö, Helsinki. Saatavissa:
http://www.stm.fi/c/document_library/get_file?folderId=42730&name=DLFE-14906.pdf (Luettu 9.8.2011).

Staggers, N., Gassert, C.A. & Curran, C. 2001. Informatics Competencies for Nurses at Four Levels of Practice. Journal of Nursing Education 40(7), 303 - 316.

Staggers, N., Gassert, C.A. & Curran, C. 2002. A Delphi Study to Determinen Informatics Competencies for Nurses at Four Levels of Practice. Nursing Research 51(6), 383 – 390.

Sydänmaalakka, P. 2007. Älykäs organisaatio. Gummerus Kirjapaino Oy, Helsinki.

Tammisalo, T. 2005. Sosiaali- ja terveydenhuollon tietojärjestelmien tietoturvan ja tietosuojan hallinnan periaatteet ja hyvät käytännöt. Ohje sosiaali- ja terveydenhuollon organisaatioille ja toimintayksilöille tietojärjestelmien tietoturvan ja tietosuojan kehittämiseksi. Stakes. Sosiaali- ja terveysalan tutkimus- ja kehittämiskeskus. Helsinki.
Saatavissa:
http://www.stakes.fi/verkkojulkaisut/raportit/Ra5-2005.pdf (Luettu 20.9.2010).

Tammisalo, T. 2007. Sosiaali- ja terveydenhuollon organisaatioiden tietoturvan hallinnointi. Periaatteet ja menetelmät. Stakes. Sosiaali- ja terveysalan tutkimus- ja kehittämiskeskus. Helsinki.
Saatavissa:
http://www.stakes.fi/verkkojulkaisut/raportit/R5-2007-VERKKO.pdf(Luettu 20.9.2010).

Valtiovarainministeriö. 2003. Valtionhallinnon tietoturvakäsitteistö. Valtionhallinnon tietoturvallisuuden johtoryhmä 4/2003. Helsinki. Saatavissa:
http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/50903/50902_fi.pdf (Luettu 28.4.2011).

Valtiovarainministeriö. 2004a. Tietoturvallisuus ja tulosohjaus. Valtionhallinnon tietoturvallisuuden johtoryhmä 2/2004. Helsinki. Saatavissa:
http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20040420Tietot/86049.pdf (Luettu 15.5.2011).

Valtiovarainministeriö. 2004b.Valtionhallinnon keskeisten tietojärjestelmien turvaaminen. 5 /2004. Helsinki. Saatavissa:
http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/90727_fi.pdf (Luettu 1.6.2011).

Valtiovarainministeriö. 2006. Asianhallinnan tietoturvallisuutta kokeva ohje. 5/2006. Saatavissa:
http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20060622Asianh/Vahti_5_06.pdf (Luettu 1.9.2011).

Valtiovarainministeriö. 2007. Tietoturvallisuudella tuloksia. Yleisohje tietoturvallisuuden johtamiseen ja hallintaan. Valtionhallinnon tietoturvallisuuden johtoryhmä 3/2007. Saatavissa: http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20071128Tietot/vahti3_07_netti.pdf (Luettu 1.6.2011).

Valtiovarainministeriö. 2008a. Tärkein tekijä on ihminen – henkilöstöturvallisuus osana tietoturvallisuutta. Valtionhallinnon tietoturvallisuuden johtoryhmä 2/2008. Helsinki. Saatavissa: http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20080218Taereki/Vahti2_08low.pdf (Luettu 1.4.2011).

Valtiovarainministeriö. 2008b. Tietoturvallisuus on asenne! Selvitys julkishallinnon tieturvakoulutustarpeista. Valtionhallinnon tietoturvallisuuden johtoryhmä 6/2008. Helsinki. Saatavissa: http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20081211Tietot/vahti6_taitto_NETTI_%2b_KANNET.pdf (Luettu 1.4.2011).

Valtiovarainministeriö. 2009.Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuuden kehittämisestä. Valtionhallinnon tietoturvallisuuden johtoryhmä 7/2009. Helsinki. Saatavissa: http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20091126Valtio/name.jsp (Luettu 26.11.2010).

