TIETOTURVAN JA TIETOSUOJAN KEHITTÄMINEN KUVANTAMISESSA

Case Päijät-Hämeen sosiaali- ja terveydenhuollon kuntayhtymä, kuvantamisen tulosalue

LAHDEN AMMATTIKORKEAKOULU
Liiketalouden koulutusala
Julkisten palvelujen johtaminen
Opinnäytetyö
Syksy 2009
Kaisa Lehtinen ja Mervi Tuominen

Lahden ammattikorkeakoulu
Julkisten palvelujen johtaminen

Lehtinen, Kaisa & Tuominen, Mervi: Tietoturvan ja tietosuojan kehittäminen kuvantamisessa

Julkisten palvelujen johtamisen opinnäytetyö, 62 sivua, 3 liitesivua

Syksy 2009

TIIVISTELMÄ

Tämän opinnäytetyön tavoitteena on laatia yksinkertaiset ja pelkistetyt tietoturva- ja tietosuojaohjeet sekä toimintamalli ohjeiden saattamiseksi osaksi käytännön työtä Päijät-Hämeen sosiaali- ja terveydenhuollon kuntayhtymän kuvantamisen tulosalueelle.

Tämä opinnäytetyö on tehty toiminnallisena tutkimuksena, se toteutettiin käyttäen kvalitatiivista havainnointia työympäristössä ja tekemällä kyselytutkimus koko tulosalueen henkilökunnalle. Kyselytutkimusta täydentäviä kysymyksiä tarkennettiin kyselytutkimuksen jälkeen haastatteluilla ja muutamilla pistokokeilla työpisteisiin.

Tutkimuksen taustatietoina käytettiin pääosin lakeja ja normeja, aihetta käsittelevää kirjallisuutta ja Päijät-Hämeen sosiaali- ja terveydenhuollon kuntayhtymän tietoturvapolitiikkaa sekä jo aiemmin laadittuja tietoturva- ja tietosuojaohjeita ja sitoumuksia.

Kyselytutkimuksen avulla kartoitettiin henkilöstön nykytilan perustietoja tietoturvasta ja tietosuojasta. Kyselyn vastausprosentti oli 57, mitä voidaan pitää hyvänä ottaen huomioon osittaisesta henkilöstöpulasta aiheutuneet työkiireet. Kyselyn tuloksena ilmeni muun muassa henkilöstön huoli käyttäjätunnusten väärinkäyttömahdollisuuksista, tietojärjestelmien ajoittaisista katkoksista ja häiriötilanteet järjestelmien toiminnoissa. Tietoja tietoturva- ja tietosuojakäytänteistä ja ohjeista toivottiin tietoiskujen, koulutuksen sekä henkilökohtaisen opastuksen avulla. Selkeä ohjeistus oli myös toivomuslistalla.

Johtopäätöksenä voidaan todeta, että sähköistyvän yhteiskunnan mahdollistama nopea, vaivaton ja tehokas tiedon liikkuminen aiheuttaa henkilökunnalle arkielämän toiminnassa epävarmuutta tiedon suojaamisesta ja turvallisesta tiedon kanssa toimimisesta. Selkeitä, napakoita omaan työhön kohdistettuja ohjeistuksia kaivataan työelämässä.

Avainsanat: Tietoturva, tietosuoja, kuvantaminen

Lahti University of Applied Sciences
Degree Programme in Business Studies

LEHTINEN, KAISA & TUOMINEN, MERVI: Improving security and data protection in imaging

Bachelor's Thesis in Management of Public Services, 62 pages, 3 appendices

Autumn 2009

ABSTRACT

This thesis was conducted with two goals in mind. One was to create simple and clear guidelines for security and data protection for Joint Authority for Päijät-Häme Social and Health Care. The other was to make a plan on how to bring these guidelines into practice within Joint Authority for Päijät-Häme Social and Health Care's imaging division.

Our thesis has been carried out as a functional study. This thesis was conducted using qualitative observation and a questionnaire survey presented to the staff in the division. Afterwards there were interviews and random checks performed to get answers to those questions which were not in the survey. Further questions were also been made.

The background information of this thesis were mainly law and norms, literature related to the topic, Joint Authority for Päijät-Häme Social and Health Care's Security Policy and previously made security and data protection guidelines and obligations.

The aim of the questionnaire survey was to examine staff´s current knowledge of security and data protection. The rate of return (57%) was good having regard to the fact that there is a lack of resources within some staff groups which causes rush in the wards. Based on the questionnaire survey, it seems that there are some security problems. For example staff seemed to be worried about the possible abuse of usernames, occasional system failures and errors in systems. There seemed to be a request for information of codes and guidelines for security and data protection by using spots, education and personal guidance. Also a clear documentation was on the wish list.

As a conclusion it can be drawn that the quick data movement makes the staff of Joint Authority for Päijät-Häme Social and Health Care uncertain about the data protection and security on an everyday basis when working with data. There's a need for clear and compact guidelines in working life.

Key words: Data protection, Security, Imaging

SISÄLLYS

1 JOHDANTO

1.1 Työn tavoite, tutkimusongelma ja rajaus

Tämä opinnäytetyö on toiminnallinen tutkimus, jonka tavoitteena on tuottaa Päijät-Hämeen sosiaali- ja terveydenhuollon kuntayhtymän, josta myöhemmin käytetään pelkästään nimitystä yhtymä, kuvantamisen tulosalueelle toimivat tietoturva- ja tietosuojaohjeet sekä suunnitelma ohjeiden käytäntöön siirtämiseksi. Ohjeet ja toteuttamissuunnitelma tukevat tietoturvallista ja tietosuojattua toimintaa käytännön työssä.

Tietoturvalla tarkoitetaan tietojen, palvelujen, järjestelmien ja tietoliikenteen suojaamista. Tietoturva käsittää kaikki ne keinot, joilla pyritään estämään tiedon tuhoutuminen, muuttuminen tai joutuminen sivullisten käsiin. Samalla kuitenkin tiedon tulee olla niiden henkilöiden saatavilla, joilla siihen on oikeus. Tieto tallennetaan sellaisessa muodossa, että se on luettavissa, ymmärrettävissä ja tulkittavissa oikein. Lisäksi tiedon on oltava kattavaa, ajantasaista, oikeassa muodossa ja helposti käytettävissä ilman tulkinta- ja väärinkäyttömahdollisuutta. Ohjeet ja hallittu ohjeiden käyttöönotto tukevat tietoturvallista ja tietosuojattua toimintaa käytännön työssä. (Kleemola & Tervo-Pellikka 1998, 5-6).

Tietosuojasta puhuttaessa tarkoitetaan henkilön yksityisyyden suojan huomioonottamista henkilötietojen käsittelyssä yksityisyyden ja oikeusturvan varmistamiseksi (Sähköisen viestinnän tietosuojalaki 16.6.2004/516). Vaikka tietosuojan piiriin voivat kuulua myös valmisteilla olevat sopimukset, keskeneräiset tarjouskilpailut, käynnissä olevat henkilöstön hakuprosessit, työterveyshuollon tiedot ja organisaation toimintaa koskevat tiedot, eli yrityssalaisuudet, jätimme nämä käsittelemättä opinnäytetyössämme ja keskityimme lähinnä henkilöstön arkipäivän toimintaan. Tiedonkulkuun liittyvät tekniset seikat rajataan pois tästä työstä.

1.2 Työn taustaa

Aiheen valintaan vaikuttivat molemmille opinnäytetyön tekijöille opintojen myötä herännyt kiinnostus tietoturvaa ja tietosuojaa kohtaan sekä työnantajan antama toimeksianto tietosuoja- ja tietoturvaohjeiden laatimiseksi. Tämä työ tehtiin yhtymän kuvantamisen tulosalueelle, jossa sitä sovelletaan käytännön työssä. Ohjeisiin on otettu pohjaksi lait ja asetukset sekä saatavilla olevat tietoturva- ja tietosuojaohjeistukset ja yhtymän tietoturvapolitiikka. Tietoturvapolitiikka vahvistaa tietojenkäsittelyn perusturvatason eli periaatteet, jotka luovat perustan tietoturvallisuuden kehittämistoimille. Turvattavia tietoja ovat sekä manuaalisessa että sähköisessä muodossa olevat tiedot.

1.3 Tutkimuksen kulku

Tämän opinnäytetyön empiriaosuus on toteutettu kvalitatiivisella tutkimusmenetelmällä pohjautuen kyselytutkimukseen koko tulosalueen henkilöstölle (68 henkeä). Kyselyn tavoitteena oli kartoittaa henkilöstön nykytiedon taso tietoturvaa ja – suojaa koskien ja kerätä taustatietoja ohjeita ja toimeenpanosuunnitelmaa varten. Kyselytutkimuksen analysoinnin jälkeen on tarkennettu vielä epäselväksi jääneitä ja kyselyn perusteella heränneitä mielenkiintoisia seikkoja kohdistetun haastattelun keinoin. Yhtenä tutkimusmenetelmänä on käytetty myös havainnointia.

Tulosalueen toimipisteiden käytänteitä havainnoimalla on tehty ohjeet kyselytutkimuksesta saatuun informaatioon perustuen ja soveltamalla koulutuksessa saatuja tietoja ja taitoja. Ohjeistus on pyritty laatimaan yhtymän tietoturva- ja tietosuojaohjeiden kanssa toimiviksi huomioiden kuvantamisen toiminnan erityisvaatimuksia. Tietosuojavaltuutetun mukaan viranomaiset voivat laatia omaan toimintaansa sopeutettuja käytännesääntöjä. (Tietosuojavaltuutetun toimiston sivut)

Kyselytutkimuksen, haastattelujen ja havainnointitutkimuksen jälkeen peilataan yhtymän yhteisiä ohjeistuksia kuvantamisen tulosalueen toimintatapoihin. Tämän

jälkeen tuloksiin perustuen laaditaan kuvantamiseen kohdennetut lakeihin perustuvat tietoturva- ja tietosuojaohjeet sekä suunnitelma näiden jalkauttamiseksi.

Kyselytutkimuksen ja haastatteluiden avulla on pyrkimyksenä selvittää, miten tietoturva ja tietosuojalainsäädäntö kohtaavat ja koskettavat työntekijää käytännössä kuvantamisen alueella. Myös selvitetään henkilöstön kokemukset tietoturvasta ja tietosuojasta omassa työympäristössään.

Kuvantamisen tulosalueen toiminnassa liikkuu paljon henkilötietoja sisältävää tietoa. Tietoa käsitellään ja se kulkee muun muassa sähköisesti, paperilla, filmillä, suullisesti, henkilökohtaisissa kontakteissa, faxilla, ja puhelimessa. Moniammatillisessa yhteistyössä tiedonkulun saumattomuus ja turvallisuus ovat ehdottoman tärkeitä.

Henkilötietoja sisältävät rekisterit ovat henkilörekisterin vastuuhenkilön vastuulla. Tiedot kuvaustoimintaan tulevat henkilörekisteristä. Henkilörekisterillä tarkoitetaan käyttötarkoituksensa vuoksi yhteenkuuluvista merkinnöistä muodostuvaa henkilötietoja sisältävää tietojoukkoa, jota käsitellään osin tai kokonaan automaattisen tietojenkäsittelyn avulla taikka on järjestetty kortistoksi, luetteloksi tai muulla näihin verrattavalla tavalla siten, että henkilöä koskevat tiedot voidaan löytää helposti ja ilman kohtuuttomia kustannuksia. (Henkilötietolaki 523 /1999, 3 §., Laki potilaan asemasta ja oikeuksista 1992/785, 2 §., Ylipartanen 2004, 40)

Kuvantamisella tarkoitetaan tässä työssä Päijät-Hämeen sosiaali- ja terveydenhuollon kuntayhtymän keskussairaalassa toimivaa radiologian osastoa ja radiologian toimipisteitä yhtymän alueella. Kuvantamisen toiminta käsittää röntgen-, magneetti- tietokonetomografia-, varjoaine- ja ultraäänitutkimukset sekä toimenpiteet.

1.4 Työn rakenne

Toisessa luvussa käydään läpi normeja ja lakeja, joihin tietosuoja ja tietoturva perustuvat. Koska tietosuojalainsäädäntö on saanut keskeisen sisältönsä ihmisoi-

keusopimuksien ja perusoikeuslainsäädännön lisäksi EU - lainsäädännöstä, aihetta lähdetään käsittelemään sieltä saakka. Huomataan, että lait ovat erittäin hajanaisia ja niissä on osittaista päällekkäisyyttä. Kuten esimerkiksi laki viranomaisen toiminnan julkisuudesta (JulkL) ja perustuslain (PL) päällekkäisyydet aiheuttavat tulkintaongelmia.

Kolmannessa luvussa tutkitaan termejä tietoturva ja tietosuoja, sekä muita niihin läheisesti liittyviä termejä. Mitä tietoturva ja tietosuoja vaativat henkilökunnalta, ja kuinka niiden tulisi vaikuttaa esimiesten toimintaan ja asenteisiin. Myös käytön seurantaa ja valvontaa käsitellään, sekä toimenpiteitä epäiltäessä mahdollisia tietosuojarikkomuksia. Käyttöoikeuksien hallintaa sekä muita keinoja, joilla käyttöturvallisuus varmistetaan, käsitellään tässä työssä.

Neljännessä luvussa tarkastellaan Päijät-Hämeen sosiaali- ja terveydenhuollon yhtymän toimintaympäristöä ja kartoitetaan, miten tietoturvallisuustoiminta on organisoitu ja vastuut jaettu.

Viidennessä luvussa siirrytään tarkastelemaan kuvantamisen tulosalueen toimintaympäristöä ja organisaatiota. Kuvantamisen toimintaprosesseja, toiminnan erityiskysymyksiä ja tietoturvaseikkoja käydään läpi. Kuvantamisen henkilöstöturvallisuutta, tietoturvapäivityksiä sekä käyttöturvallisuutta katsastetaan. Päällisin puolin kerrotaan ohjelmisto-, laitteisto-, ja tietoliikenteen turvallisuudesta. Fyysinen turvallisuus on tärkeää tietokoneiden varassa toimivassa tietojärjestelmässä. Fyysisin turvallisuustoimenpitein luodaan toimintaolosuhteet, joilla varmistetaan järjestelmien saumaton toiminta. Tässä luvussa tarkastellaan myös tietojen turvallista käsittelyä, toiminnan jatkuvuutta ja riskienhallintaa kuvantamisen toimintaympäristössä.

Kuudennessa luvussa eli empiriaosuudessa kerrotaan tutkimusmenetelmistä ja analysoinnista Webropol-kyselynä tehtyä kyselytutkimusta, jonka tarkoituksena oli selvittää henkilöstön tiedon tasoa tietosuoja- ja tietoturva-asioissa sekä heidän kiinnostustaan kyseisiin asioihin. Muun muassa kysyttiin sähköpostin käytöstä, henkilökunnan havaitsemista tietoturvariskeistä sekä koulutuksen tarpeesta ja

minkälaista koulutusta henkilökunta haluaa. Kyselytutkimuksen määräajan päätyttyä analysoitiin kyselytutkimuksen vastaukset. Analysoinnin kuluessa mietittiin vielä, mitkä seikat mahdollisesti vaatisivat tarkennusta. Muutama pistokoe tehtiin kuvantamisen toimipisteisiin havainnoiden tietoturvallisuus- ja tietosuojaseikkoja ja haastateltiin vielä henkilökuntaa tarkennusta vaativien seikkojen selvittämiseksi. Analysoinnin perusteella laadittiin ohjeet tietoturva-asioista ja ehdotelmalista jalkauttamissuunnitelmaa varten.

Tätä opinnäytetyötä aloittaessamme sovimme, että molemmat opinnäytetyöntekijät tekevät sovitusti oman osuutensa. Laadimme yhdessä alustavan tutkimussuunnitelman, joka muuttui ja muotoutui työn edetessä. Kumpikin kokosi materiaalia työn teoriaosuutta varten. Työnjako muotoutui koko ajan työn edetessä. Kokoonnuimme usean kerran viikossa sovitusti ja hahmottelimme materiaalista yhdessä kokonaisuutta. Pidimme aluksi päiväkirjaa ohjaajamme kehotuksesta, mutta huomasimme pian kumpikin kirjoittavamme samoja asioita, joten päiväkirjan kirjoittaminen jäi. Pääosin teimme työtä tiiviisti yhdessä, välillä omilla tahoillamme, koko ajan yhteyttä pitäen ja tietoja vaihtaen. Tutkimuksen kuluessa yhteistyö sujui erittäin hyvin ja joustavasti, molemmat saivat uutta tietoa ja oppivat uusia taitoja toisiltaan ja työstä.

1.5 Tietoturvallisuuden kehittäminen

Yhtymässä on vuoden 2009 aikana laadittu tietoturvapolitiikka, tietosuoja- ja tietoturvasitoumuslomake ja internetin ja sähköpostin käyttöohjeistus on tekeillä. Tämän vuoden kuluessa on myös keskussairaalan tulosryhmä laatinut ohjeistuksen käyttöoikeuksien hallinnasta eri käyttäjäryhmiä koskien. Pohdimme yhtymän yleisen ohjeistuksen soveltuvuutta kuvantamisen käyttöympäristöön. Näihin ohjeistuksiin pohjautuen muokkasimme kuvantamisen tulosalueelle ohjeistuksen huomioiden kuvantamisen toimintatapoja.

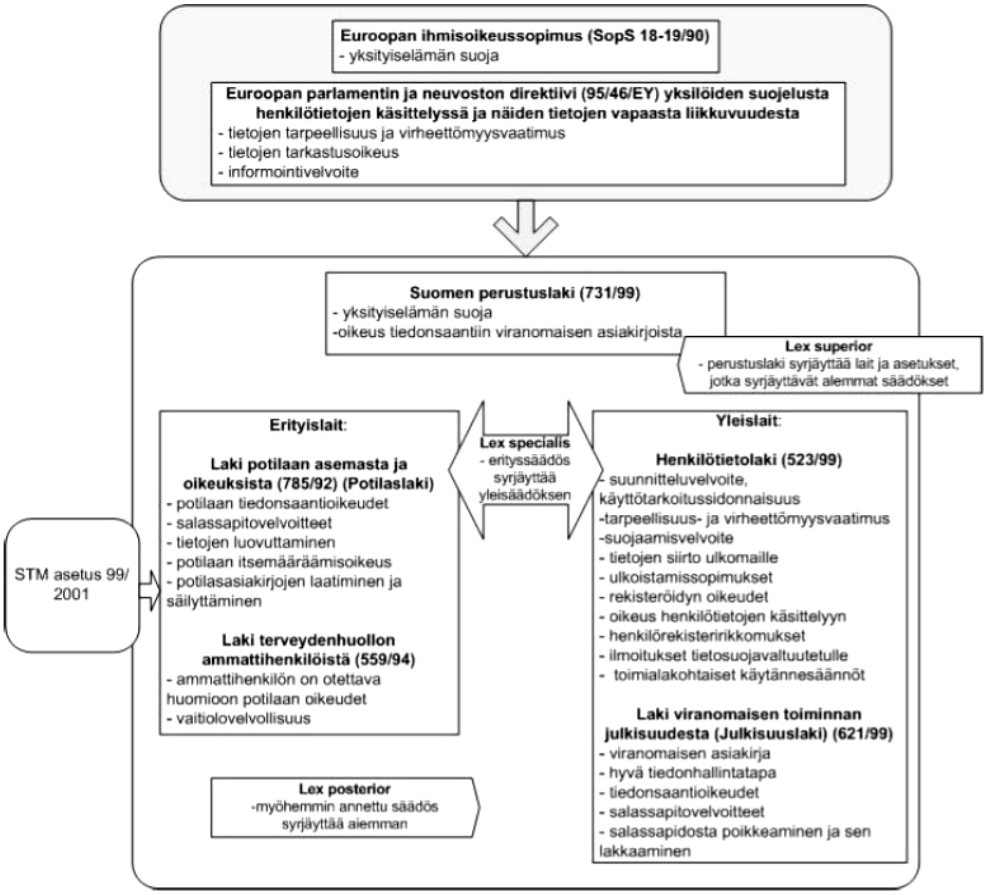
Yhtymän tietoturvallisuuden kehittäminen ja toiminta tapahtuu kansallisten ja kansainvälisten tietoturvallisuutta koskevien lakien ja asetusten pohjalta sekä erilaisia tietoturvallisuudesta annettuja ohjeita ja suosituksia noudattaen. Tässä työs-

sä käsitellään tärkeimpiä normeja ja ohjeita. Toimintaa ohjaavat mm. tietosuojasäädökset sekä joukko muita lakeja, säädöksiä, ohjeita ja standardeja. Tietoturvallisuutta koskevat määräykset ovat keskeisiä ja velvoittavia. Velvoitteissa korostetaan salassapidon, vaitiolovelvollisuuden ja yksityisyyden suojan toteutumista sekä tietoturvallisuuden, tietosuojan, hyvän tietojenkäsittelytavan ja laadun merkitystä. Toiminnan turvallisuuteen kuuluu olennaisena osana tietojen turvaaminen. (Ylipartanen 2004, 63 - 64)

2 TIETOTURVAA JA TIETOSUOJAA KOSKEVIA LAKEJA JA ASETUKSIA TERVEYDENHUOLLOSSA

Lait ja normit sääntelevät terveydenhuollon toimintaa. Suomen terveydenhuoltoon ja tietosuojaan liittyvä lainsäädännön hajaannus aiheuttaa hankaluuksia lakien tulkinnassa niiden osittaisen päällekkäisyyden vuoksi. (Järvinen 2006, 22)

Keskeisimmät lait tietosuojan kannalta terveydenhuollossa ovat potilaslaki, julkisuuslaki, henkilötietolaki ja sähköisen viestinnän tietosuojalaki. (Ylipartanen 2004, 34 - 35, 40 - 42, 51 - 60)



Kuvio 1. Terveydenhuollon henkilötietojen käsittelyyn liittyviä oikeusnormeja (Reponen 2006, 14)

Työhömme löytyi Reposen pro gradu-työstä (2006) ylläoleva kuvio 1

terveydenhuollon henkilötietojen käsittelyyn liittyvistä oikeusnormien hierarkiasta. Kuvan teksti on hieman vanhentunutta, mutta se selkeyttää lakien ja asetusten hierarkiaa ja niiden suhdetta toisiinsa nähden.