Viitala, R. 2005. Johda osaamista. Osaamisen johtaminen teoriasta käytäntöön. Otavan Kirjapaino Oy, Keuruu.

Vilkka, H. 2007. Tutki ja mittaa. Määrällisen tutkimuksen perusteet. Gummerus Kirjapaino oy, Jyväskylä.

Virtainlahti, S. 2009. Hiljaisen tietämyksen johtaminen. Kariston Kirjapaino Oy, Hämeenlinna.

Ylipartanen, A. 2010. Tietosuoja terveydenhuollossa. Potilaan asema ja oikeudet henkilötietojen käsittelyssä. AS Pakett, Tallinna.

LIITTEET

Liite 1.

Kysely hoitohenkilöstölle tietosuoja- ja tietoturvaosaamisesta

I TAUSTATIEDOT

Vastaa seuraaviin kysymyksiin valitsemalla oikea vaihtoehto ja tarvittaessa täydennä vastaustasi kirjoittamalla sille varattuun tilaan

1) Nykyinen työsuhteesi

- Vakinainen
- Määräaikainen tai sijainen

2) Työpaikkasi kuuluu

- Perusterveydenhuoltoon
- Erikoissairaanhoitoon

3) Kuinka kauan olet käyttänyt sähköisiä potilastietojärjestelmiä työssäsi

- Alle 1 vuosi
- 1 - 5 vuotta
- 6 - 10 vuotta
- Yli 10 vuotta

4) Kuinka usein käytät sähköisiä potilastietojärjestelmiä työssäsi

- Useita kertoja päivässä
- Muutaman kerran viikossa
- Muutaman kerran kuukaudessa
- Harvemmin
- En koskaan

5) Ammatillinen koulutuksesi

- ☐ Korkeakoulututkinto
- ☐ AMK -tutkinto
- ☐ Opistotason tutkinto
- ☐ Kouluasteen tai 2.asteen tutkinto
- ☐ Muu, mikä

6) Sisältyikö ammatilliseen koulutukseesi tietosuojaan ja -turvaan liittyviä opintoja

- ○ Runsaasti
- ○ Jonkin verran
- ○ Vähän
- ○ Ei lainkaan

7) Oletko osallistunut työnantajan järjestämään tietosuoja- ja tietoturvakoulutukseen organisaatiossasi

- ○ Useammin kuin kerran
- ○ Kerran
- ○ En koskaan

8) Millaiseksi arvioisit oman tietosuoja- ja tietoturvatietämyksesi

- ○ Erittäin hyvä
- ○ Hyvä
- ○ Huono
- ○ Erittäin huono
- ○ En osaa sanoa

II YLEINEN TIETOSUOJA JA TIETOTURVA

Valitse seuraavien väittämien kohdalla mielipidettäsi parhaiten kuvaava vaihtoehto

9) Yleistä tietosuojaa ja tietoturvaa koskevat väittämät

	Samaa mieltä	Eri mieltä	En osaa sanoa
Potilasasiakirjoissa olevat tiedot ovat salassa pidettäviä	○	○	○
Salassapitovelvollisuus päättyy palvelusuhteen tai tehtävän päättymisen jälkeen	○	○	○
Potilasasiakirjoissa olevat tiedot ovat arkaluonteisia	○	○	○
Potilasasiakirjoihin saa tehdä merkintöjä vain potilaan hoitoon osallistuvat terveydenhuollon ammattihenkilöt	○	○	○
Terveydenhuollon opiskelijan potilasasiakirjoihin tekemät merkinnät hyväksyy työyksikössä hänen ohjaajansa tai tämän valtuuttama henkilö	○	○	○
Merkinnät potilasasiakirjoihin tehdään käyttäen yleisesti tunnettuja ja hyväksyttyjä käsitteitä ja lyhenteitä	○	○	○
Potilasasiakirjoihin saa merkitä vain niiden käyttötarkoituksen kannalta tarpeeellisia tietoja	○	○	○
Potilasasiakirjoihin saa merkitä vain potilasta itseään koskevia tietoja	○	○	○
Potilasasiakirjoihin kirjataan vain sellaisia arkaluonteisia tietoja, jotka ovat potilaan hoidon kannalta välttämättömiä	○	○	○