Tietosuojalainsäädäntö rajoittaa potilaan hoitoon ja terveyteen liittyvien tietojen antamista ilman henkilön suostumusta, se informoi potilaita heidän terveystietojensa käytöstä, sekä antaa potilaille oikeuden heidän omiin sairauskertomuksiinsa. (Kleemola & Tervo-Pellikka 1998, 164 – 165, Ylipartanen 2004, 49 - 50)

2.1 Henkilötietojen käsittely

Asiakkaalla on omia tietojaan koskeva itsemääräämisoikeus. Henkilötietolain 26 – 28 §. nojalla kansalaisella on oikeuksia omien tietojensa tarkistamiseen ja tarvittaessa niiden oikaisuun. Itsemääräämisoikeuden tarkoituksena on yksilön suojaamisen periaate, heikomman suojaaminen muiden taholta tulevilta oikeudenloukkauksilta. Tästä syystä lainsäädännössä on erityisesti korostettu potilaan koskemattomuutta ja itsemääräämisoikeutta, mikä käsittää oikeuden potilasasiakirjatietojen suojaan sekä oikeuden tarkastaa potilasasiakirjatietonsa. Viranomainen on velvollinen antamaan tietoja aktiivisesti ja oma-aloitteisesti, tämä perustuu perusoikeuksien turvaamisvelvoitteeseen. (Perustuslaki 731/1999, 21 §., Henkilötietolaki 523/1999 26 – 28 §., Mäenpää 2008, 38)

Terveyden- ja sosiaalihuollon palveluiden käyttöä koskevat tiedot ovat salassa pidettäviä. Henkilötietolailla pyritään turvaamaan, ettei yksityiselämän suojaa tai muita yksityisyyden suojaa turvaavia perusoikeuksia rajoiteta ilman laissa säädettyä perustetta henkilötietoja kerättäessä, talletettaessa, käytettäessä, siirrettäessä, luovutettaessa tai muutoin käsiteltäessä. (Henkilötietolaki 523 /1999 26 – 28 §., Järvinen 2002, 411 - 413)

Henkilötietolaki edellyttää tietojen käyttöön asiayhteyttä ja siten käyttöoikeus ei ole itsessään riittävä peruste terveystietojen käytölle tai luovutukselle. Tietojen luovuttaminen perustuu lakiin tai asiakkaan kirjalliseen suostumukseen, josta on oltava merkintä potilasasiakirjoissa. Asiakkaan suostumuksen yhteydessä hänelle

tulee luovuttaa jäljennös tai sähköinen tiedonsaanti suostumuksesta. Suostumuksista muodostuu osa toimintayksikön sähköistä potilasrekisteriä, joten rekisterin pitäjä on vastuussa tietojen lainmukaisesta kohtelusta. (Henkilötietolaki 523/1999, 8 §., Ylipartanen 2004, 43)

Tietosuojalainsäädäntömme on saanut keskeisen sisältönsä ihmisoikeussopimusten ja perusoikeuslainsäädännön lisäksi EU-lainsäädännöstä. Tietosuojalainsäädännön tehtävänä on luottamuksen luominen ja ylläpito.(EU 95/46, Mäenpää 2008, 53)

Tietojen käsittelyn sähköistymisen myötä on tietojen keräämisen kapasiteetti ja niiden siirtämisen nopeus lisääntyneet merkittävästi. Tietotekniikan kehitys on luonut haasteellisen ympäristön yksityisyyden suojaamiselle. Yksityisyyden suojalla on vahva sidos perusoikeuksiin. Yksityiselämän suojaa koskevan perusoikeussäännöksen taustalla on Euroopan ihmisoikeussopimuksen 8 artikla jossa sanotaan että jokaisella on oikeus hyvitykseen kansallisessa tuomioistuimessa häneen kohdistuneista teoista, jotka loukkaavat lailla turvattuja perusoikeuksia. Euroopan unionin perusoikeuskirjan 7 artiklan mukaan jokaisella Euroopan unionin kansalaisella on oikeus henkilötietojensa suojaan. EU:n lainsäädännössä määritellään tarkasti, mitä tietoja rekisterinpitäjillä on oikeus kerätä. Perusoikeussäännöksen käsitteistö pohjautuu kansainvälisiin sopimuksiin. Säännöksen tulkinnassa on mahdollista tukeutua ihmisoikeussopimusten soveltamiskäytäntöön. (EU 95/46, EU 02/58, Kleemola & Tervo-Pellikka, 1998 11 – 14, Ylipartanen 2004, 34 - 35, 40 - 42, 51 - 60)

Euroopan ihmisoikeustuomioistuimen kannanotoilla on merkitystä Suomen kansainvälisten velvoitteiden kannalta. YK:n ihmisoikeuksien 12 artikla julistaa:

> *”älköön mielivaltaisesti puututtako kenenkään yksityiselämään, perheeseen, kotiin tai kirjeenvaihtoon älköönkä loukattako kenenkään kunniaa ja mainetta. Jokaisella on oikeus lain suojaan sellaista puuttumista tai loukkausta vastaan.”*

Julistuksen sisältöä on myöhemmin täsmennetty ihmisoikeussopimuksilla, joista Suomen kannalta merkittävimpiä lienevät Euroopan neuvoston sopimukset. (YK:n ihmisoikeussopimus 12 artikla, Syrjänen 2006, 36 – 37).

Henkilötietojen käsittelylle luo perustan perustuslain 10 §., jossa säädetään yksityiselämän suojasta. Valtio turvaa yksilön suojan lailla ja valtio huolehtii organisatorisista ja muista toimenpiteistä, jotka ovat tarpeen yksilönsuojan toteuttamiseksi, kuten valvonta-koneistosta. Tämä perusoikeus merkitsee oikeutta lakisääteiseen yksilönsuojaan tietojenkäsittelyssä ja jokaisella on siten oikeus saada henkilötiedoilleen riittävä suoja. (Perustuslaki 731/1999, 10 §., Valtionhallinnon tietoturvallisuuden johtoryhmä 2/2008, Kleemola & Tervo-Pellikka 1998, 26 – 27.)

Perustuslain 10 §. käsittelee myös kirjeen, puhelun tai muun luottamuksellisen viestin salaisuutta, mikä on loukkaamaton. Jokaisella on oikeus päättää omista asioistaan ja tehdä itseään koskevat henkilökohtaiseen elämään liittyvät valinnat vapaasti ilman ulkopuolisten puuttumista. Tietojenkäsittelyssä yksilöllä tulisi olla mahdollisuus vaikuttaa omien tietojensa käyttöön. Yksilöä koskevien tietojen laajamittainen tallettaminen yksilön personallisuutta kuvaavalla tavalla voi rajoittaa henkilökohtaista vapautta. (Perustuslaki 731/1999, 10 §.)

Potilaan oikeusturvan takaamiseksi hänellä on oikeus saada tietoja sähköisistä asiakasrekistereistä, asiakastiedon käsittelyyn liittyvistä tietojärjestelmistä sekä häntä koskevista asiakastietojen käsittelyistä. Tietosuojavaltuutetun mukaan henkilötietojen käsittelyn vastuut ovat osa eri tehtävien hoitoon liittyvää toiminnallista vastuuta. Johdon on huolehdittava henkilötietojen käsittelyyn liittyvien vastuiden ja tehtävien asianmukaisesta määrittelystä. Henkilöstön ohjauksesta ja koulutuksesta on huolehdittava ja käytössä olevien tietojärjestelmien on vastattava lain vaatimuksia. Tietoturvaa lisäävien pelisääntöjen noudattaminen helpottuu, kun työntekijät ymmärtävät, miksi rajoituksia asetetaan ja miten heidän oma etunsa voi olla vaarassa, jos tietoturva pettää. Tietoturva on lääketieteellisen toiminnan perusedellytys ja viime kädessä tietoturvasta huolehtiminen kuuluu organisaation johdon vastuulle. (Järvinen 2002, 111 – 112, Tietosuojavaltuutetun toimiston sivut)

Laki sähköisen viestinnän tietosuojasta (516/2006) pyrkii turvaamaan sähköisen viestinnän luottamuksellisuuden ja yksityisyyden suojan toteutumisen sekä määrittelee myös potilastietojen käsittelystä. Laki antaa laajempia tavoitteita tietosuojan toteuttamiseksi ja organisaatiot luovat omat toteuttamis- ja toimintatapansa. Hallinnollisia vaatimuksia ovat tietosuojavastaavan nimeäminen, tietosuojapolitiikan dokumentointi, henkilökunnan koulutus tietosuoja-asioista, tiedon luotettava säilyttäminen, sekä yhteistyötahojen potilastietojen käsittelyn luotettavuuden varmistaminen ja tietosuojasanktioista huolehtiminen. (Sähköisen viestinnän tietosuojalaki 516/2006, 1 §., Laki sosiaali- ja terveydenhuollon sähköisestä käsittelystä 159/2007, 1 §., 4 §., 20 §.)

Terveydenhuollon valtakunnallisten tietojärjestelmäpalveluiden järjestämiseksi ja selkeyttämiseksi säädettiin laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä. Laissa käsitellään arkistointi- ja hakemistopalveluita, suostumuksen- ja hallintapalveluita, varmennepalveluita sekä sosiaali- ja terveydenhuollon koodistopalveluita. Tietojärjestelmäpalveluiden avulla voidaan järjestää tietoturvallisesti potilastietojen säilytys, käyttö ja luovuttaminen koko valtakunnan tasolla. Varmennepalvelun tarkoituksena on terveydenhuollon työntekijöiden ja tietoteknisten laitteiden tunnistaminen ja todentaminen. Laissa käsitellään sähköistä allekirjoitusta sekä terveydenhuollon valtakunnallista tietojärjestelmäpalveluiden potilasrekistereiden ja niihin liittyvien lokirekistereiden käsittelyä ja säilyttämistä. (Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä 159/2007, 4- 9 §., 14 §.)

Terveydenhuollon ammattihenkilöstö puuttuu oleellisella tavalla ihmisen koskemattomuuteen ammattia harjoittaessaan. Terveydenhuollon ammattihenkilön yleiset velvollisuudet määrittävät muun muassa, että on otettava huomioon, mitä potilaan asemasta ja oikeuksista säädetään. Potilasasiakirjat on laadittava ja säilytettävä sekä pidettävä salassa niihin sisältyvät tiedot siten kuin asiasta säädetään. Salassa pidettäviä ja vaitiolovelvollisuuden piiriin kuuluvia ovat myös seikat, joita on saanut tehtävänsä tai asemansa perusteella tietoonsa. (Laki ja asetus terveydenhuollon ammattihenkilöistä 559/1994, 16 – 17 §.)

2.2 Viranomaisten toiminnan julkisuus ja sitä rajoittavia perusoikeuksia

Viranomaisten toiminnan julkisuudesta annetussa laissa (621/1999) säädetään oikeudesta saada tieto viranomaisten julkisista asiakirjoista sekä vaitiolovelvollisuudesta, asiakirjojen salassapidosta ja muista tietojen saantia koskevista rajoituksista sekä viranomaisten velvollisuuksista edistää lain tarkoituksen toteutumista. (Laki viranomaisen toiminnan julkisuudesta 621/1999, 10 §.)

Julkisuuslain 1 §. mukaisesti viranomaisten asiakirjat ovat julkisia, jollei muussa laissa, erikseen toisin säädetä. Salassa pidettävästä viranomaisen asiakirjasta tai sen sisällöstä saa antaa tiedon asianosaiselle, jonka oikeutta, etua tai velvollisuutta tieto koskee ja voi näin ollen vaikuttaa hänen asiansa käsittelyyn. (Laki viranomaisen toiminnan julkisuudesta 621/1999, 1 §.)

Viranomaisen tulee hyvän tiedonhallintatavan luomiseksi ja toteuttamiseksi huolehtia asiakirjojen ja tietojärjestelmien sekä niihin sisältyvien tietojen asianmukaisesta saatavuudesta, käytettävyydestä ja suojaamisesta sekä eheydestä. (Laki viranomaisen toiminnan julkisuudesta 621/1999 3 §., 17 - 18 §., Kleemola & Tervo-Pellikka 1998, 5-6)

Organisaatiolla on velvollisuus suunnitella ja toteuttaa asiakirja- ja tietohallintonsa samoin kuin ylläpitämänsä tietojärjestelmät ja tietojenkäsittelyt niin, että asiakirjojen julkisuus voidaan vaivattomasti toteuttaa ja että asiakirjat ja tietojärjestelmät sekä niihin sisältyvät tiedot arkistoidaan tai hävitetään asianmukaisesti ja että asiakirjojen ja tietojärjestelmien sekä niihin sisältyvien tietojen suoja, eheys ja laatu turvataan asianmukaisin menettelytavoin ja tietoturvallisuusjärjestelyin ottaen huomioon tietojen merkitys ja käyttötarkoitus sekä asiakirjoihin ja tietojärjestelmiin kohdistuvat uhkatekijät ja tietoturvallisuustoimenpiteistä aiheutuvat kustannukset. (Laki viranomaisen toiminnan julkisuudesta annetun lain muuttamisesta 495/2005, 18 §., Laki viranomaisen toiminnan julkisuudesta 621/1999, 18 §.)

Organisaation velvollisuus on huolehtia siitä, että sen palveluksessa olevilla on tarvittava tieto käsiteltävien asiakirjojen julkisuudesta sekä tietojen antamisessa ja

käsittelyssä sekä niiden ja asiakirjojen ja tietojärjestelmien suojaamisessa noudatettavista menettelyistä, tietoturvallisuusjärjestelyistä ja tehtävänjaosta, samoin kuin siitä, että hyvän tiedonhallintavan toteuttamiseksi annettujen säännösten, määräysten ja ohjeiden noudattamista valvotaan. (Laki viranomaisen toiminnan julkisuudesta annetun lain muuttamisesta 495/2005, 18 §.)

Hyvän tiedonhallintatavan toteuttamiseksi organisaation velvollisuus on turvata tietojärjestelmiä suunnitellessaan ja kehittäessään mahdollisuudet hyödyntää tietojärjestelmiä muiden viranomaisten toiminnassa sekä ottaa tässä tarkoituksessa huomioon yhteensopivuuden varmistamiseksi tämän lain nojalla säädetyt tekniset vaatimukset. (Laki viranomaisen toiminnan julkisuudesta annetun lain muuttamisesta 495/2005, 18 §., Laki viranomaisen toiminnan julkisuudesta 621/1999, 18 §.).

Asetuksen viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallinnasta mukaan digitaaliset röntgenkuvat luokitellaan erityissuojattavaan tietoaineistoon. Erityissuojattavaa tietoaineistoa koskevia tietoturvallisuustoimenpiteitä ovat: tietoaineistojen tietojen käsittely- ja arkistotilat ovat riittävästi valvottuja ja suojattuja, tietojärjestelmiin pääsy on valvottua, tietoaineistoja käyttävät, muuttavat ja käsittelevät ainoastaan ne, joiden tehtäviin se kuuluu ja käyttöoikeuksia valvotaan riittävästi. (Laki viranomaisen toiminnan julkisuudesta 621/1999, 18 §.)

Laissa säädetty julkisuuden rajoitus sisältää yleensä asiakirjan tai tiedon salassapitovelvoitteen. Velvoitteeseen sisältyy velvollisuus olla vaiti asiakirjan sisällöstä. Asiakirjan tai tiedon luokittelu tietoturvallisuusvaatimusten tai sen luottamuksellisuuden asteen mukaan voivat merkitä sen julkisuuden asteen rajoittamista. (Mäenpää 2008, 43)

Tietosuojasta puhuttaessa tarkoitetaan usein henkilön yksityisyyden suojan huomioonottamista henkilötietojen käsittelyssä yksityisyyden ja oikeusturvan varmistamiseksi. Tietoturvalla tarkoitetaan tietojen, palvelujen, järjestelmien ja tietoliikenteen suojaamista. Tietoturvaan lasketaan kaikki keinot, joilla pyritään estämään tiedon tuhoutuminen, muuttuminen taikka joutuminen vääriin käsiin. Samal-

la kuitenkin tieto tulee pitää niiden henkilöiden saatavilla, joilla on siihen oikeus. Tietosuoja rajoittaa henkilötietojen käsittelyä ja luovuttamista, tietoturva puoltaa avoimuutta ja tietojen saantia. Oikeudellisena ratkaisuna on ensisijaisesti julkisuuslain soveltaminen, kun kysymyksessä on tiedon saamisesta viranomaisen hallussa olevista henkilötiedoista. (Pahlman 2007, 13)

Kirjeen, puhelun tai muun luottamuksellisen viestin salaisuus on loukkaamaton. Lailla voidaan kuitenkin säätää PL 10 §:n 3 momentin mukaan välttämättömistä rajoituksista viestin salaisuuteen, jos perusteena on yksilön tai yhteiskunnan turvallisuus, kotirauhaa vaarantavien rikosten tutkinta, oikeudenkäynti, turvallisuustarkastus tai vapaudenmenetys. (Perustuslaki 731/1999, 10 §., Mäenpää 2008, 73 - 75)

Tiedollinen itsemääräämisoikeus liittyy lähinnä henkilötietojen suojaan, mutta sillä on merkitystä myös yksilöä koskevien tietojen keräämisessä ja käsittelyssä samoin kuin tietosuojan määrittelyssä. (Perustuslaki 731/1999, 7 §.)