Valitse seuraavien väittämien kohdalla mielipidettäsi parhaiten kuvaava vaihtoehto ja täydennä vastaustasi sille varattuun tilaan

10) Potilasasiakirjamerkinnöistä ja merkintöjen oikeellisuudesta vastaa käyttäjätunnuksen mukaine henkilö

- ○ Samaa mieltiä
- ○ Eri mieltä
- ○ En osaa sanoa

11) Perustele vastauksesi

12) Potilaan tullessa sairaalaan potilaalle tulee kertoa hänen henkilötietojensa käsittelystä

- ○ Samaa mieltä
- ○ Eri mieltä
- ○ En osaa sanoa

13) Perustele vastauksesi

III POTILASTIETOJEN KÄSITTELY (muun muassa käyttö, luovuttaminen, korjaaminen)

Valitse seuraavien väittämien kohdalla mielipidettäsi parhaiten kuvaava vaihtoehto

14) Potilastietojen käsittelyä koskevat väittämät

	Samaa mieltä	Eri mieltä	En osaa sanoa
Potilastietoja käsitellään ilman potilaan suostumusta vain silloin, kun osallistutaan potilaan hoitoon tai siihen liittyviin tehtäviin	○	○	○
Potilastietoja saa käsitellä ilman potilaan suostumusta vain työtehtävien tai vastuun edellyttämässä laajuudessa	○	○	○
Potilas voi kieltää hoidon kannalta tarpeellisten tietojen kirjaamisen potilasasiakirjoihin	○	○	○
Potilasasiakirjamerkinnät tehdään aina viivytyksettä heti tiedon synnyttyä	○	○	○
Virheelliset tiedot saa poistaa	○	○	○
Virheelliset tiedot tulee korjata	○	○	○
Tietojen korjaamisesta jää merkintä taustatietoihin	○	○	○
Potilaalla on oikeus tarkastaa omia henkilökohtaisia potilasasiakirjojaan	○	○	○
Hoitohenkilökunta voi katsella omia potilastietojaan potilastietojärjestelmästä	○	○	○
Potilaalta ei tarvita erillistä suostumusta luovutettaessa potilastietoja häneen hoitosuhteessa olevalle	○	○	○
Alaikäisen potilaan huoltajalla on aina oikeus saada lasta koskevia potilastietoja	○	○	○
Luovutettaessa potilastietoja tietojen vastaanottajan oikeus saada tietoja tulee tarkastaa	○	○	○
Tietojen antamisesta eri viranomaisille on säädetty erityislainsäädännöllä	○	○	○
Potilastietojen luovuttamisesta ei tarvitse tehdä erillistä merkintää potilasasiakirjoihin	○	○	○

Valitse seuraavien väittämien kohdalla mielipidettäsi parhaiten kuvaava vaihtoehto ja täydennä vastaustasi sille varattuun tilaan

15) Hoitohenkilöstö saa katsella myös sellaisten potilaiden tietoja, joihin heillä ei ole hoitosuhdetta

- ○ Samaa mieltä
- ○ Eri mieltä
- ○ En osaa sanoa

16) Perustele vastauksesi

17) Potilaan omaiselle saa luovuttaa potilastietoja

- ○ Samaa mieltä
- ○ Eri mieltä
- ○ En osaa sanoa

18) Perustele vastauksesi

19) Viranomaisille saa aina luovuttaa potilastietoja heidän niitä pyytäessä

- ○ Samaa mieltä
- ○ Eri mieltä
- ○ En osaa sanoa

20) Kerro käytännön esimerkki

21) Luovutettaessa potilastietoja tietojen luovutusta koskeva laillisuus tulee varmistaa

- Samaa mieltä
- Eri mieltä
- En osaa sanoa

22) Kuvaa, miten käytännössä toimit

23) Luovutettaessa potilastietoja tietoja koskeva tietosuojan toteutuminen tulee varmistaa

- Samaa mieltä
- Eri mieltä
- En osaa sanoa

24) Kuvaa, miten toimit

IV SUOSTUMUKSEN HALLINTA

Valitse seuraavien väittämien kohdalla mielipidettäsi parhaiten kuvaava vaihtoehto