2.3 Sosiaali- ja terveydenhuollon asiakastietojen sähköinen käsittely

Suomessa astui 2007 voimaan laki asiakastietojen sähköisestä käsittelystä. Lain tarkoituksena on parantaa sosiaali- ja terveydenhuollon organisaatioiden mahdollisuuksia hyödyntää tietotekniikkaa palveluidensa tuottamisessa. Tietotekniikan avulla toimintayksiköt saavat tietoa oikea-aikaisesti mikä edistää potilasturvallisuutta ja samalla tehostaa palvelua. Lisäksi tarkoitus on parantaa asiakkaiden mahdollisuutta vaikuttaa omaan palveluunsa. (Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä 159/2007, 1 §.)

Sähköisen viestinnän tietosuojalain tarkoituksena on turvata sähköisen viestinnän luottamuksellisuuden ja yksityisyyden suojan toteutuminen sekä edistää sähköisen viestinnän tietoturvaa ja monipuolisten sähköisen viestinnän palvelujen tasapainoista kehittymistä. (Sähköisen viestinnän tietosuojalaki 516/2004, 1 §.)

Laissa (159/2007) säädetään yleiset vaatimukset sosiaali- ja terveydenhuollon asiakastietojen sähköiselle käsittelylle sekä eri rekisterinpitäjien ja muiden asiakastietoon oikeutettujen välisestä sähköisestä asiakaskastietojen luovuttamisesta. Tarkoituksena on turvata tietojen käytettävyys, eheys ja säilyminen sekä asiakkaiden tietosuoja. Lakia sovelletaan julkisten ja yksityisten sosiaali- ja terveyspalveluiden tuottajien toimintaan. Asiakastietojen sähköisen käsittelyn yleisten vaatimusten luvussa säädetään tietojen käytettävyydestä, säilyttämisestä ja hävittämisestä sekä käytön ja luovutuksen seurannasta lokirekisterien avulla. Lisäksi siinä määritellään vaatimuksia sähköisen asiakirjan yksilöintiin, osapuolten tunnistamiseen ja todentamiseen sekä asiakirjan sähköiselle allekirjoittamiselle. (Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä 159/2007, 4 – 9 §.)

2.4 Arkistointi

Arkistolain mukaan asiakirjan kaksi perusmuotoa ovat kirjallinen ja sähköinen tallenne. Sähköisiä tallenteita ovat digitaaliset asiakirjat, optiset asiakirjat ja muut sähköiset asiakirjat. Asiakirja on kuvallinen tai suullinen esitys kuten esityslista, päätös, selvitys, suunnitelma, lausunto, hakemus, taulukko tai piirros. Asiakirja voi olla lisäksi käyttönsä vuoksi yhteen kuuluviksi tarkoitetuista merkeistä muodostuva tietty kokonaisuus tai asiaa koskeva viesti, joka on saatavissa selville vain automaattisen tietojenkäsittelyn tai äänen- ja kuvantoistolaitteen tai muiden apuvälineiden avulla. Asiakirjoina pidettäviä viestejä ovat mm. atk-tallenteet, cd-levyt, magneettinauhat ja mikrofilmit. (Arkistolaki 831/1994, 6 §., Pahlman 2007, 13).

Sosiaali- ja terveysministeriön asetuksen ja arkistolain mukaan on laadittava suunnitelma asiakirjojen säilytysajoista ja tavoista. Suunnitelmasta on tultava esiin potilasasiakirjojen ja muun hoitoon liittyvän materiaalin luokittelu ja niiden säilytysajat, kuten röntgenlausunnot ja – kuvat tallenteina ja sähköiset tallenteet. (STM 298/2009, Arkistolaki 831/1994, 7 – 8 §.)

Potilaan asemasta ja oikeuksista annetun lain (785/1992) mukaan digitaaliarkistoinnissa tarvitaan kuvien siirtoon sairaalasta toiseen teknisinä tallenteina potilaan lupa. Digitaalisen tiedonsiirron turvallisuudesta vastaavat tietohallinto ja tietohallinnan alihankkijat. Sähköisistä potilasasiakirjoista on muodostettava arkistointipalveluun tallennettaessa ehyt asiakirjakokonaisuus yksilöimällä palvelutapahtuma- ja palvelukokonaisuudet tunnusten avulla. Hävitettäessä asiakirjoja palvelutapahtumasta tai palvelukokonaisuudesta tulee jäädä merkintä arkistoon. (STM asetus 298/2009, 4 §., Laki potilaan oikeuksista 785/1992, 21 §.)

Perustan sähköiselle terveyspalvelujen tuottamiselle muodostaa toimiva tietohallinto, sekä dokumentoinnille, toimintojen johtamiselle ja seurannalle ja palveluprosessien kehittämiselle. Terveydenhuollon perusjärjestelmien sisältämistä tiedoista muodostetaan aluetietojärjestelmä, jossa potilastiedot ovat turvallisesti ja alueellisesti käytettävissä. Potilastiedot voidaan tallentaa palveluja tuottavaan tietojärjestelmään ja tietoja voidaan luovuttaa palveluja tuottavien ja tilaavien kesken. (STM asetus 298/2009).

3 TIETOTURVA JA TIETOSUOJA TERVEYDENHUOLLOSSA

Tietosuojasta puhuttaessa tarkoitetaan henkilön yksityisyyden suojan huomioonottamista henkilötietojen käsittelyssä. Tietosuojan rajoittaessa henkilötietojen käsittelyä ja luovuttamista, tietoturva puoltaa avoimuutta ja tietojen saantia. (Laki viranomaisen toiminnan julkisuudesta 621/1999, 10 §.)

Yksilön oma vastuu korostuu päivittäisissä toiminnoissa. Tietoturvatoimien tehtävänä on vähentää ja ennaltaehkäistä tietoturvariskien syntyminen, varmistaa tietojen saatavuus kaikissa olosuhteissa ja toiminnan jatkuvuus, sekä turvata asiakkaiden ja potilaiden oikeusturvan ja yksityisyyden suojan säilyminen. Lisäksi tehtävänä on tietojen oikeellisuuden ja luotettavuuden varmistaminen sekä se, että asianosaiset ovat tiedostaneet tietoturvan merkityksen. (Päijät-Hämeen sosiaali- ja terveydenhuollon kuntayhtymän sivut, 2009.)

Tietosuojavastaava on henkilö, joka auttaa rekisterinpitäjää saavuttamaan hyvän henkilötietojen käsittelytavan ja korkean tietosuojan tason, sekä on yhtymän tietosuojan erityisasiantuntija ja antaa asiantuntija-apua sekä henkilöstölle että johdolle. (HE 253/2006, Sisäasiainministeriö, poliisiosasto, määräys SMDnro/2008/353, Päijät-Hämeen sosiaali- ja terveydenhuollon kuntayhtymän sivut, 2009)

Tietoturvavastaava on henkilö, jonka tehtävänä on ohjata ja valvoa yhtymän tietoturvapolitiikan toteutumista. Tietoturvavastaavan tehtävänä on tukea tietoturvajohdon toimintaa. Tietoturvavastaava kehittää ja ylläpitää tietoturvallisuutta, tietoturvatoimintaa, tietoturvallisuuden tilannekuvaa sekä oikeiden käytäntöjen ja asenteiden omaksumista. Tietoturvavastaava toimii yhteyshenkilönä tietoturvallisuuden johtoryhmään. Tietoturvavastaava raportoi tietoturvallisuudesta organisaation johdolle. (HE 253/2006, Päijät-Hämeen sosiaali- ja terveydenhuollon kuntayhtymän sivut, 2009.)

3.1 Johdon ja esimiehen vastuu tietoturvallisessa toiminnassa

Kaiken tietoturvallisuutta edistävän toiminnan pohjana on johdon asenne. Johdon ja esimiesten on otettava tietoturvallisuuden vaatimukset huomioon päätöksenteossa ja omassa henkilökohtaisessa toiminnassaan. Esimiesten odotetaan huolehtivan omalta osaltaan alaistensa tietoturvatietoisuuden lisäämisestä, näiden tietoturvatietoisuuden arvioinnista, sen olevan perillä tietoturvailmoituksiin suhtautumistavoista ja tarvittaessa toimenpiteisiin ryhtymistavoista. (Valtionhallinnon tietoturvallisuuden johtoryhmä 10/2006.)

Tietoturvaa koskevien menettelytapojen noudattamisen ohjaaminen ja tukeminen kuuluvat esimiesten tehtäviin. Heidän tehtävänsä on myös varmistaa omaan vastuualueeseensa kuuluvien tietoturvamenettelyjen asianmukainen suorittaminen. Esimiesten tehtävänä on myös käyttöoikeuksien ja pääsynhallinnan määrittely ja seuranta alaisten työtehtäviensä perusteella tarvitsemiin tietojärjestelmiin ja tietoihin. Tarpeettomien käyttöoikeuksien poistaminen ja rajoittaminen kuuluvat esimiehen vastuulle. Hallintolain mukaan sairaalan samoin kuin yrityksenkin tietoturvalta edellytetään sisältö- ja laatuvaatimuksia. Työntekijöiden ymmärtäessä rajoitusten asettamisen syyt ja oman etunsa vaarantumisen, tietoturvan mahdollisesti pettäessä, helpottuu myös tietoturvaa lisäävien pelisääntöjen noudattaminen. Tietoturvasta huolehtiminen on viime kädessä organisaation johdon vastuulla, tietoturvan ollessa lääketieteellisen toiminnan perusedellytyksenä. (Sisäasiainministeriö, poliisiosasto, määräys SMDno/2008/353, Järvinen 2002, 111 - 112)

3.2 Henkilöstön vastuu tietoturvallisessa toiminnassa

Tietoturvallisuudesta annettuihin ohjeisiin tutustuminen ja sitoutuminen niiden noudattamiseen kuuluvat organisaatiossa työskentelevien velvollisuuksiin. Henkilöstön osallistuessa tietoturvakoulutukseen, se oppii tunnistamaan tietoturvariskit omissa työtehtävissään ja toimintaympäristössään. Tietoisuus riskeistä auttaa myös ehkäisemään niitä. Henkilöstön aloitteelliseen tietoturvatoiminnan kehittämiseen kannustetaan. Työntekijän havaitessa tietoturvaongelmia, hän voi raportoida niistä omalle esimiehelleen, jonka tehtävä on viedä asiaa eteenpäin tietotur-

vavastaavalle tai tietosuojavastaavalle. (Valtionhallinnon tietoturvallisuuden johtoryhmä 10/2006, Järvinen 2002, 111 - 112.)

3.3 Käytön seuranta ja valvonta

Epäillyt tietoturvarikkomukset tulee selvittää ja dokumentoida tarkasti ja selvitysten perusteella syntyvät tarpeet tarkastusten tekemiseen, järjestelmien parannuksiin, lisäohjeistukseen tai muihin toimenpiteisiin tulee toteuttaa. Lokitietojen käsittelyssä on noudatettava tietoturvallisia menettelytapoja. (Sisäasiainministeriö, poliisiosasto, määräys SMDno/2008/353.)

Petteri Järvisen (2002) mukaan luottamuksellisuuden edellytyksenä on todentaminen, joka tarkoittaa identiteetin toteamista, esimerkiksi ainoastaan oikean henkilön käytössä olevaa salasanaa tai digitaalista allekirjoitusta, joilla todentaminen ainoastaan onnistuu. Todentamisen jälkeen käyttäjä saa valtuutuksen (auktorisointi) tietojen käsittelyyn ja pääsynvalvonnan (access control) tehtävänä on huolehtia vain todennettujen henkilöiden pääsy järjestelmän tietoihin. Käyttöjärjestelmä ja sovellukset vastaavat pääsyn valvonnasta johon liittyy myös käytön seuranta (audit). Järjestelmä kirjaa kaikki tapahtumat ja näiden lokitietojen avulla pystytään jäljittämään joko vahingossa tai tarkoituksella tapahtuneita tietoturvarikkomuksia. (Järvinen 2002, 22 – 27, Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista 617/2009, 2 §.)

Julkisuuslain mukaisen valitusprosessin aikana lokitietoja ei saa tuhota säilytysajan päättyessä. Haitallisista tietoturva- ja tietosuojatapahtumista kerätään jatkuvasti ajan tasalla olevaa tietoa yhdyshenkilöverkoston ja teknisten valvontatietojen avulla. Kaikki merkittävät haitalliset tapahtumat kirjataan tulevien kehittämistoimien perustaksi. Myös ns. ”läheltä piti” -tapaukset rekisteröidään. Onnettomuuksien, turvallisuusrikkomusten ja palvelujen keskeytysten seuraukset analysoidaan. (Julkisuuslaki 621/1999, 6 §., Päijät-Hämeen sosiaali- ja terveydenhuollon kuntayhtymän sivut, 2009)

Tietosuojarikkomuksia epäiltäessä voidaan yhtymän nimetyltä henkilöltä pyytää lokitietojen tarkistamista. Esimies voi tarkkailla lokitietoja, mikäli on aihetta epäillä asiatonta toimintaa tai työajan liiallista käyttöä työhön liittymättömään tietoverkon käyttöön. Tällöin esimiehen on ilmoitettava asianomaiselle, että hänen lokitietojaan tarkastetaan.(Päijät-Hämeen sosiaali- ja terveydenhuollon kuntayhtymän sivut, 2009)

3.4 Käyttöturvallisuus

Käyttöoikeuksien hallinta tarkoittaa sitä, että henkilöille myönnetään oikeuksia tietojärjestelmiin ja muihin resursseihin vain heidän tehtäviensä edellyttämässä laajuudessa. Esimiehet tai heidän valtuuttamansa henkilöt vastaavat alaistensa käyttöoikeuksien määrittämisestä ja poistamisesta. (Päijät-Hämeen sosiaali- ja terveydenhuollon kuntayhtymän sivut, 2009)

Nimetyt käyttöoikeusyhdyshenkilöt huolehtivat käyttöoikeuksien hallinnasta. Käyttöoikeudet ja niiden muutokset haetaan lomakkeella tai sähköisesti ja anomukset arkistoidaan. Työtehtävien vaihtuessa tai työsuhteen keskeytyessä tai päättyessä esimies tai hänen valtuuttamansa henkilö huolehtii oikeuksien muuttamisesta, lukitsemisesta tai peruuttamisesta. (Päijät-Hämeen sosiaali- ja terveydenhuollon kuntayhtymän sivut, 2009)

Käyttöoikeudet ovat henkilökohtaisia. Yhteiskäyttötunnuksia voidaan hyväksyä käytettäväksi ainoastaan erityisistä tarpeista johtuen ja tällöin tulee käytönvalvonta hoitaa muita kontrolleja käyttäen.(Päijät-Hämeen sosiaali- ja terveydenhuollon kuntayhtymän sivut, 2009)

Potilaan tunnistetietojen lähettäminen selväkielisenä avoimessa verkossa on kielletty. Potilaan suostumusta edellytetään potilastietoja välitettäessä konsultaatioon. Röntgenkuvan tuottanut laitos on velvollinen vastaamaan arkistoinnista. Järjestelmästä tulee ottaa varmuuskopio ulkopuoliseen systeemiin, kuten esimerkiksi tutkimustyötä varten. (Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä 159/2007)

Tietoa voivat lukea tai muokata vain ne, joille tällainen oikeus on etukäteen annettu. Potilastietojärjestelmien tietosuoja ja käyttöoikeudet voidaan katsoa monitasoiseksi suojaksi, jonka mukaan järjestelmiin tehdään käyttäjäkohtaiset tietosuojamääritykset. Käyttäjähallinnan minimimäärityksinä ovat henkilökohtainen käyttäjätunnus ja salasana, joka mahdollistaa sisäänkirjautumisen organisaation tietoverkkoon ja siellä oleviin käyttäjälle määriteltyihin palveluihin. (Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä 159/2007, 19 §.).

Sisäinen tietosuoja pohjautuu varmistusperiaatteeseen, jossa hoitosuhde oikeuttaa tietoon. Käyttöoikeudet järjestelmään on niillä henkilöillä, jotka tarvitsevat työssään potilaan kuvia. Erilaisilla käyttäjäprofiileilla ja rooleilla rajataan käyttöoikeudet ja näkymät. Tiedon eheys tarkoittaa sitä, ettei mikään ulkopuolinen taho pysty luvatta muuttamaan tiedon sisältöä. Eheys on tärkeää tietojen arkistoinnissa. Esimerkiksi turvajärjestelmiin liittyvät lokitiedostot. Kuva-arkistointi on hoidettava siten, etteivät ne ole kenenkään myöhemmin muokattavissa. (Järvinen 2002, 22 – 24.)

Tietojärjestelmien toiminnan turvaaminen takaa tietojen ja palvelujen saatavuuden. Kun tietoja tarvitaan, on verkkoyhteyksien oltava kunnossa. Varmuuskopioinnilla ja laitteiden teknisellä toimivuudella turvataan ja varmistetaan tietojen saatavuus. Vanhat tiedostot vanhentuneilla tallennusmenetelmillä, kuten röntgenkuvat filmillä, aiheuttavat ongelmia, esimerkiksi vertailukuvia nopeasti tarvittaessa. Vertailukuvien etsintä ja skannaus digitaaliseen muotoon voivat viivästyttää hoidon tai tutkimuksen aloittamista. (Järvinen 2002, 22 – 24.)

Henkilötietolain mukaan rekisterinpitäjän on toteutettava tarpeelliset tekniset ja organisatoriset toimenpiteet henkilötietojen suojaamiseksi asiattomalta pääsyltä tietoihin ja vahingossa tai laittomasti tapahtuvalta tietojen hävittämiseltä, muuttamiselta, luovuttamiselta, siirtämiseltä taikka muulta laittomalta käsittelyltä. Toimenpiteiden toteuttamisessa on otettava käytettävissä olevat tekniset mahdollisuudet, toimenpiteiden aiheuttamat kustannukset, käsiteltävien tietojen laatu, määrä ja ikä sekä käsittelyn merkitys yksityisyyden suojan kannalta. Suojaamisvelvoi-

te koskee sekä manuaalisia että sähköisesti ylläpidettäviä rekistereitä. (Henkilötietolaki 523/1999, 10 §, Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä 159/2007, 16 §.)

4 PÄIJÄT-HÄMEEN SOSIAALI- JA TERVEYDENHUOLLON KUNTAYHTYMÄN TOIMINTAYMPÄRISTÖ

4.1 Päijät-Hämeen sosiaali- ja terveydenhuollon kuntayhtymä

Päijät-Hämeen sosiaali- ja terveydenhuollon kuntayhtymä, käyttönimeltään Päijät-Hämeen sosiaali- ja terveysyhtymä aloitti toimintansa 1.1.2007. Yhtymä muodostettiin tuottamaan erikoissairaanhoidon palveluja kaikille 15 jäsenkunnalleen, perustason terveys- ja sosiaalipalveluja 8 kunnalle ja ympäristöterveydenhuollon palveluja 11 kunnalle. Eri organisaatioiden liittäminen yhteen, useiden erilaisten käytänteiden ja toimintakulttuureiden yhdistäminen on vaatinut toimintojen yhtenäistämistä ja sovittelemista tietoturvallisen ja tietosuojatun toiminnan takaamiseksi. Yhtymän toimialat ovat erikoissairaanhoito, sosiaali- ja perusterveydenhuolto sekä ympäristöterveydenhuolto. (Päijät-Hämeen sosiaali- ja terveydenhuollon kuntayhtymän sivut, 2009)

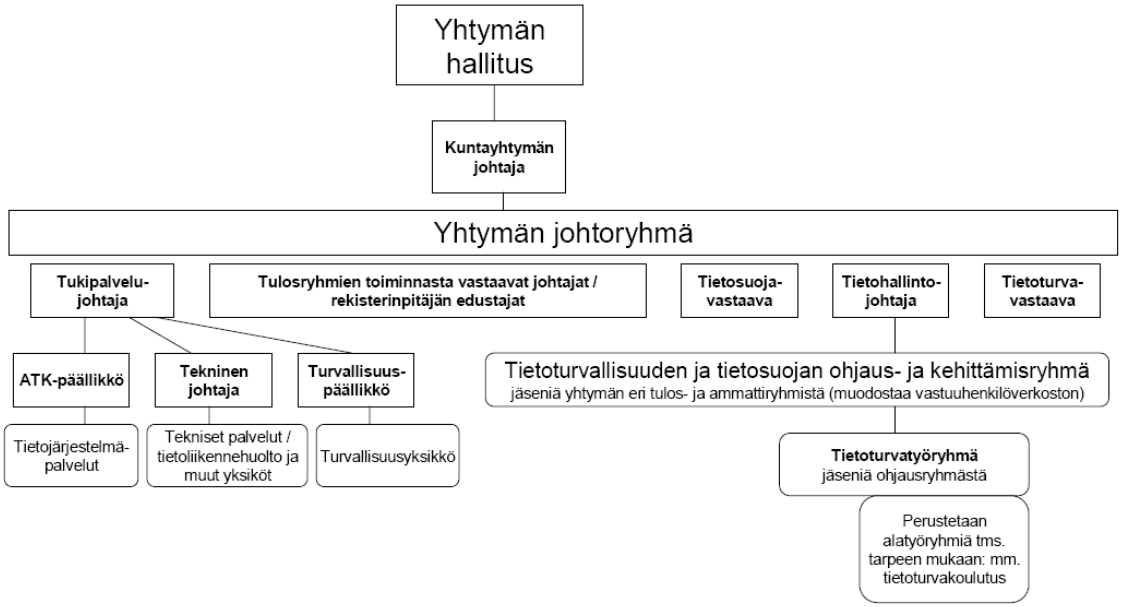
Yhtymän ylintä päätösvaltaa käyttää valtuusto, johon jäsenkuntien kunnanvaltuustot valitsevat jäsenet. Valtuuston alaisena yhtymää johtaa hallitus. Hallituksen jaosto vastaa laissa sosiaali- ja terveyslautakunnalle sekä kunnan terveydensuojeluviranomaiselle määrätyistä tehtävistä siltä osin kuin kunnat ovat antaneet sosiaalihuollon, perusterveydenhuollon tai ympäristöterveydenhuollon tehtävien hoitamisen yhtymälle. (Päijät-Hämeen sosiaali- ja terveydenhuollon kuntayhtymän sivut, 2009)

Hallinnon ja talouden tarkastuksen järjestämisestä vastaa tarkastuslautakunta. Ruotsinkielisen väestön palvelujen kehittämiseksi ja yhteensovittamiseksi yhtymässä on kielellisen vähemmistön lautakunta. Yhtymän konsernihallinnon tehtäviä hoitaa yhtymähallinto, jota johtaa yhtymän johtaja. (Päijät-Hämeen sosiaali- ja terveydenhuollon kuntayhtymän sivut, 2009)

Tulosryhmiä on seitsemän ja ne ovat peruspalvelukeskus, ensihoito- ja päivystyskeskus, keskussairaala, kuntoutuskeskus, lääketieteellisten palvelujen keskus,

ympäristöterveyskeskus ja hallinto- ja tukipalvelukeskus. Vakinaista henkilökuntaa yhtymässä on noin 3200. (Päijät-Hämeen sosiaali- ja terveydenhuollon kuntayhtymän sivut, 2009)

4.2 Tietoturvallisuuden organisointi ja vastuut



Kuvio 2. Päijät-Hämeen sosiaali- ja terveydenhuollon kuntayhtymän tietoturvaorganisaatio (Päijät-Hämeen sosiaali- ja terveydenhuollon kuntayhtymän sivut, 2009)

Tietoturvatyön johtaminen on osa toiminnanohjausprosessia, kuten yllä olevasta kuvasta nähdään. ”Käytännön tietoturvatoimia hallinnoi ja hoitaa nimetty Päijät-Hämeen sosiaali- ja terveysyhtymän tietoturvallisuusorganisaatio.” (Päijät-Hämeen sosiaali- ja terveydenhuollon kuntayhtymän sivut, 2009)

Yhtymän hallituksen hyväksymän tietoturvapolitiikan mukaan yhtymän johtaja vastaa tietoturvallisuuden yleisestä järjestämisestä. Tietosuojasta ja tietoturvallisuudesta vastaavat johtoryhmän alaisuudessa toimivat henkilöt. Tulosryhmän toiminnasta vastaavat sekä tulosalueiden ja -yksiköiden esimiehet ovat omalta osaltaan vastuussa tietoturvan toteuttamisesta omissa yksiköissään. Näiden vastuulla

ovat sekä fyysinen, tekninen, toiminnallinen että valvonnallinen toiminta. Johdon vastuulle kuuluvat myös tietoturvanäkökohtien huomioon ottaminen ulkoistettaessa toimintoja, laitehankinnoissa tai palvelujen hankkimisessa ulkopuolisilta. (Päijät-Hämeen sosiaali- ja terveydenhuollon kuntayhtymän sivut, 2009)

Tietoturvatyön toimintaan kuuluvat päivittäisten toimien ohella tietojen turvaamismenettelyjen määrittely ja ylläpito, työhön osoitettujen riittävien resurssien turvaaminen sekä välineistön ja toimenpiteiden turvallisuudesta ja tietoturvaominaisuuksista huolehtiminen. (Päijät-Hämeen sosiaali- ja terveydenhuollon kuntayhtymän sivut, 2009)

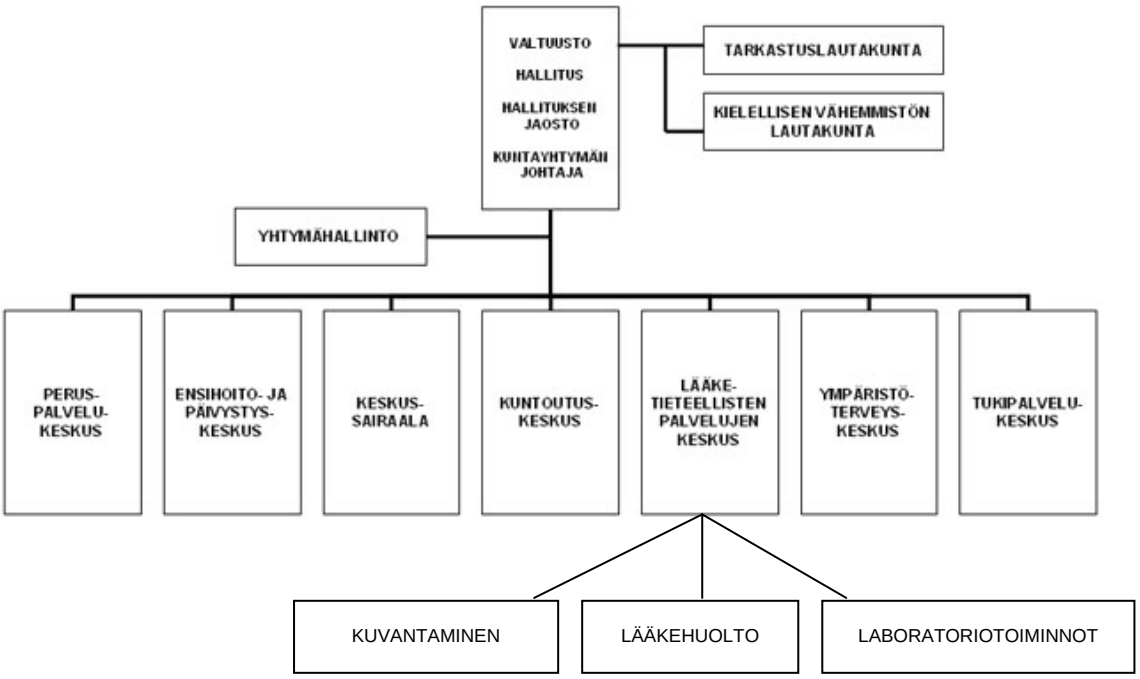
Henkilörekisterilain mukaisesta rekisterihallinnosta annetun ohjeen mukaan rekisterinpitäjien edustajat (tietojärjestelmien omistajat rekistereineen) vastaavat tietoturvan ja tietosuojan toteutumisesta jokaisen rekisterin osalta. Käyttötarkoituksen perusteella yhtymän henkilörekisterit voidaan jakaa kolmeen ryhmään, jotka ovat potilasrekisteri, henkilöstöhallinnon rekisteri ja työterveyshuollon rekisteri. (Päijät-Hämeen sosiaali- ja terveydenhuollon kuntayhtymän sivut, 2009, Henkilötietolaki 523/1999.)

5 KUVANTAMISEN TULOSALUE

5.1 Tulosryhmän ja tulosalueen kuvaus

Lääketieteellisten palvelujen keskus tuottaa koko Päijät-Hämeen sosiaali- ja terveydenhuollon yhtymän alueen laboratorio- kuvantamis- ja lääkehuollon palvelut.

Tulosryhmään kuuluvat Artjärven, Hartolan, Iitin, Myrskylän, Nastolan, Pukkilan, Orimattilan ja Sysmän sekä Läntisen perusturvapiirin laboratorio- ja kuvantamistoiminnot sekä lääkehuolto. Henkilöstöä tulosryhmässä on 213 ja talousarvio vuonna 2009 on 15 999 000 euroa. (Päijät-Hämeen sosiaali- ja terveydenhuollon kuntayhtymän sivut, 2009)



Kuvio 3. Päijät-Hämeen sosiaali- ja terveydenhuollon kuntayhtymän organisaatio, Lääketieteellisten palvelujen keskus, Kuvantaminen (Päijät-Hämeen sosiaali- ja terveydenhuollon kuntayhtymän sivut, 2009, mukaeltu)

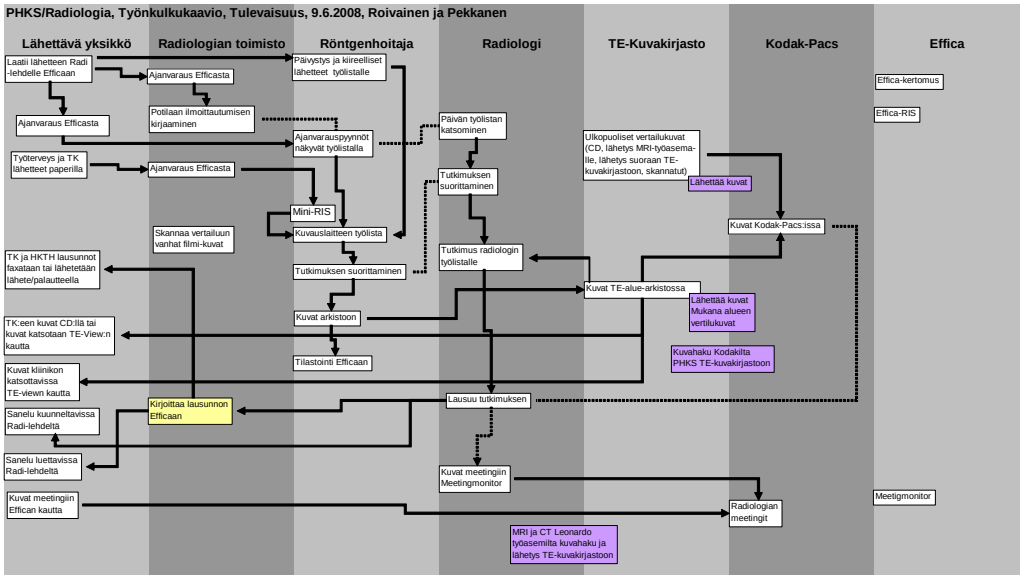
Kuvantamisen tulosalueeseen kuuluvat Päijät-Hämeen keskussairaalassa toimiva radiologian toimipiste sekä alueella toimivat seitsemän toimipistettä. Tulosalueen eri toimipisteissä työskentelee toiminnasta vastaavan ylilääkärin alaisuudessa yhteensä 63 henkilöä.

Kuvantamisen toimintaa ohjaavat toisessa luvussa mainitut lait ja normit tietoturvan ja tietosuojan osalta. Näiden lisäksi toimintaa ohjaavat ja toiminnan oikeutusperiaatteita määrittelevät myös muun muassa kuntalaki (365/1995), potilasvahinkolaki (585/1986) ja säteilylaki (592/1991). Säteilyturvakeskus valvoo toimintaa ja lain noudattamista. Oikeutusperiaatteen mukaan säteilyn käytöstä on oltava enemmän hyötyä kuin haittaa, joten turhia röntgenkuvauksia on pyrittävä välttämään. Yksilönsuojaperiaate määrittelee, että työntekijöiden ja yksilön säteilyannostus ei saa ylittää vahvistettuja enimmäisarvoja. Röntgenkuvien merkitys sairauksien tunnistamisessa on diagnosoinnin kannalta keskeistä ja siksi järjestelmien on toimittava siten, että kuvat ovat oikeassa paikassa oikeaan aikaan oikeassa muodossa niiden henkilöiden saatavilla, jotka sitä nimenomaisesti tarvitsevat asiakkaan hoidon tai sen suunnittelun vuoksi. Organisaation johdon vastuulla on järjestää laitteistot ja ohjelmistot siten, että sähköinen tiedonsiirto toimii varmasti, aukottomasti, viivytyksettä, tietoturvallisesti ja tietosuojatusti. (Säteilylaki 592/1991, 12 §., 14 §.)

5.2 Kuvantamisen toimintaprosessit

Tässä luvussa on selostettu kuvantamisen toimintaa lähinnä siltä osin kuin toiminnan eri vaiheissa käsitellään tietoturvaa ja tietosuojaa vaativia seikkoja. Kuvantamisen toiminnassa käsitellään henkilötietoja eri toimipisteissä. Röntgenkuvat tallennetaan digitaaliseen kuva-arkistoon. Kuvia voivat katsella yhtymän terveysasemilla sekä keskussairaalassa ne henkilöt, joille on annettu kuvankatseluun käyttäjähallinnan määrittelemät oikeudet ja joilla on siihen oikeus asiakkaan hoidon tai hoidon suunnittelun vuoksi. Sähköisen kuvansiirron muihin organisaatioihin ja arkistoinnin hoitavat tietohallinto ja ohjelmistot tietosuojatuin ja varmistetuin menetelmin. Kuvien lähettäminen tapahtuu lain säännöksen mukaisesti

asiakkaan kirjallisella suostumuksella, josta on oltava merkintä potilasasiakirjoissa. Tietoturvallisuuden ja – suojan on oltava osana kaikkea toimintaa.



Kuvio 4. Pacs-hoitajien laatima Radiologian työnkulkukaavio (Roivainen & Pekkanen 6/2008)

Yllä oleva kuvio kuvaa hyvin radiologian toimintojen työnkulkua moniammatillisessa yhteistyössä ja etenemistä asiakkaan ajanvarauksesta tutkimuksen kautta valmiiseen tulkintaan. Työnkulussa tiedon saumaton ja turvallinen siirtyminen on ehdottoman tärkeää.

Radiologian toimistossa hoidetaan ajanvarausta kiireellisten, työterveyshuollon ja terveysasemien tutkimusten osalta. Ajanvaraus toimii sähköisesti, asiakkaiden henkilötiedot tulevat henkilörekisteristä. Työterveyshuollon ja terveysasemien asiakkaiden tutkimuspyynnöt ovat paperimuodossa. Toimistohenkilökunta kirjaa asiakkaiden ilmoittautumisen, ohjaa heidät oikeisiin odotustiloihin ja yksiköihin, varmistaa, että vanhat vertailukuvat ovat käytettävissä, skannaa vanhat filmikuvat digitaaliseen muotoon, kirjoittaa ja tulostaa lausuntoja. Suurimman osan röntgenkuvien lausunnoista kirjoittavat ja tulostavat tekstinkäsittelijät. (Roivainen & Pekkanen 6/2008)

Röntgenhoitaja seuraa monitorilta työlistaa, jonka kautta pääsee asiakastietoihin, joista näkyvät tutkimuspyynnöt. Röntgenhoitajan on kirjattava paperimuodossa olevat työterveyshuollon ja terveysasemien lähettämien potilaiden tutkimuspyynnöt manuaalisesti järjestelmään. Ennen tutkimuksen aloittamista röntgenhoitajan on luettava lähettävän lääkärin kirjoittama säteilylain mukaisesti laadittu tutkimuspyyntö. Tutkimuspyynnöstä on selvittävä riittävät taustatiedot tutkimuksen oikeutukseen. Ilman tutkimuspyyntöä ei röntgenkuvausta voi teknisesti eikä käytännössä aloittaa digitaalisessa kuvantamisessa. Kun pyyntö on asianmukainen ja luettu, kutsuu röntgenhoitaja asiakkaan odotusaulasta nimellä tutkimushuoneeseen, suorittaa tutkimuksen tutkimusprotokollan mukaisesti, tilastoi annetut säteilyarvot, tiedot tutkimuksen kulusta, mahdolliset huomautukset ja laittaa kuvat sähköiseen arkistoon. Röntgenhoitaja ohjaa asiakkaan seuraavaan pisteeseen. Kuvantamistapahtuman aikana toimitaan näyttöpäätteiden kautta henkilötietoja käsittelevissä sähköisissä potilasasiakirjoissa sekä asiakaskontaktissa. (Roivainen & Pekkanen 6/2008)

Potilaskuljettajat saavat röntgenhoitajilta paperiset kuljetuspyynnöt, jotka sisältävät potilaan nimen, osaston, kuljetusvälineen ja tutkimushuoneen, johon asiakas tulee noutaa. Kuljettaminen tapahtuu osastoilta kuvantamiseen ja takaisin osastoille. Potilaspaperit ja röntgenkuvat tulevat potilaan mukana sängyn päällä kaikkiin toimenpiteisiin. Ellei kysymyksessä ole toimenpide, sähköisten järjestelmien mahdollistamana ei enää tarvitse papereita tai kuvia potilaan mukana kuljettaa, joten tässä tietoturva ja tietosuoja ovat konkreettisesti parantuneet. (Roivainen & Pekkanen 6/2008)

Radiologi (röntgenlääkäri) tutkii päätteeltä oman tutkimushuoneensa päivän työlistan, suorittaa potilaan erikoistutkimukset röntgenhoitajan avustuksella. Radiologi katsoo ja tulkitsee kuvat monitorilta sekä sanelee digitaalisesti tutkimuksen tuloksen. Radiologin katsoessa aiheelliseksi käydä kuvauksen tai toimenpiteen tulokset yhdessä hoitavien lääkäreiden kanssa läpi, ne valitaan meeting-listalle. Röntgenmeetingissä radiologit ja hoitavat lääkärit tarkastelevat tehtyjä tutkimuksia ja radiologit antavat palautetta tutkimusten oikeutuksesta sekä lausuvat röntgenkuvat. Meetingin jälkeen linkki meetinglistan ja asiakkaan kuvien väliltä pois-

tetaan ja kuvat säilyvät arkistossa. Radiologin tutkinnan, kuvankäsittelyn, lausunnon antamisen ja meetingtoiminnan ajan käsitellään henkilötietoja sähköisesti. (Roivainen & Pekkanen 6/2008)

Alueen toimipisteissä työskentelee yhdestä kahteen ja puoleen röntgenhoitajaa toimipistettä kohden sekä yksi terveyskeskusavustaja. Kuvaustoiminta ja asiakastietojen käsittely tapahtuvat pääpiirteittäin teoriassa saman kaavan mukaan kuin keskussairaalan röntgenosastolla, sovellettuna toimipisteen omien vaatimusten ja toimiympäristön mukaan. Asiakkaan röntgenkuvat siirtyvät TE-aluearkistoon. Röntgenlääkärit käyvät toimipisteissä viikoittain tekemässä tutkimuksia ja lausumassa kuvia digitaalisesti. Laskutusta varten toimipisteistä lähetetään asiakaslistoja röntgenosastolle keskussairaalaan. (Haastattelut)

Pacs-hoitajat ovat sähköisen kuvankäsittelyn, tilastoinnin ja arkistoinnin järjestelmäasiantuntijoita. Pacs-hoitajat polttavat röntgenkuvia CD-levyille ja hoitavat kuvansiirrot toisiin organisaatioihin sähköisesti. Heidän tehtäviinsä kuuluu myös uusien työntekijöiden perehdyttäminen sähköiseen potilastietojärjestelmään. Pacs-hoitajat ovat kaiken aikaa tekemisissä tietoturva- ja tietosuoja-asioiden kanssa ja varmistavat tietohallinnon sekä ohjelmistotalojen kanssa tietoturvallista ja tietosuojattua toimintaympäristöä kuvantamisessa. (Haastattelut)

5.3 Erityiskysymyksiä toiminnoissa

Työterveyshuollon tutkimuspyynnöt eivät ole sähköisessä potilashallintajärjestelmässä. Työterveyshuoltolain mukaan työterveyshuollon rekisteri on pidettävä erillään työnantajan rekistereistä. Tutkimuspyynnöt toimitetaan paperilla radiologian toimistoon ajanvarausta varten. Röntgenhoitaja kirjaa tutkimuspyynnön erilliseen järjestelmään, suorittaa ja tilastoi tutkimuksen ja arkistoi kuvat. Paperipyynnöt toimitetaan radiologille, joka tutkimuksen jälkeen tulkitsee kuvat ja sanelee lausunnot nauhalle. Sanelun jälkeen paperit kuljetetaan tekstinkäsittelijöille, jotka kirjoittavat lausunnot ja tulostavat sen paperille. Lausuntoja ei tallenneta potilastietojärjestelmään, vaan Pacs-hoitajien tarkistuksen jälkeen vastaus faxataan työterveyshuoltoon, jossa ne siirretään heidän omaan sairauskertomusjärjes-

telmäänsä. Kuvat arkistoidaan yhteiseen kuva-arkistoon. Työterveyshuollon aukioloaikojen ulkopuolella lausunnot eivät ole käytettävissä. Paperisista asiakirjoista sähköisiin siirtyminen nopeuttaisi toimintaa ja tietoturvallisuus paranisi. (Työterveyshuoltolaki 1383/2001 18 §., 21 §., HE 75/2000, Nyyssölä 2009, 36 - 37)

Havainnoimamme käytänteen mukaan kuvien, kuvauspyyntöjen ja siirrettävien tallenteiden postitus ostopalvelutoiminnoissa muihin organisaatioihin tapahtuu postitse. Lausunnot ja kuvat tallennetaan ostopalvelutoiminnoissa muistitikulle ja lähetetään postitse kuvantamiseen järjestelmään siirrettäväksi. CD-levyille tallennetut kuvat lähetetään pyydettäessä postitse tai kuriiripostina asiakkaille.