25) Suostumuksen hallintaa koskevat väittämät

	Samaa mieltä	Eri mieltä	En osaa sanoa
Tieto potilaan antamasta suostumuksesta tietojen luovuttamiseen tulee näkyä potilasasiakirjamerkinnöistä	○	○	○
Potilas voi kieltää potilastietojensa luovuttamisen silloin, kun luovutus edellyttää potilaan suostumusta	○	○	○
Potilaalla ei ole oikeutta peruuttaa antamaansa suostumusta	○	○	○

Valitse seuraavan väittämän kohdalla mielipidettäsi parhaiten kuvaava vaihtoehto ja täydennä vastaustasi sille varattuun tilaan

26) Potilaan antama suostumus tietojen luovuttamisesta koskee palvelutapahtumaa tai palvelukokonaisuutta

- ○ Samaa mieltä
- ○ Eri mieltä
- ○ En osaa sanoa

27) Perustele vastauksesi

V HENKILÖSTÖTURVALLISUUS

Valitse seuraavien väittämien kohdalla mielipidettäsi parhaiten kuvaava vaihtoehto

28) Henkilöstöturvallisuutta koskevat väittämät

	Samaa mieltä	Eri mieltä	En osaa sanoa
Käyttäjätunnukset ja salasanat on tarkoitettu vain henkilökohtaiseen käyttöön	○	○	○
Käyttöoikeudet potilastietojärjestelmiin määritellään työtehtävien ja vastuun mukaisesti	○	○	○
Tietosuojaan ja tietoturvaan liittyvästä väärinkäytöstä seuraa aina rangaistus	○	○	○
Suurin tietoturvallisuutta vaarantava tekijä on henkilökunnan toiminta	○	○	○

29) Olen tietoinen organisaation tietoturvasitoumuksen sisällöstä ja sen merkityksestä

○ Kyllä

○ En

30) Olen tietoinen organisaation tietosuojakäsikirjan ohjeistuksen sisällöstä

○ Kyllä

○ En

31) Tiedän paperimuodssa olevan salassa pidettävän tietoaineiston hävittämisen menettelytavat

○ Kyllä

○ En

VI KÄYTTÖTURVALLISUUS

Valitse seuraavien väittämien kohdalla mielipidettäsi parhaiten kuvaava vaihtoehto

32) Käyttöturvallisuutta koskevat väittämät

	Samaa mieltä	Eri mieltä	En osaa sanoa
Henkilökohtaisia käyttäjätunnuksia ja salasanoja ei saa luovuttaa muiden tietoon tai käyttöön	○	○	○
Sähköisiä potilastietojärjestelmiä voi toisinaan käyttää työtoverin käyttäjätunnuksilla	○	○	○
Tietojärjestelmien käyttäjä voidaan tunnistaa henkilökohtaisten käyttäjäoikeuksien perusteella	○	○	○
Potilastietojärjestelmästä ei tarvitse kirjautua ulos, kun työskentely lopetetaan	○	○	○
Potilas- ja hoitotietojen lähettäminen sähköpostin välityksellä on turvallista	○	○	○
Facebookissa voi kertoa hoidossa olevista potilaista ilman potilaiden henkilötietoja	○	○	○
Salassa pidettävät tulosteet on säilytettävä aina lukitussa säilytystilassa	○	○	○
Tarpeettomat salassa pidettävät tulosteet tulee hävittää aina välittömästi	○	○	○
Sähköisten potilasasiakirjojen käyttöä ei ole mahdollista seurata eikä valvoa	○	○	○
Henkilöstön potilastietojen käsittelyä ei seurata säännöllisesti	○	○	○
Potilastietojen katselusta jää aina merkintä lokitietoihin	○	○	○

VII AVOIMET KYSYMYKSET

Vastaa seuraaviin kysymyksiin kirjoittamalla vastauksesi niille varattuun tilaan

33) Miten nykyiset tietosuoja ja -turvamääräykset mielestäsi mahdollistavat joustavan toiminnan? Kerro käytännön esimerkki.

34) Mitä muuta haluat tuoda esille liittyen tietosuojaan ja tietoturvaan?

Kiitos vastauksestasi