Sähköinen kuvamateriaalin välittäminen tapahtuu tietojärjestelmäpalveluiden hoitamin tarvittavin salausmenettelyin muihin terveydenhuollon organisaatioihin sekä potilastietojen välittäminen alueen terveysasemille. Viestinvälityksen tietosuojaa koskevat vaatimukset ja vastuut on määritelty sopimuksissa. (Päijät-Hämeen sosiaali- ja terveydenhuollon kuntayhtymän sivut, 2009)

5.4 Henkilöstöturvallisuus

Tietojärjestelmien käyttäjähallinta rakentuu henkilötietojen hallinnasta, käyttöoikeuksien ja pääsynhallinnasta, tunnistamisesta, käyttöoikeuksien jakamisesta sekä käyttöoikeuksien seurannasta. Käyttäjähallintaan kuuluvat organisaatiossa yhteisesti sovitut toimintatavat, joiden perusteella tietojärjestelmien käyttöoikeuksia määritellään, luodaan, ylläpidetään ja hyödynnetään. (Päijät-Hämeen sosiaali- ja terveydenhuollon kuntayhtymän sivut, 2009)

Käyttäjähallinta perustuu henkilön asemaan organisaatiossa ja roolimäärityksiin. Tietojärjestelmän käyttäjälle myönnetään tehtävän vaatimat oikeudet tietojärjestelmiin. Esimies vastaa henkilöstönsä käyttöoikeuksien hallinnoinnista, niiden myöntämisestä, muuttamisesta ja poistamisesta. Kuvantamisen tulosalueella työskentelee useiden eri yksiköiden ja eri esimiesten alaisia henkilöitä sekä vaihtuvia sijaisia. Näiden käyttäjäoikeuksien hallinta olisi pystyttävä hoitamaan hallitusti tarpeettomien käyttäjäoikeuksien voimassaolon poissulkemiseksi. Tietoturvapoli-

tiikka ohjeistaa toimintatavat työsuhteen päättyessä. Esimiehen tai hänen valtuuttamansa henkilön tulisi ilmoittaa tietohallintoon henkilön työsuhteen päättyessä asianmukaisesti käyttöoikeuksien ja materiaalin luovuttamiseksi. Hankaluutta aiheuttavat henkilöiden liikkuvuus ja usean eri esimiehen alaisuudessa työskentely. (Päijät-Hämeen sosiaali- ja terveydenhuollon kuntayhtymän sivut, 2009)

Kuvastamisessa yleisperehdyttämisvaiheessa esimies käy läpi tietoturva- ja tietosuoja-asiat uuden henkilön tullessa työhön. Henkilöstön omaa panosta tietoturvallisuuden tehostamiseen ja tiedottamiseen painotetaan. Käytännössä uusi työntekijä perehtyy tietojärjestelmiin omassa työpisteessään. Jokainen omalta osaltaan voi myös vaikuttaa tietoturvallisuuteen panostamalla työympäristössään. (Päijät-Hämeen sosiaali- ja terveydenhuollon kuntayhtymän sivut, 2009)

Etätyöskentelymahdollisuuden käyttö on tällä hetkellä vähäistä erikseen määritellyillä henkilöillä ja tapahtuu suojatussa verkossa turvallisen VPN-yhteyden kautta. Kasvava mobiililaitteiden käyttö tulee huomioida tietoturvatyössä. (Haastattelut)

5.4.1 Tietoturvapäivitykset ja käyttöturvallisuus

Tiedon oikeudeton käyttö on estettävä luottamuksensuojaperiaatteen mukaan. Tiedon lukemiseen tai muokkaamiseen on oikeus vain käyttäjähallinnan antamilla valtuutuksilla, esimerkiksi kuvien hakeminen arkistosta. Potilastietojärjestelmien tietosuoja ja käyttöoikeudet voidaan katsoa monitasoiseksi suojaksi, jonka mukaan järjestelmiin tehdään käyttäjäkohtaiset tietosuojamääritykset. Henkilökohtainen salasana ja käyttäjätunnus ovat minimimäärityksiä tietoverkkoon sisäänkirjautumisessa. (Päijät-Hämeen sosiaali- ja terveydenhuollon kuntayhtymän sivut, 2009)

Kuvantamisessa salasanojen vaihto tapahtuu pakotetusti ja valvotusti kolmen kuukauden välein. Jokaisella on henkilökohtainen vastuu omien tunnuksiensa ja salasanojensa käytöstä. Työasemat avataan pääosin yleistunnuksilla, kirjautuminen potilashallintajärjestelmään on ohjeistettu tehtäväksi jokaisen omilla tunnuk-

silla. Tämä on tärkeää myös tilastoinnin, seurannan sekä laadunvalvonnan vuoksi.

Paperitulosteissa tieto luokitellaan tietosuojattuun ja keräyspaperiin. Sähköisessä järjestelmässä tietosuojattua tietoa ovat henkilötietoja koskevat tiedot. Paperimuodossa olevan salatun ja tietosuojatun materiaalin hävittäminen tapahtuu keskitetysti yhtymän yleisten käytänteiden ja säädettyjen määräaikojen mukaisesti. Sähköisen salatun materiaalin hävittämisen hoitaa tietohallinto lain säätämien määräaikojen puitteissa. (Haastattelut)

Tietojen ja tietojärjestelmien vastuuhenkilöt kuvantamisessa on nimetty pelkästään kuvankäsittelyjärjestelmään. Nämä huolehtivat järjestelmän perusperehdyttämisestä, koulutuksesta sekä vastaavat käyttöoikeuksien antamisesta. Koko yhtymän alueella sijaitsevien toimipisteiden käyttöoikeuksien antamisen hoitavat alueen pääkäyttäjät. Tietohallinto antaa perusoikeudet verkkoon ja sähköpostiin sekä niihin tiedostoihin, joihin työntekijälle määritellään oikeudet. Näistä oikeuksista päättää ja vastaa esimies. Kuvantamisessa opiskelijoille ei anneta henkilökohtaisia oikeuksia yhtymän järjestelmiin, vaan he toimivat valvotusti ohjaajan valvonnassa. (Haastattelut)

Tietojärjestelmäpalvelut hoitavat varmuuskopioinnin tietoturvallisuuden vaatimalla tasolla. Virustarkastukset, päivitykset ja automaattitarkastukset on organisoitu tietoturvallisuusnäkökulmat huomioiden. (Haastattelut)

5.4.2 Ohjelmisto-, laitteisto-, ja tietoliikenteen turvallisuus

Havainnointiin ja haastatteluihin perustuen selvisi, että kuvantamisessa käytetään useita eri ohjelmistoja, joita muun muassa ovat toimisto-ohjelmistot, henkilöstön tietojen käsittelyyn tarkoitetut ohjelmistot, henkilöstön itseasiointijärjestelmät, potilastietojen rekisteröintitehtäviin ja käsittelyyn tarkoitetut ohjelmistot, eli potilastietojärjestelmät. Näiden järjestelmien käytöstä vastaa yhtymän tietojärjestelmäpalvelut organisaation käytänteiden mukaisesti.

Siirrettävien medioiden käytössä on korostettava turvatoimia etenkin vierailevien luennoitsijoiden, konsulttien, vuokralääkäreiden ja esittelijöiden toimiessa yhtymän verkossa. Tietoturvallisuusluokittelussa kuvantamisessa korkeimmalle luokitellut kuvankäsittelypäätteet on suojattu ohjelmiston- ja laitteistontoimittajan toimesta. Tietojärjestelmäpalvelut hoitavat tietoliikenteen salaamisen. Sähköpostiliikenteen käyttö on suodatettua ja tarvittaessa salattua.

5.5 Fyysinen turvallisuus

Tietokoneiden varassa toimiva tietojärjestelmä on teknisesti haavoittuva. Fyysisin turvallisuustoimenpitein luodaan ja ylläpidetään tietotekniikan vaatiman käyttöympäristön (tilat, laitteet, tiedonsiirto ja käyttö) toimintaolosuhteet, joilla varmistetaan tietoteknisten järjestelmien toiminta niin, että pystytään takaamaan tietojen ja palvelujen saumaton ja asianmukainen käytettävyys tarpeen tullen. (Järvinen 2002, 22 - 24.)

Laitteiden sijoittaminen ja tilojen suojaaminen on hoidettu valvomalla yhtymän kiinteistöjä, niiden erikois- ja laite- yms. tiloja luvattomia tai rikollisia toimia vastaan sekä onnettomuuksilta että luonnontuhoilta. Havainnointimme mukaan kuvantamisen asiakaspalvelupisteessä tietosuojan turvaamiseksi on asennettu heijastesuojat sivullisille näkyvyyden estämiseksi. Oman työhuoneen haltijat ovat ohjeistettu lukitsemaan huoneensa ja päätteensä huoneesta poistuessaan. Radiologian aulatiloihin pääsee virka-aikana, virka-ajan ulkopuolella kulku on mahdollista vain kulkuluvan omaaville.

Kulunvalvonta on järjestetty henkilöstön osalta henkilökohtaisella kulunvalvontajärjestelmällä sekä yleisesti valvontakameroin. Tietoturvallisuuden kannalta merkittävät paikat on asianmukaisesti lukittu ja suojattu onnettomuuksien varalta. Lukittuihin tiloihin on pääsy vain tarkoin rajatulla henkilöstöllä ja kulunvalvonta on tarkkaa. Tunnistukset, hälytykset ja torjunta vahinkojen varalta näihin tiloihin on järjestetty yleisten tietoturvallisuusohjeiden mukaisesti.

Yhtymän ulkopuolisten tahojen konsultointisopimuksiin sekä esimerkiksi laitteiston- ja ohjelmistontoimittajia varten laadittaviin hankintasopimuksiin kirjataan tietoturvasitoumus.

Sosiaali- ja terveysministeriön asetuksessa potilasasiakirjoista ohjeistetaan, että toiselta palvelujen tuottajalta palvelujen hankinnassa on sovittava kirjallisella sopimuksella potilasasiakirjatietojen rekisterinpitoon ja tietojen käsittelyyn liittyvistä tehtävistä ja vastuusta sekä varmistua siitä, että potilasasiakirjoihin sisältyvien tietojen salassapitoa ja vaitiolovelvollisuutta koskevia säännöksiä noudatetaan. Toiminnassa syntyneistä potilasasiakirjoista tulee ilmetä palvelun hankinnan tapa sekä palvelun tilaaja, tuottaja ja toteuttaja. (Sosiaali- ja terveysministeriön asetus potilasasiakirjoista 298/2009, 5 §.)

5.5.1 Tietojen turvallinen käsittely

Tietojärjestelmäpalveluiden toimesta turvataan toiminnalle tärkeiden tietojärjestelmien ja tietoverkkojen keskeytymätön toiminta, estetään tietojen ja tietojärjestelmien joutuminen vääriin käsiin, valtuudeton käyttö, tahaton tai tahallinen tiedon tuhoutuminen tai vääristyminen. Lisäksi varaudutaan normaaliajan toiminnan tietojenkäsittelyn turvaamisen lisäksi toiminnan keskeytyksiin ja niistä toipumiseen. (Päijät-Hämeen sosiaali- ja terveydenhuollon kuntayhtymän sivut, 2009)

Tietojen suojaamisvelvoite koskee sekä manuaalisia että sähköisesti ylläpidettäviä rekistereitä. Paperisen ja sähköisen tietosuojatun materiaalin hävittäminen tapahtuu lain säätämien määräaikojen mukaisesti.

Tietojen ja tietojärjestelmien vastuuhenkilöt on nimetty rekisteriselosteessa ja tietojärjestelmäselosteessa. Tietojärjestelmissä ylläpidettävien järjestelmien käytön tulee perustua henkilökohtaisiin käyttäjätunnuksiin ja salasanoihin niin, että jälkikäteen käyttäjät ovat todennettavissa. (Päijät-Hämeen sosiaali- ja terveydenhuollon kuntayhtymän sivut, 2009)

5.5.2 Toiminnan jatkuvuus ja riskienhallinta

Yhtymässä tehtiin tietoturvallisuuden riskikartoitus syksyllä 2008. Tämän tutkimustyön osana teimme tietoturvallisuuden riskikartoitusta keskussairaalan osalta kuvantamisessa kyselytutkimuksella ja pistokokeilla alueen toimipisteisiin.

Kuvantamisessa on laadittu toimintakäsikirjaan toimintaohjeita toiminnan jatkuvuuden varmistamiseksi häiriötilanteissa kuvankäsittelyn, tallennuksen ja potilashallintoa koskien. Toimintaohjeiden sisältönä ovat toimiminen normaalioloissa, poikkeusoloissa, kriisin tai onnettomuuden sattuessa tai katastrofitilanteessa. Potilasturvallisuuden säilyttäminen kaikenlaisissa tilanteissa on ensiarvoisen tärkeää. Auditointi suoritettiin 2003. (Radiologian toimintakäsikirja, 2009)

Organisaation tehtävänä on luokitella tietojärjestelmät kriittisyyden mukaan. Jokaisen tietojärjestelmän osalta laaditaan toimintasuunnitelma järjestelmään kohdistuvan häiriön todennäköisen keston ylittäessä suurimman sallitun keskeytysajan. Suunnitelma ja sen testaus ovat järjestelmän omistajan vastuulla. Aineiston laatija vastaa tietoaineiston luokittelusta, ellei lainsäädäntö muuta vaadi. Jokaisella tietojärjestelmällä tai sen osalla on oltava yksikäsitteinen omistaja tai haltija. Tietoturvallisuuden toteuttamista ohjaavat dokumentit ovat vahvistettuja ja asianomaisten kohderyhmien saatavilla. (Sisäasiainministeriö, poliisiosasto, määräys SMDnro/2008/353., Päijät-Hämeen sosiaali- ja terveydenhuollon kuntayhtymän sivut, 2009)

5.5.3 Tietoturvallisuusasioista tiedottaminen

Tiedottamisvastuu, koskien myös tietoturvallisuusasioita, kuuluu yhtymän toiminnasta vastuussa oleville tahoille, yhtymän johtajalle ja yhtymän tulosryhmien johtajille. Tietosuoja-asioihin liittyvässä tiedottamisessa rekisterinpitäjä on ensisijaisesti yhteydessä tietosuojavastaavaan. Yhtymän tietoturvallisuuspolitiikka on julkisesti kaikille luettavana internetsivustoilla. (Päijät-Hämeen sosiaali- ja terveydenhuollon kuntayhtymän sivut, 2009).

6 TUTKIMUS JA TUOTOS

6.1 Tutkimusmenetelmät

Tämä opinnäytetyö on toteutettu kvalitatiiviseen tutkimusmenetelmään pohjautuen toiminnallisena tutkimuksena. Kvalitatiiviseen tutkimusmetodologiaan kuuluu yhtenä strategialajina toimintatutkimus. Kyselytutkimuksella koko kuvantamisen tulosalueen henkilöstölle on kartoitettu ja saatu tutkittavaksi henkilöstön nykytiedon tasoa tietoturvaa ja – suojaa koskien. Kyselytutkimuksen analysoinnin jälkeen tarkennetaan kyselyn perusteella heränneitä mielenkiintoisia seikkoja kohdistetun haastattelun keinoin. Haastattelut ovat toteutettu pääosin havainnointikäyntien yhteydessä. (Vilkka 2007, 44).

Tutkijat osallistuvat tutkimuskohteen toimintaan havainnoimalla yleisiä toimintatapoja, käyttämällä osallistuvaa havainnointia (sisällä toiminnassa havainnointi). Kohdistetussa havainnoinnissa havainnoitsijan osallistuessa päivittäisiin toimintoihin hän kohdistaa havainnointiaan tapahtumiin, tilanteisiin ja asioihin käytännön toiminnassa. Tutkimuskohteen jäsenten tarkkailulla pyritään vielä osallistuvan ja tarkkailevan havainnoinnin keinoin seuraamaan, kuinka nämä noudattavat sitä normia ja ihannetta, jonka ovat tuoneet esiin kyselytutkimuksessa ja haastattelussa. (Vilkka 2007, 45 - 45)

Osallistuva havainnointi onnistuu Vilkan mukaan siksi, että työskentely tapahtuu tutkittavan organisaation sisällä, joten toimintatapojen tunteminen ja yhteisen kielen olemassaolo edesauttavat tutkimuksen suorittamista. Organisaatiokulttuuri, totutut käytänteet ja toimintatavat saattavat olla myös haittaavia tekijöitä, voidaan sortua liian objektiiviseen ja yksipuoliseen havainnointiin, koska toiminta on niin tuttua. (Vilkka 2007, 45).

Tutkimuksen kuluessa pääsimme osallistumaan tietosuojan ja tietoturvan ohjaus- ja kehittämisryhmän kokouksiin seuraamaan yhtymän tietoturva- ja tietosuojaoh-

jeistuksen esivalmisteluja ja kuulemaan ajankohtaisista asioista. Kokouksissa pohdittiin erilaisia ongelmia, kuten luetaanko ohjeita, riittävätkö yhdet yhteiset ohjeet kaikille vai tarvitaanko erilaisia täsmennettyjä ohjeita eri toimiympäristöille.

Laadullinen tutkimus eli kvalitatiivinen tutkimus on tutkijan omaan intuitioon, tulkintaan, järkeilykykyyn, yhdistämis- ja luokittamisvalmiuksiin perustuvaa. Päätelmiä voidaan tehdä monella tavoin, ne voivat jopa olla ristiriitaisia samasta aineistosta tutkittuna. Kvalitatiivinen tutkimusote soveltuu tutkimukseen, kun ollaan kiinnostuneita tapahtumien yksityiskohtaisista rakenteista, tietyissä tapahtumissa mukana olleiden yksittäisten toimijoiden merkitysrakenteista, sellaisten luonnollisten tilanteiden tutkimuksessa, joita ei voida järjestää kokeeksi tai joissa ei voida kontrolloida läheskään kaikkia vaikuttavia tekijöitä tai halutaan saada tietoa sellaisista tapauksiin liittyvistä syy-seuraussuhteista, joita ei voida tutkia kokeen avulla. (Metsämuuronen 2000, 8, 14)

Tapaustutkimus tutkii monipuolisia ja monilla tavoilla hankittuja tietoja käyttäen tapahtumaa tai toimivaa ihmistä tietyssä ympäristössä, voi olla arkipäivän tapahtuma. Yin (1983) on sitä mieltä, että pyrkimyksenä on ymmärtää ilmiötä entistä syvällisemmin. Tapaustutkimuksessa sosiaalisten totuuksien monimutkaisuus ja sisäkkäisyys tarjoavat vaihtoehtoisten tulkintojen tukea, joita voidaan käyttää erilaisten tulkintojen pohjana. Eli tästä näkökulmasta katsoen, vaikka kuvantamisen toiminta perustuu lakeihin ja normeihin, on käytännön työssä usein toimittava sen mukaan kuin tapaus, sen kiireellisyys tai asioiden järjellinen hoitaminen vaatii. Tiedon on oltava käytettävissä mahdollisimman nopeasti, oikeassa muodossa niillä toimijoilla jotka sitä tarvitsevat. Tapaustutkimus voidaan ymmärtää keskeiseksi kvalitatiivisen metodologian strategiaksi, eli lähes kaikki kvalitatiivinen tutkimus on tapaustutkimusta. (Metsämuuronen 2000, 18)

Symbolisen interaktionismin mukaan kulttuuri muovaa ihmisen käyttäytymistä. Inhimillinen käyttäytyminen on luovaa, tietoisen ja tiedostamattoman päätöksenteon seurausta. Käyttäytymisen päätöksenteko perustuu sosiaalisessa vuorovaiku-

tuksessa syntyneille tulkinnoille. Sen kannalta on oleellista huomioida tutkittavien tilanteiden tulkitsemistavat, koska toiminta ohjautuu tulkinnan kautta. (Metsämuuronen 2000, 19).

Hirsjärvi ja Hurmeen (1985) mukaan haastattelun lajit on jaettu tiedonhankinnallisiin ja terapeuttisiin. Tiedonhankintahaastattelut tähtäävät informaation keräämiseen. Ne jaetaan käytännön haastatteluun, joka tähtää käytännön ongelman ratkaisemiseen ja tutkimushaastatteluun, joka tähtää systemaattiseen tiedon hankintaan. (Metsämuuronen 2000, 39, Hirsjärvi & Hurme 1985, 26)

6.2 Kyselytutkimus

6.2.1 Taustaa ja tavoite

Yhtymän organisaatio on tehnyt kattavia ohjeiden uudistuksia sekä strategialinjauksien päivityksiä viimeisen kahden vuoden aikana tietoturvan- ja tietosuojan alueella. Keväällä -09 julkaistiin tietoturvapolitiikka, ja parhaillaan on työn alla koko taloa koskevat tietosuoja- ja tietoturvaohjeet. Yhteisten ohjeiden koskiessa noin 3700 henkilöä eri tulosryhmistä, tulosalueemme esimiehiä kiinnosti, kuinka ohjeet voitaisiin mitoittaa erityisesti kuvantamisen tulosalueelle huomioiden alueen erityispiirteet.

Toimeksiantajan tarpeesta ja saadaksemme pohjatietoa tutkimukselle teimme kvalitatiivisen kyselytutkimuksen tulosalueen koko 68 hengen henkilöstölle. Kyselyn tavoitteena oli selvittää kuvantamisen tulosalueen henkilökunnan tietoja tietoturva- ja tietosuoja-asioissa, sekä heidän asenteitaan niihin. Toivoimme myös saavamme henkilökunnalta vihjeitä, miten näitä asioita tulisi viedä eteenpäin. Olisiko esimerkiksi perehdytys, koulutus, minkälainen koulutus, sairaalan sisäinen infokanava, jne. tehokkain tapa jalkauttaa tietoa. Tavoitteena oli myös kartoittaa henkilökunnan havaitsemia puutteita tietoturva-asioissa sekä heidän parannusehdotuksiaan ja realistisia toimenpide-ehdotuksia konkreettisiin kehittämiskohteisiin, joita yksikössä voitaisiin resurssien puitteissa toteuttaa tietoturvan ja -suojan pa-

rantamiseksi, eli löytää toteuttamiskelpoisia käytännön toimintamalleja työolojen kehittämiseksi.

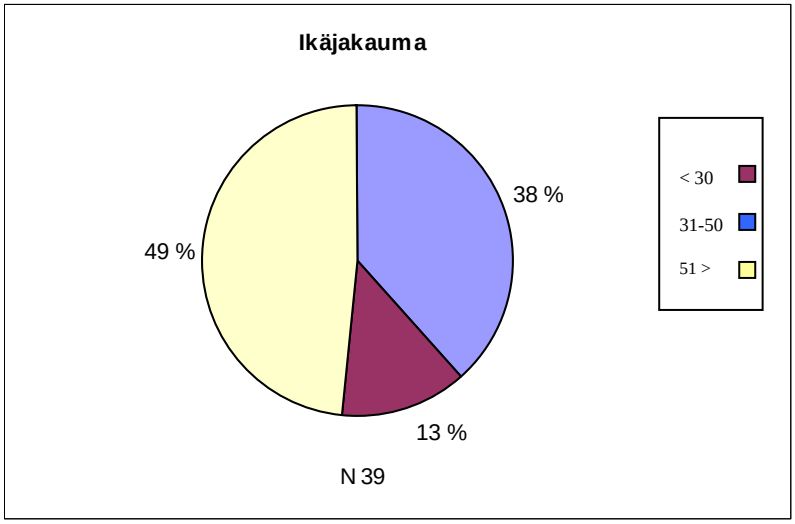
6.3 Kyselyn kulku ja analysointi

Webropolilla tehdyn kyselyn lähetimme koko kuvantamisen henkilökunnalle (68), vastausaikaa oli kaksi viikkoa. Saimme vastauksia 39 henkilöltä määräaikaan mennessä, joten vastausprosentiksi tuli 57 %. Vastausprosentin oltua lähes 60 % ja kaikkien ammattiryhmien osallistuttua kyselyyn, pidämme kyselytutkimuksen tuottaman tuloksen reliabiliteettia hyvänä. Saimme hyvän ja kattavan analysoitavan materiaalin. Tutkimuksesta palautteena tulemme tekemään PowerPoint esityksen kokoamistamme tutkimuksen tuloksista henkilökunnalle osastokokoukseen.

Kyselyn rakenteen suunnittelimme siten, että aluksi kartoitimme muutamia taustatietoja. Kysyimme ikää, ensisijaista työskentelypaikkaa, ammattiryhmää ja työskentelyaikaa nykyisen työnantajan palveluksessa.

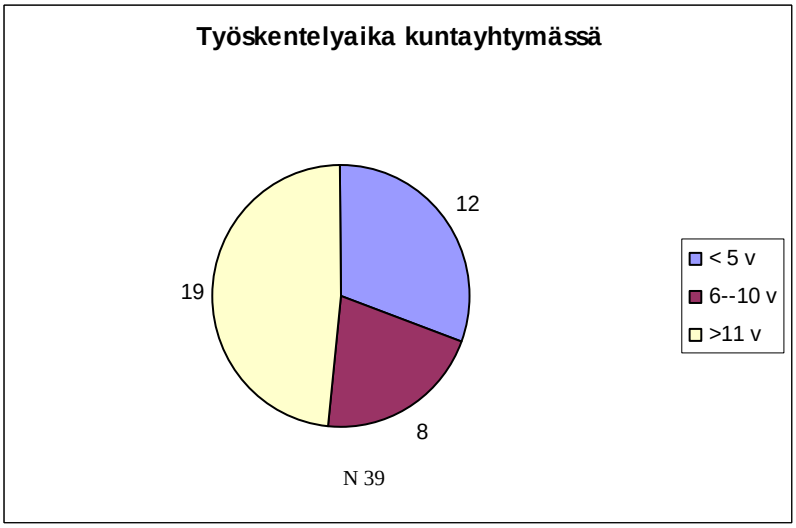
Ensimmäisessä kysymyksessä paikallistimme vastaajat. Ensisijaisena työskentelypaikkana suurimmalla osalla henkilökunnasta on keskussairaala. Alueen toimipisteissä työskenteleviä oli yhteensä 8 vastaajaa.

Ammattiryhmittäin vastaajat jakaantuivat siten, että lääkäreistä 2/3, hoitajista 3/4 ja muusta henkilöstöstä hieman alle puolet vastasi. Tutkimuksemme luotettavuuden näkökulmasta moniammatillisen työyhteisön kaikkien ammattiryhmien osallistuminen vastauksillaan kyselyyn oli positiivinen piirre.



Kuvio 5: Vastauksensa palauttaneen henkilöstön ikäjakauma

Henkilöstön ikärakenne vastaa hyvin yllä olevasta kuviosta 5 näkyvää tutkimukseen vastanneiden ikäjakaumaa.



Kuvio 6: Päijät-Hämeen sosiaali- ja terveydenhuollon kuntayhtymässä työskentelyajasta

Kuten edellä olevasta kuviosta 6 näkyy, vastanneista suurin osa on työskennellyt yhtymän palveluksessa yli 11 vuotta, alle kuusi vuotta työskentelyajakseen ilmoitti 12 vastaajaa. Kahdeksan vastaajaa oli työskennellyt 6 – 10 vuotta.

Kysymyksessä viisi halusimme selvittää perehdytysasioita, koskien muun muassa henkilötietojen salassapitoa, tietojen suojaamista sekä yksityisyyden loukkaamattomuutta.

Alueen toimipisteiden kahdeksasta vastaajasta neljä ilmoitti perehdytyspaikakseen nykyisen työpaikkansa. Yksi ei ollut saanut ollenkaan perehdytystä ja kolme oli aikaisemmissa työsuhteissa. Radiologiassa työskentelevistä 19 oli perehdytetty tietoturva- ja tietosuoja-asioihin yhtymässä, kolme aikaisemmissa työsuhteissa, kuusi henkilöä ei katsonut saaneensa lainkaan tietoturva- ja tietosuojaperehdytystä ja kahden perehdytys oli tapahtunut ulkopuolisissa koulutuksissa.

Keskussairaalan radiologiassa henkilökunnan perehdyttäminen näyttää näiden vastausten mukaan jääneen suhteessa henkilökunnan määrään vähemmälle kuin alueen henkilökunnan. Tämän tuloksen mukaan radiologian henkilökunnalle voisi järjestää perehdytystä tietoturva-asioissa.

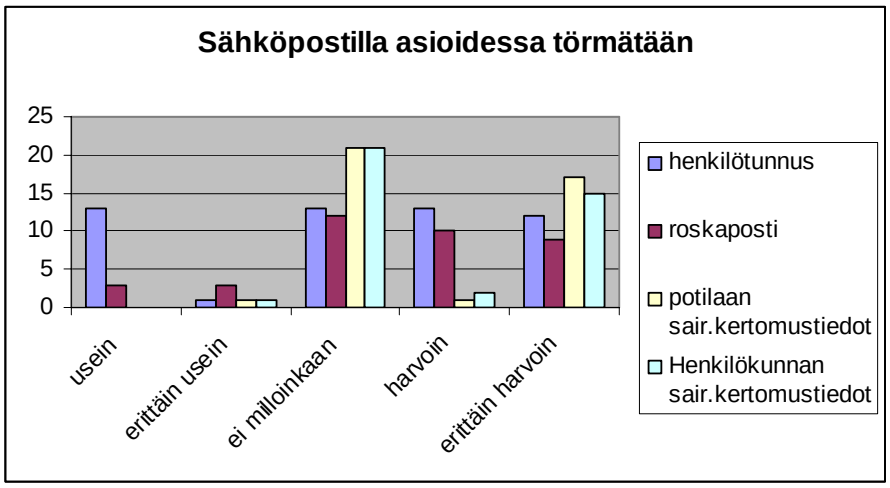
Tutkimme työsuhteen keston ja tietoturva- ja tietosuojaperehdytyksen saaneiden suhdetta. Alle viiden vuoden työsuhteessa olleista suurin osa oli perehdytetty yhtymässä. Yli 11 vuotta työskennelleistä perehdytys oli jäänyt vastaajien mukaan saamatta kokonaan kuudelta henkilöltä. Tämä osoittaa, että perehdytykseen on panostettu viime aikoina työsuhteen aloittaneisiin enemmän kuin aikaisempina vuosina.

Kysymyksessä kuusi halusimme selvittää oliko henkilökunnalla selvillä minkä tai keiden suojaamiseksi tietosuoja- ja tietoturvaohjeistus on. Lähes kaikki olivat ymmärtäneet, että ohjeistus on tarkoitettu kaikkien suojaksi, eli henkilökunnan, asiakkaiden ja organisaation suojaksi. Kahdeksan henkilön mielestä ohjeistus suojasi pelkästään asiakkaita.

Kysely on tehty samoihin aikoihin kun tulosalueella päädyttiin vaihtamaan salasana kolmen kuukauden välein järjestelmän toimesta, joten osa varmaankin on vastannut kysymykseen jo ennakoiden tätä käytäntöä. 14 vastaajaa ei ollut vaihtanut koskaan aiemmin salasanaansa.

Tietoturvapolitiikkaan tutustumista koskevaan kysymykseen liitimme linkin josta voi suoraan siirtyä tutustumaan ko. tietoturvapolitiikkaan. Linkistä huolimatta 25 vastaajaa ilmoitti, ettei ollut tutustunut siihen. Se voisi kuvata kiinnostuksen tasoa.

Päivittäin suurin osa vastaajista käyttää sähköpostia työasioihin, vain neljä käyttää tuskin lainkaan. Henkilöstön sähköisen asioinnin vuoksi jokaisella on oltava sähköpostiosoite, jotta pystyy hoitamaan henkilöstöasiansa sähköisesti.



Kuvio 7: Tietosuojatun materiaalin esiintyminen sähköpostissa, N 39

Siitä huolimatta ettei henkilötunnuksia eikä muitakaan potilastietoja saisi lähettää sähköpostin välityksellä, tietosuojattua tietoa kuitenkin vastaanotetaan sähköpostin välityksellä.

Seuraavaksi kartoitimme henkilökunnan tietoisuutta tietoturvan ja tietosuojan esiintymisestä arkipäivän toiminnoissa. Hieman yli puolet vastaajista tunnisti käytännön työssä tietoturvan esiintymisen jossain määrin, loput tunnistivat suuressa määrin. Kaikki vastaajat siis tiedostivat tietoturvan ja – suojan liittyvän jokapäiväiseen työhön. Tämä osoittaa, että turvaseikkoja tunnistetaan työssä.

Esiin nousivat salasanat, salassapito- ja vaitiolovelvollisuus, potilas- ja henkilötietojen käsittely, papereiden lajittelu ja kuvien arkistointi. Kuvien siirtojen yhteyteen liittyvät lupakäytännöt, potilastyö ja kahvipöytä- ynnä muut keskustelut esiintyivät havainnoissa.

Yli puolet vastanneista, 67,4 %, ei ollut huomannut mitään puutteita tai virheitä edellä mainituissa toiminnoissa. Yhteistunnukset arveluttivat 43,6 %:ia. Kuitenkin osa vastaajista arveli, ettei asialle ole mitään tehtävissä, koska kirjautumistoimet hidastaisivat liikaa työnkulkua. Ratkaisuksi ehdotettiin tunnistusmenettelyjen nopeuttamista. Tällöin voisi lyhyemmän poistumisen ajaksi kirjautua ulos järjestelmästä.

Potilaspaperit, puhelinkäyttäytyminen, henkilökunnan tiedot, silloin kun hän on potilaan roolissa ja työympäristön avoimet tilat olivat myös huolena. Epäiltiin yhtymän kirjekuorien riittävää turvallisuuden tasoa.

> *”Oma asenne ja yleinen välinpitämättömyys ovat tietosuojariskejä. Lapsellinen luottamus siihen, ettei kukaan käytä omia tunnuksia väärin. Henkilötietojen suojaus tulee muistaa kaikessa toiminnassa. Jokaisen oma asenne/suhtautuminen tulisi saada sellaiseksi, että itse kukin huolehtisi omalta osaltaan tietoturvan ja -suojan toteutumisesta*.”

Kysyttäessä tehokkainta kanavaa tietoturva- ja tietosuojaohjeistuksen saamiseksi toivottiin koulutusta käytännössä. Toivottiin myös mahdollisuutta osallistua koulutukseen. Uuden työntekijän perehdyttämisen yhteydessä pidettiin tärkeänä muistuttaa tietosuoja- ja tietoturvaohjeista. Sähköpostia pidettiin myös tehokkaimpana muotona. Haluttiin lyhyitä yksinkertaisia ohjeita. Myös infokanavaa pidettiin tehokkaana tiedotuskanavana.

> *”Pitkät ja kuivat sepustukset jäävät usein lukematta.”*

Asiantuntijoiden luentoja toivottiin osastokokouksissa tai yhteisissä palavereissa. Lyhyet infotilaisuudet esimerkiksi pari kertaa vuodessa yleisesti koko henkilökunnalle. Infotilaisuuksien pitäjiksi ehdotettiin esimiestä, tietoturvahenkilöitä, tietoturvayksikköä sekä ATK-yhdyshenkilöitä. Näistä vastauksista päätellen koulutushalukkuutta ja tarvetta henkilöstöllä olisi.

Kolme vastaajaa ei mielestään tarvitse, ei halua, eikä kaipaa ohjeistuksia. Kaikista tietoturva- ja tietosuojaseikoista toivottiin kertausta ja perusasioista muistuttamista, jotta osattaisiin opettaa uusille työntekijöille kaikki huomioitavat asiat oikein. Yleisiä tietoturva-ohjeita käytännön työhön kaivattiin, esimerkiksi tietoa salasanan vaihtoajoista ja niin edelleen.

> *”Jos työhön liittyvien järjestelmien/ohjelmien käyttö ei käytännön työssä onnistu tietoturvaohjeita tarkasti noudattaen (hidastamatta /hankaloittamatta työn suorittamista), pitäisi siitä saada tieto/lupa esimiehelle/tietoturvavastaavalle tms. työntekijöiden suojelemiseksi.”*

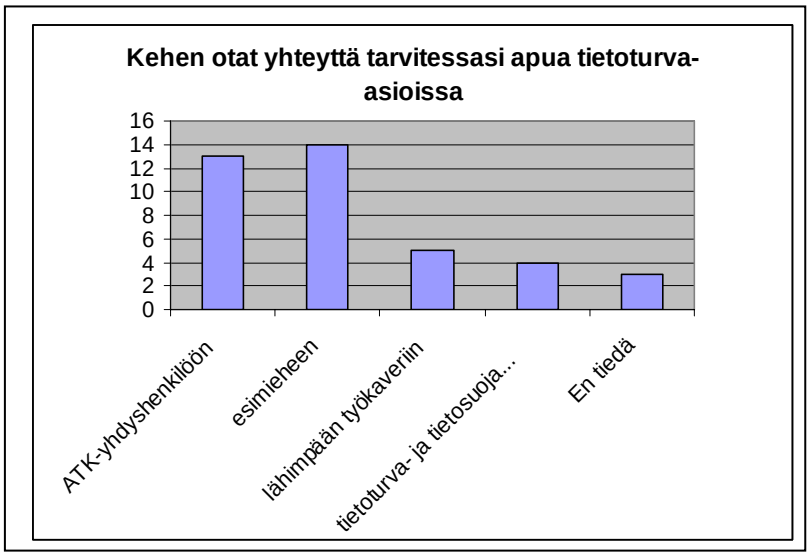
Toivottiin, että ohjeet ja rajoitukset eivät haittaisi potilaan turvallista ja tehokasta hoitoa.

> *”Toivoisin ainakin potilaana, että kaikki olennainen tieto olisi käytettävissä hoitamiseeni, ja sitä käytettäisiin vain minua suojaavalla tavalla.”*

> *”Pitää käyttää ihan omia aivoja, mikä sopii ja mikä ei. Tähän pätee vähän sama kuin muuhunkin toimintaan että ohjeista olisi enemmän apua kuin haittaa. Asiat voi tehdä todella hankalaksi jos intoillaan liikaa ja sitten turhautuvat oikeiden asioiden hoitajat. Nykyinen ruksi potilaan luvasta pitäisi riittää.”*

Omaa työtä koskevia kirjallisia, selkeitä, yksiselitteisiä, käytännönläheisiä, päivitettyjä ja yhtenäisiä ohjeita eri työpisteisiin kaivattiin. Selkeän, yksinkertaisen ohjeistuksen lisäksi toivottiin ammatillista tietojenkäsittelyä, omaatuntoa sekä

oikeaa asennetta siihen miten ja mihin tietoja käytetään, sekä tietoturvasta jatkuvaa informointia kaikilla kanavilla. Tästä saimme vahvistusta ohjeiden laatimisen tarpeelle.



Kuvio 8: Keneen otetaan yhteyttä tietosuoja-asioissa, N 39

Kuten kuviosta 8 on nähtävissä, esimies ja ATK-yhdyshenkilö ovat ensisijaiset yhteydenottokanavat. Yhteneväistä mielipidettä ei näytä olevan, joku ilmoitti ottavansa kaikkiin neljään ensimmäiseen vaihtoehtoon yhteyden tarvittaessa.

Kokonaisuudessaan vastausten perusteella huomasimme, että koulutusta ja opastusta sekä lyhyitä, yksinkertaisia työläheisiä ohjeita kaivataan. Useasta vastauksesta nousi esiin, että henkilöstö on tiedostanut tietoturvallisuuden olevan asenne. Kyselyn aihe koettiin tarpeelliseksi.

Teknisesti ohjelmoimme kyselyn siten, että jokaiseen kysymykseen oli pakko vastata, joten kysymyksissä ei päässyt eteenpäin ennen kuin oli tehnyt jonkinlaisen merkin joka kohtaan. Tämä saattoi olla kiireisen työn ja henkilökuntavajeen lisäksi syynä siihen, että kyselyyn saimme niin pienen vastausmäärän. Pidämme vastausmäärää riittävänä voidaksemme tulkita kyselytutkimuksen tuloksen luotettavaksi. Metsämuurosen mukaan johtopäätösten tekeminen on salapoliisin työtä, johon mielipiteeseen yhdymme täysin. (Metsämuuronen 2000, 67)

6.4 Havainnointi

Osallistuvan havainnoinnin metodiin päädyimme**,** koska molemmat tutkijat työskentelevät saman organisaation sisällä ja lisäksi toinen työskentelee tutkittavalla kuvantamisen tulosalueella, ja hän pystyi olemaan myös toimijan roolissa. Organisaation sisällä työskennellessä tutkimuksen kohteen koodisto, kieli ja toiminnot ovat tuttuja, joten kulttuurin omista lähtökohdista käsin tilanteen tarkkailu on mahdollista (Metsämuuronen 2000, 45). Työmme on toimintatutkimus jossa käytetään yhtenä tutkimusmenetelmänä osallistuvaa havainnointia. Tutkimuksen aikana esille tulleet epäkohdat herättivät keskustelua ja toimenpiteitä työyhteisössä.

Havainnointitutkimustamme suoritimme seuraamalla toimintaa normaaleissa, päivittäisissä tilanteissa ja pistokokeilla toimipisteisiin. Kyselytutkimusten antamien tulosten perusteella päädyimme tarkkailemaan kohdistetusti henkilöstön toimintaa järjestelmiin sisään- ja uloskirjautumisissa, päätteiden ja laitteiden sijoittelua, aukioloa, lukituksia ja henkilökunnan toimintaa asiakaskontakteissa. Havainnoilla saimme vahvistuksen haastattelujen ja kyselytutkimuksen antamaan informaatioon.

Havaintotutkimuksen vahvistukseksi pääsimme osallistumaan yhtymän tietosuojan ja tietoturvan ohjaus- ja kehittämisryhmän kokouksiin. Seurasimme tietoturva- ja tietosuojaohjeistuksen esivalmisteluja ja ajankohtaisia ja tulevia tietoturvaan liittyviä asioita kuten jo aiemmin olemme maininneet.

Havainnointikierrosten ja pistokokeiden yhteydessä teimme muutamia spontaaneja haastatteluja. Sähköisen asioinnin koetaan helpottaneen työntekoa kaikissa toimipisteissä, esimerkiksi tiedon siirron nopeutumisessa. Henkilökohtaisesti tietoturvaan ja tietosuojaan vaikuttaminen tapahtuu haastateltavien mukaan oikealla asenteella ja vastuullisuudella, esimerkiksi siten, ettei samanaikaisesti asioi asiakkaan kanssa ja puhu puhelimessa.

Yhden havainnointikierroksen teimme päivystysaikana keskussairaalan radiologian osastolla. Tarkastelimme työpisteiden fyysistä turvallisuutta ja toimintatapoja. Kuvantamiseen pääsevät päivystysaikana vain kulkuluvan omaavat henkilöt.

Haastattelemiemme röntgenhoitajien mukaan päätteiden aukiolo on välttämätöntä päivystystapauksien kiireellisyyden vuoksi. Päätteiden avaaminen ja järjestelmään sisäänkirjaus vie kohtuuttomasti aikaa. Työympäristö on fyysisesti lukitussa tilassa.

Potilaskuljetuksissa sähköiset järjestelmät ovat parantaneet potilaan tietosuojaa kuljetustilanteissa. Syynä tähän on potilasasiakirjojen ja röntgenkuvien kuljettamisen vähentyminen asiakkaan mukana.

6.5 Ohjeet

Sosiaali- ja terveysministeriön asetuksen 3§. mukaan terveydenhuollon toimintayksikön terveydenhuollosta vastaavan johtajan rekisterinpitäjän edustajana vastuulla on huolehtia siitä, että toimintayksikössä on kirjalliset ohjeet potilasasiakirjoihin sisältyvien tietojen käsittelystä ja menettelytavoista (STM asetus 2001, 3 §.). Myös sähköisestä asioinnista käytännössä on vastuu toimintayksikön vastaavalla johtajalla. (Pajukoski 2004, 79)

Viranomaisen velvollisuus hyvään tiedonhallintatapaan edellyttää huolehtimista siitä, että viranomaisen palveluksessa olevilla on tarvittava tieto sekä käsiteltävien asiakirjojen julkisuudesta että tietojen antamisesta. On huolehdittava tietojen, asiakirjojen ja tietojärjestelmien suojaamismenettelyjen noudattamistapojen tiedottamisesta henkilöstölle. Henkilöstöllä on oltava tiedot tietoturvallisuusjärjestelyistä ja -tehtävänjaosta. Lisäksi hyvän tiedonhallintatavan toteuttamiseksi annettujen säännösten, määräysten ja ohjeiden noudattamista valvotaan. Joten henkilöstölle on laadittava ohjeistukset näiden velvollisuuksien täyttymiseksi. (Julkisuuslaki 18 §., Pajukoski 2004, 79)

Muun muassa yllämainituista syistä ja valmisteluna myös tulevaan auditointiin saimme opinnäytetyönä tehtäväksi tietoturva- ja tietosuojaohjeiden laatimisen kuvantamisen tulosalueelle. Lisäksi työhömme ehdotettiin lisänä ohjeiden jalkauttamissuunnitelman laatimista.

Ohjeiden laatimisen pohjatyönä kysyimme tutkimuksessamme henkilökunnalta, miten he katsoisivat ohjeiden käytäntöön saattamisen sujuvan tehokkaimmin työn lomassa. Vastauksissa toivottiin koulutusta, tiedottamista, perehdyttämistä ja selkeitä ohjeita. Näiden vihjeiden perusteella laadimme lyhyehköt ohjeet ja alustavan toimeenpanosuunnitelman.

Liian ylimalkaisten ohjeistusten laatiminen voi johtaa omiin tulkintaratkaisuihin, koska sisältö voidaan sisäistää helposti eri tavoin. Tarkkojen helposti tulkittavien ohjeistusten mukaan toimiessa voidaan välttää ristiriitaisia tulkintatapoja ja pystytään toimimaan yhtenäisesti, joten on tärkeää saada laadittua helposti omaksuttavat ohjeistukset. (Koskinen 2009)

Toimeksiantonamme oli laatia kuvantamisen toimintaan sopeutetut tietoturva- ja tietosuojaa koskevat ohjeet. Aloitimme ohjeiden teon tutustumalla lakeihin ja asetuksiin sekä tietosuojavaltuutetun toimiston sivuihin. Tietosuojavaltuutetun mukaan viranomaisten omaan toimintaan sopeutettuja käytännesääntöjä voidaan laatia.

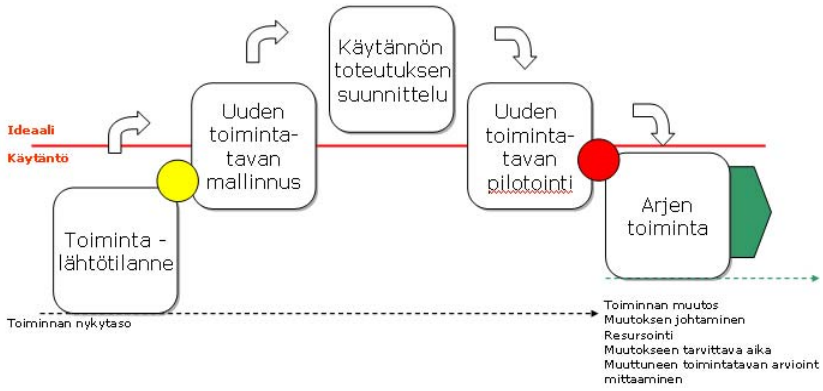
Kyselytutkimuksen, havainnoinnin ja haastattelujen pohjalta kartoitimme kuvantamisen erityistarpeita. Ohjeistus yhtenäistettiin yhtymän yleisten tietoturva- ja tietosuojaohjeiden kanssa huomioiden kuvantamisen toiminnan erityisvaatimuksia. Laatimamme ohjeet tarkistetaan, muokataan ja hyväksytetään organisaatiossa ennen niiden käyttöönottoa.

6.6 Toimeenpano- eli jalkauttamissuunnitelma

Jalkauttamisen hyvä suunnittelu huolellisesti panostaen henkilöstön koulutustarpeisiin, koulutukseen ja resursointiin, antaa paremmat mahdollisuudet saada henkilöstö sitoutettua uusiin toimintatapoihin ja näin noudattamaan niitä. Selkeä tiedottaminen auttaa parantamaan uusien ohjeistusten noudattamista ja motivoi henkilöstöä. (Koskinen 2009)

Toimeenpanosuunnitelmaa laadittaessa pohditaan tutkittavan ympäristön kokonaisuutta. On pyrittävä hahmottamaan kehittämiskohde, joka on tässä tapauksessa kuvantamisen tietoturvallinen ja tietosuojattu toiminta kokonaisuudessaan. Kokonaisuuden hahmottaminen koostuu lähtökohdista, taustatekijöistä, odotettavissa olevista mahdollisista tuloksista, toteutuksesta ja toimenpiteistä, koottavasta tietoaineksesta sekä kokonaisuuden arvioinnista. (Hallikainen & Hälikkä 2009)

Löysimme kuvion (Anttila, 2007) realistisesta evaluaation (tapauskohtaisesti arvioiva) mallista. Teimme liitteenä 2 olevan mukaellun kuvan, joka auttoi oman työmme hahmottamisessa, erityisesti toimeenpanosuunnitelman laatimisen suunnittelussa.



Kuvio 9. Jalkauttamisen mallinnuskuva (Hallikainen & Hälikkä 2009)

Yllä olevasta kuvasta saimme hyvää tietoa ja auttoi meitä jalkauttamisen suunnittelussa. Malli voisi olla soveltamiskelpoinen myös terveydenhuollon toimintaympäristössä.

Jalkauttamissuunnitelman tarkoituksena on antaa vinkkejä tietoturva- ja tietosuojaohjeistuksen muuttamiseksi arjen toiminnaksi. Sähköistyneessä työskentelympäristössä tarvitaan ja saadaan ohjeita jatkuvasti. Ohjeet muuttuvat nopeasti muutokset ovat voimakkaita, henkilökunta väsyy ja muutosvastarinta lisääntyy. Tämän vuoksi ohjeistuksen saattaminen osaksi käytännön työtä on haasteellista. (Sampo 2009)

Lähtötilanteen kartoittaminen tapahtui osallistuvan havainnoinnin ja kyselytutkimuksen avulla. Selvitimme toiminnan nykytilaa henkilöstön käytännön työn tietoturva- ja tietosuojan toiminnoissa. Tutkimusten tulosten perusteella hahmottelimme rungon toimeenpanosuunnitelmalle, joka toimii pohjana käytännön toteutuksen suunnittelussa. Käytettävissämme olevan ajan rajallisuuden vuoksi joudumme jättämään suunnitelman käytäntöön saattamisen ja toteuttamisen organisaatiolle. (Hallikainen & Hälikkä 2009)

Laatimamme ohjeistuksen toteuttamissuunnitelman käyttöönoton saattamisen omaan ympäristöömme jätämme kehittämistyöksi. Vastuun jalkauttamissuunnitelmamme antamien vinkkien käytäntöön saattamisen onnistumisesta siirrämme myös mahdollisille toteuttajille. Yhdessä suunnitellen ja päättäen vahvistuvat onnistumisen mahdollisuudet. (Koskinen 2009)

Ideaalitilanteena olisi saada henkilökunnan asenteet, sitoutuneisuus ja toiminta suuntautumaan kohti käytännön toiminnan tietoturvaohjeiden noudattamista. Ohjeiden jalkauttamisen ongelmana ovat tämän hetkinen käytännön ja ideaalitilanteen yhteensovittaminen. Tämä on sujuvan ja potilasturvallisen työn mahdollistamiseksi haasteellista. (Hallikainen & Hälikkä 2009)

Jalkauttamisen onnistumiseen ei vaikuta suunnitelman sisällön laajuus, vaan miten onnistuneesti yhteisön jäsenet ovat sen sisäistäneet. Jokaisen on pohdittava omaa osuuttaan ja panostaan suunnitelman onnistumiseen. Työyhteisön jäsenten tulee ymmärtää tiedon siirtämisen merkitys ja heidät tulee valmentaa tapahtuviin muutoksiin, jotta he osaisivat reagoida ja pystyisivät mukautumaan niihin. Kaikkien toimiessa sovitusti suunnitelma alkaa toteutua ja päämäärä lähestyy. Sovittuja ohjeita noudattamalla joudutaan etsimään uudenlaisia toimintatapoja tai ratkaisuja, koska niihin ei aikaisemmin ole ollut valmiita käytäntöjä. (Koskinen 2009)

Ohjeistusten jalkauttaminen, saattaminen arkipäivän toimintaan saattaa olla kriittisin vaihe ohjeistuksen prosessissa. Suunnitteluun ja ohjeiden laatimiseen käytetty aika ja panostus saattavat olla käytännössä turhia. Toimintamallien jalkauttami-

seen on panostettava vahvasti, kannattaa miettiä systemaattista mallia, joka kulkee koko henkilöstön läpi, näin vähentäen muutosvastarintaa. (Koskinen 2009)

Jalkauttamisen vaiheistamisen suunnittelu olisi tärkeää, jolloin saataisiin askel kerrallaan hallitusti hoidettua tiedon siirto ja omaksuminen sille ryhmälle ja organisaatiolle, jonka käyttöön se on tarkoitettu. Johdolta vaaditaan muutosjohtajuuden taitoja, koska johdon tehtävänä on muutoksen hahmottaminen laaja-alaisesti ennakolta siten, että pystytään reagoimaan muutoksen vaikutuksiin toiminnassa. (Koskinen 2009, Sampo 2009)

Prosessissa voi olla ongelmallista prosessin mitattavuus ja mittarit, mitä toimintatapojen käyttöönotolla on tavoitteena saavuttaa ja niiden saattamisella käytäntöön. Tulosten mittaamismetodit ja mittarit saattavat olla vaikeasti luokiteltavissa.(Hallikainen & Hälikkä 2009)

Uuden käytännön käyttöönoton jälkeen on vaikea tietää, milloin tuloksien mittaamista voidaan suorittaa. Oikeanlaisten ja hyvien mittareiden löytäminen on haasteellista. (Hallikainen & Hälikkä 2009)

7 YHTEENVETO

”Sähköinen potilastietojärjestelmä on tuonut uusia riskejä potilasturvallisuuteen. Vanhat työtavat ja uudet tietojärjestelmät eivät toimi yhteen, joten työtapoja on uudistettava. Ongelmia syntyy etenkin siirtymävaiheessa, jos kaikki eivät käytä uutta järjestelmää ja ajantasaiset tiedot eivät päivity. Uuden oppiminen vie aina oman aikansa, ja järjestelmätkin voivat olla aika hankalia käyttää. Yleensä muutokset aiheuttavat vastarintaa. Ne, jotka eivät sitoudu uudistuksiin, väittävät potilasturvallisuuden vaarantuvan, koska aika menee tietojärjestelmien opetteluun” (Saranto, ESS, 2009). Päädyimme kyselytutkimuksemme ja havainnointimme perusteella samaan lopputulokseen.

Yksilön vastuu korostuu toimittaessa erittäin aralla tietosuojausta ja – turvaa vaativalla sektorilla, tapahtuupa toiminta sähköisesti, henkilökohtaisessa kontaktissa tai manuaalisesti. Tarvitaan sitoutumista annettujen ohjeiden noudattamiseen päivittäisillä tietoturvallisilla toimintatavoilla. Henkilöstön sisäistäessä ohjeistukset, heidät saadaan ymmärtämään vastuunsa ja toimintansa vaikutukset sekä myös lakien ja ohjeiden rikkomisesta aiheutuvat rangaistustoimenpiteet. Tietoturvatoiminnan tavoitteena on vastata tiedon oikea-aikaisuudesta ja siitä, että se on oikeassa paikassa ja oikeassa muodossa niiden henkilöiden käytettävissä, joilla on siihen laillinen tai työtehtävänsä vaatima valtuutus.

7.1 Johtopäätökset

Kyselytutkimuksen vastausten perusteella henkilöstö kaipasi koulutusta tietoturva- ja tietosuoja-asioihin liittyen. Tietoturvan ja tietosuojan tärkeys tiedostettiin. Lisäksi toivottiin omaan toimintaan liittyviä lyhyitä ja selkeitä käytännön ohjeita. Sähköisen tiedonkäsittelyn lisääntyminen vaatii ohjeistusten päivittämistä ja täsmentämistä. Näihin seikkoihin myös lait ja asetukset asettavat velvoitteita.

Tutkimustyömme tuloksena havainnoimme käytännön työssä esiin tulevia toimintatapoja. Inhimilliset tekijät, kuten äänekäs puhe esimerkiksi asiakasta kutsuttaessa kuvaukseen, käyttäjätunnusten ”lainaaminen”, yhteistunnusten käyttö ja paperilla oleva tieto nousivat esiin. Lisäksi arveluttivat useissa eri organisaatioissa ja eri osastoilla kiertävä henkilökunta, kuten huoltotoimissa ulkopuolisista organisaatioista käyvät henkilöt.

Havaintotutkimuksen ja pistokokeissa suoritettujen haastattelujen perusteella totesimme, että vaikka kaikki toimintakäytänteet tietoturvan tai tietosuojan kannalta eivät ole suositeltavia, niin käytännön työn sujuvuuden ja potilasturvallisuuden vuoksi ne ovat tarpeellisia ja toimintakulttuuri tekee ne mahdolliseksi. Kuten aiemmin tutkimusmenetelmäosiossamme on mainittu, kulttuuri muovaa inhimillistä käyttäytymistä (symbolisen interaktionismi), joka on luovaa tietoisen ja tiedostamattoman päätöksenteon seurauksena (Metsämuuronen 2000, 18). Tässä tapauksessa käytössä olevat toimintatavat ovat yleisesti tulkittuja sosiaalisia käytännemalleja. Luotetaan työtovereiden etiikkaan siten, ettei tarvitse epäillä väärinkäytöksiä yhteisessä työssä. Lakien ja asetusten mukaan toimiminen saattaa aiheuttaa liikaa rajoitteita, joten toiminnassa on pyrittävä huomioimaan myös järkevyys ja turvallisuusseikat. Tulevaisuudessa käyttöönotettava sähköinen toimikortti kertakirjautumisineen tulee muuttamaan tilannetta.

Teknisistä tekijöistä, jotka rajasimme tässä työssä hyvin pieneen osaan, kyselytutkimuksemme vastauksissa pohdittiin, miten mahdollisten teknisten vikojen aiheuttamat katkokset vaikuttavat tiedon eheyteen ja saatavuuteen. Organisatorisina tekijöinä voisimme mainita resurssipulan vuoksi käytettävät ostopalvelut.

Opimme ja sisäistimme myös hyvin paljon aihettamme koskevista laeista ja asetuksista, joita kaikkia emme edes tässä työssä käyneet läpi. Havaitsimme kysymysten laadinnan tarkan suunnittelun olevan erittäin tärkeää. Opimme, että kannattaa miettiä tarkkaan monelta suunnalta, ei vain kysymysten laatijan näkökulmasta, kuinka vastaajat mahdollisesti tulkitsevat kysymyksen.

Saamamme tuki tätä työtä tehdessämme on ollut organisaation taholta niin konsultoinnin, haastatteluiden kuin tarkastustenkin muodossa positiivista. Tästä päätellen tietoturva- ja tietosuoja-asiat katsotaan tärkeiksi. Niiden kehittämiseen halutaan panostaa ja organisaatiossa ollaan kiinnostuneita aiheeseen liittyvästä tutkimus- ja selvitystyöstä.

7.2 Pohdinta

Jouduimme karsimaan alkuperäisestä tutkimussuunnitelmastamme paljon johtuen ajan puutteesta, kuten käynnit kaikissa toimipisteissä, joten näiden fyysiset olot jäivät havainnoimatta. Rajauksia oli tehtävä paljon asian mielenkiintoisuuden vuoksi. Mitä enemmän asiaa tutkimme, sitä enemmän olisimme halunneet tietää ja selvittää.

Toiminnan kehittämiseksi ajanmukaisten laitteiden ja järjestelmien ylläpito ja hankinta olisivat sähköisen tiedonkäsittelyn nopeassa kehityksessä tärkeitä. Tiedon käytettävyys, eheys, pysyvyys, ajan tasaisuus ja saatavuus käyttöön oikeutetuille henkilöille tulisi pystyä turvaamaan.

Konkreettisena kehittämistoimenpiteenä ehdottaisimme heijastesuojien hankkimista niihin näyttöpäätteisiin, joiden sijoituksessa ei voida huomioida tietoturvaseikkoja. Asiakaskontakteissa kannattaa miettiä puheiden kuuluvuutta väärinkäsitysten välttämiseksi, koska myös henkilökohtaiset kohtaamiset vaativat tietoturvallista ja tietosuojattua toimintaa.

Jatkokehittämisehdotuksenamme on henkilöstön kouluttamiseen panostaminen sekä selkeä tiedottaminen tietoturva-asioista, näiden pohjana voisi käyttää jalkauttamissuunnitelmalistaamme. Atk-yhdyshenkilöiden roolin määrittämistä koko yhtymän alueella voisi selkiyttää ja näin nopeuttaa tiedon perillemenoa toimipisteissä.

Jalkauttamissuunnitelman perusteella tehtyjen toimenpiteiden avulla tarkoituksena olisikin saada henkilöstö aktiivisesti miettimään, kehittämään ja soveltamaan toi-

mintatapojaan tietoturvallisuuden ja – suojan parantamiseksi jokapäiväisten toimintatapojen vakiinnuttamiseksi.

Tehtäväksiantomme oli laaja, joten jalkauttamissuunnitelman jouduimme jättämään ylimalkaiseksi listaksi siitä, mitä voisi tehdä, mikäli olisi aikaa ja resursseja. Tämän listan annamme organisaatiolle vihjelistana, josta voidaan toteuttaa aiheelliseksi katsotut ja käyttökelpoiset toimenpide-ehdotelmamme, kuten opiskelijoiden käyttäminen rakenteisten ohjeistusten tekoon.

Jatkotutkimuksena tähän työhön ehdotamme mittariston kehittämistä ohjeistuksen jalkauttamisen seuraamiseksi.

Jo tämän opinnäytetyömme teon aikana raportoidessamme työn kulkua esimiehelle, tulosalueella on herännyt keskustelua tietoturvallisuuteen ja tietosuojaan liittyvistä seikoista ja niiden tärkeydestä. Pieniä toiminnan parannuksiakin on hiljalleen ryhdytty tekemään.

Vaitiolovelvollisuuden, tietoturvallisen ja tietosuojatun toiminnan katsotaan kuuluvan terveydenhuollossa toimivan henkilökunnan velvollisuuksiin ja etiikkaan. Organisaation tehtävänä on huolehtia siitä, että ohjeistukset ovat kunnossa ja henkilöstö on saanut tarvittavan koulutuksen ja perehdytyksen. Jokaisella on henkilökohtaisesti kuitenkin vastuu siitä, mitä tekee ja kuinka sen tekee.

LÄHTEET

KIRJALLISET LÄHTEET:

Anttila, P., 2007. Realistinen evaluaatio ja tuloksellinen kehittämistyö. Artefakta 19. Hamina: Akatiimi Oy.

Hirsjärvi, S & Hurme, H.1985: Teemahaastattelu. Jyväskylä: Gaudeamus.

Järvinen, P. 2002, Tietoturva ja yksityisyys, Jyväskylä, WSOYpro

Kleemola, M. Tervo-Pellikka, R., 1998, Tietosuoja, vaatimukset verkottuvassa tietojärjestelmässä, Jyväskylä, Gummerus

Metsämuuronen, J. 2000, Laadullisen tutkimuksen perusteet, Viro, Jaabes OÜ

Mäenpää, O. 2008, Julkisuusperiaate, Jyväskylä, WSOYpro

Nyyssölä, M. 2009, Yksityisyyden suoja työsuhteessa, Juva, WSOYpro

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

Pajukoski, M. 2004, Sähköinen asiointi sosiaali- ja terveydenhuollossa, Lainsäädännön rajat ja mahdollisuudet, Sosiaali- ja terveysalan tutkimus- ja kehittämiskeskus STAKES

STM Potilasasiakirjojen laatiminen sekä niiden ja muun hoitoon liittyvän materiaalin säilyttäminen Opas terveydenhuollon henkilöstölle, Oppaita 2001:3, 2002, Helsinki, Edita, PRIMA Oy

Vilkka, H. 2007, Tutki ja havainnoi, Vaajakoski, Gummerus kirjapaino Oy

Ylipartanen, A. 2004, Tietosuoja terveydenhuollossa, Helsinki, Tietosanoma Oy

TUTKIMUSRAPORTIT:

Järvinen, P. 2006, PACS-järjestelmät ja potilaan tietosuojan toteutuminen, Oulun yliopisto, Pro gradu

Reponen, K. 2006, Terveydenhuollon organisaation tietoturvallisuus henkilöstön arvioimana, Kuopion yliopisto, Pro gradu

Syrjänen, P. 2006, Yksityisyyden suoja ja henkilöarviointi, Tampere, Tampereen Yliopistopaino Oy – Juvenes print, Väitöskirja

AIKAKAUS- JA SANOMALEHTIARTIKKELI:

Saranto, K. 2009. Sähköisessä potilastietojärjestelmässä turvallisuusriskejä. Etelä-Suomen Sanomat 30.6.2009

ELEKTRONISET LÄHTEET:

1995/46/EY, Euroopan parlamentin ja neuvoston direktiivi yksilöiden suojelusta, henkilöiden suojelusta ja vapaasta viestinnästä. Annettu Brysselissä 24.10.1995. [viitattu 18.10.2009] Saatavissa internetissä:
http://eur-lex.europa.eu/LexUriServ/

2002/58/EY Euroopan parlamentin ja neuvoston direktiivi henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla (sähköisen viestinnän tietosuojadirektiivi). Annettu Brysselissä 12.7.2002.
[viitattu 18.10.2009] Saatavissa internetissä:
http://eur-lex.europa.eu/LexUriServ/

HE 96/1998, Valtionhallinnon tietoturvallisuuden johtoryhmä 2/2008
Annettu Naantalissa 24.7.1998.
[viitattu 8.10.2009] Saatavissa internetissä:
(http://www.tietosuoja.fi/)

FINLEX ® - Valtion säädöstietopankki
Arkistolaki (1994/831)
Annettu Helsingissä 23.9.1994. [viitattu 20.10.2009] Saatavissa internetissä:
(http://www.finlex.fi/fi/laki/ajantasa/1994/19940831)

FINLEX ® - Valtion säädöstietopankki
Erikoissairaanhoitolaki 2000/652
Annettu Helsingissä 30..6.2000 [viitattu 20.10.2009] Saatavissa internetissä:
http://www.finlex.fi/fi/laki/ajantasa/haku.php

FINLEX ® - Valtion säädöstietopankki
Hallintolaki 2003/434
Annettu Helsingissä 6.6.2006. [viitattu 20.10.2009] Saatavissa internetissä:
(http://www.finlex.fi/fi/laki/alkup/2000/2000)

FINLEX ® - Valtion säädöstietopankki
Henkilötietolaki 1999/ 523
Annettu Helsingissä 22.4.1999.[viitattu 20.10.2009] Saatavissa internetissä:
http://www.finlex.fi/fi/laki/ajantasa/1999/19990523)

FINLEX ® - Valtion säädöstietopankki
Kuntalaki 1995/365
Annettu Helsingissä 17.3.1995.[viitattu 20.10.2009] Saatavissa internetissä:
(http://www.finlex.fi/fi/laki/ajantasa/1995/19950365)

FINLEX ® - Valtion säädöstietopankki
Laki ja asetus terveydenhuollon ammattihenkilöistä 1994/559
Annettu Helsingissä 28.6.1994. [viitattu 20.10.2009] Saatavissa internetissä:
(http://www.finlex.fi/fi/laki/ajantasa/1994/19940559)

FINLEX ® - Valtion säädöstietopankki
Laki potilaan asemasta ja oikeuksista lain muuttamisesta 2000/653
Annettu Helsingissä 23.6.2005.[viitattu 20.10.2009] Saatavissa internetissä:
(http://www.finlex.fi/fi/laki/alkup/2000/2000)

FINLEX ® - Valtion säädöstietopankki
Laki viranomaisen toiminnan julkisuudesta 1999/621, 2005/495
Annettu Helsingissä 21.5.1999. [viitattu 20.10.2009] Saatavissa internetissä:
(http://www.finlex.fi/fi/laki/ajantasa/1999/19990621)

FINLEX ® - Valtion säädöstietopankki
Potilasvahinkolaki 1986/585
Annettu Naantalissa.25.7.1999. [viitattu 20.10.2009] Saatavissa internetissä:
http://www.finlex.fi/fi/laki/ajantasa/1986/19860585

FINLEX ® - Valtion säädöstietopankki
Sosiaali- ja terveysministeriön asetus potilasasiakirjoista 2009/298
Annettu Helsingissä 30.3.2009. [viitattu 20.10.2009] Saatavissa internetissä:
(http://www.finlex.fi/fi/laki/ajantasa/2009/20090298)

FINLEX ® - Valtion säädöstietopankki
Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä
2007/159 Annettu Helsingissä 9.2.2007. [viitattu 20.10.2009] Saatavissa internetissä: (http://www.finlex.fi/fi/laki/ajantasa/2007/20070159)

FINLEX ® - Valtion säädöstietopankki
Säteilylaki 1991/592. Annettu Helsingissä 27.3.1991.[viitattu 20.10.2009] Saatavissa internetissä:http://www.finlex.fi/laki/ajantasa/1991/19910592)

FINLEX ® - Valtion säädöstietopankki
Sosiaali- ja terveysministeriön asetus potilasasiakirjojen laatimisesta sekä niiden ja muun hoitoon liittyvän materiaalin säilyttämisestä. Annettu Helsingissä 19.1.2001.[viitattu 25.10.2009] Saatavissa internetissä:
http://www.finlex.fi/fi/laki/alkup/2001/20010099

Päijät-Hämeen sosiaali- ja terveydenhuollon kuntayhtymän Internet-sivut 2009
http://www.phshp.fi/

Sisäasiainministeriö, poliisiosasto, määräys SM nro 2008/353
Tietoturvaperiaatteet. Annettu 30.7.2008. [viitattu 20.10.2009] Saatavissa internetissä: http://www.intermin.fi

Tietosuojavaltuutetun toimiston sivut:
Henkilötietojen luovuttaminen viranomaisten henkilörekisteristä,

[viitattu 20.10.2009] Saatavissa internetissä:
http://www.tietosuoja.fi/uploads/fkdjwcbogib.rtf

Varhaiskasvatuksen sähköinen asiointi ja viestintä – hanke – tuloksien muuttaminen arjen toiminnaksi 2009. Kuopion kaupunki, Koulutuspalvelukeskus, päivähoito, Hallikainen, J. & Hälikkä. S. [viitattu 20.6.2009]
Saatavissa internetissä: http://www.sosiaaliportti.fi/

Koskinen, J-M. 2009. Strategiasta käytännöksi. Liiketalous, liiketalouden osaajat ja ammattilaiset. 2009 [viitattu 20.6.2009] Saatavissa internetissä:
http://www.liiketalous.fi/

Sampo, T. 2009. Strategian jalkauttaminen, liiketalouden näkökulma. Maanpuolustuskorkeakoulu, johtamisen laitos. [viitattu 20.6.2009] Saatavissa internetissä:
http://www.mpkk.fi/

SUULLISET LÄHTEET:

Inkinen S. 2009. Osastonhoitaja, Päijät-Hämeen Sosiaali- ja terveydenhuollon kuntayhtymä. Haastattelut tutkimustyön eri vaiheissa. 2009.

Taipale, A-O. 2009. Tietohallintojohtaja. Päijät-Hämeen Sosiaali- ja terveydenhuollon kuntayhtymä. Haastattelut tutkimustyön eri vaiheissa. 2009.

Kuvantamisen henkilöstöä. 2009. Päijät-Hämeen Sosiaali- ja terveydenhuollon kuntayhtymä. Haastattelut tutkimustyön eri vaiheissa. 2009.

MUUT LÄHTEET:

Päijät-Hämeen sosiaali- ja terveydenhuollon kuntayhtymän Tietoturvapolitiikka, 2009

Radiologian toimintakäsikirja, Päijät-Hämeen sosiaali- ja terveydenhuollon kuntayhtymä, 2009

Roivainen, N. & Pekkanen, H. . Päijät-Hämeen sosiaali- ja terveydenhuollon kuntayhtymän Radiologian työnkulkukaavio, 6/2008

Valtionhallinnon tietoturvallisuuden johtoryhmä10/2006

Yin, R.K, 1983, Case Reseach. Design and Methods. Applied Social Research Methods series vol 5. Lontoo:Sage, 23

LIITTEET

Tietoturva- ja tietosuojakysely kuvantamisen henkilökunnalle

Opiskelemme Lahden Ammattikorkeakoulun Julkisten palvelujen johtamisen koulutusohjelmassa. Päättötyönämme teemme "Tietoturvan ja tietosuojan kehittäminen kuvantamisen tulosalueelle".
Tämän kyselyn tarkoituksena on selvittää kuvantamisen henkilökunnan toimintatapoja tietoturvan ja tietosuojan kannalta.
Toivomme laajaa osanottoa kyselyymme saadaksemme kattavan ja luotettavan materiaalin tutkimustyötämme varten.
Vastausaika alla oleviin kysymyksiin päättyy 4.9.2009.

1) Pääasiallinen toimipisteesi on *

- ○ Keskussairaalassa
- ○ Alueen toimipisteessä

2) Ammattiryhmäsi *

- ○ lääkäri
- ○ hoitaja
- ○ muut

3) Ikäryhmäsi *

- ○ alle 30
- ○ 31 - 50
- ○ yli 51

4) Kuinka kauan olet työskennellyt PHSOTEY:ssä *

- ○ alle 5 vuotta
- ○ 6 - 10 vuotta
- ○ yli 11 vuotta

5) Toimimme tietoturvallisessa työympäristössä, johon osana kuuluu tietosuoja, koskien mm henkilötietojen salassapitoa ja suojaamista sekä yksityisyyden loukkaamattomuutta. Oletko saanut tietoturvaa- ja tietosuojaa koskevaa perehdytystä? *

- ○ Olen PHSOTEY:ssä
- ○ Olen entisessä työpaikassa
- ○ En ole
- ○ Muualla, missä

6) Onko tietoturva ja -suoja tarkoitettu mielestäsi suojaamaan *

- ○ Henkilökuntaa
- ○ Asiakkaita
- ○ Organisaatiota
- ○ Kaikkia näitä

7) Tuleeko tietoturva esiin käytännön työssäsi? *

- ○ En ole huomioinut
- ○ Jossain määrin
- ○ Suuressa määrin, miten?

8) Kuinka usein vaihdat salasanasi? *

- ○ Kuukausittain
- ○ Kolmen kuukauden välein
- ○ Vuosittain
- ○ Muistaessani
- ○ En koskaan

9) Tunnistatko omassa työskentely-ympäristössäsi tietoturvariskejä, millaisia? *

10) Oletko tutustunut PHSOTEY:n tietoturvapolitiikkaan?

*

- Olen
- En

11) Oletko allekirjoittanut tietoturva- ja tietosuojasitoumuksen? *

- Olen PHSOTEY:ssä
- Olen entisessä työpaikassani
- En ole

12) Oletko huomannut puutteita / virheitä tietosuojaan tai tietoturvaan liittyvissä asioissa / toiminnoissa työpaikallasi? *

- Olen
- En ole

13) Mikäli olet huomannut, mainitse lyhyesti esimerkkejä? *

14) Kuinka usein tarvitset organisaation sähköpostia työasioiden hoitoon? *

- Päivittäin
- Viikoittain
- Kuukausittain
- Tuskin lainkaan
- En ollenkaan

15) Kuinka usein törmäät tietosuojaan / tietoturvaan liittyviin kysymyksiin asioidessasi sähköpostilla? *

	Erittäin usein	Usein	En milloinkaan	Harvoin	Erittäin harvoin
Henkilötunnus *	☐	☐	☐	☐	☐
Roskaposti *	☐	☐	☐	☐	☐
Potilaan sairauskertomustietoja *	☐	☐	☐	☐	☐
Henkilökunnan sairauskertomustietoja *	☐	☐	☐	☐	☐

16) Mikä on mielestäsi tehokkain kanava saada tietoturva- ja tietosuojaohjeistusta? *

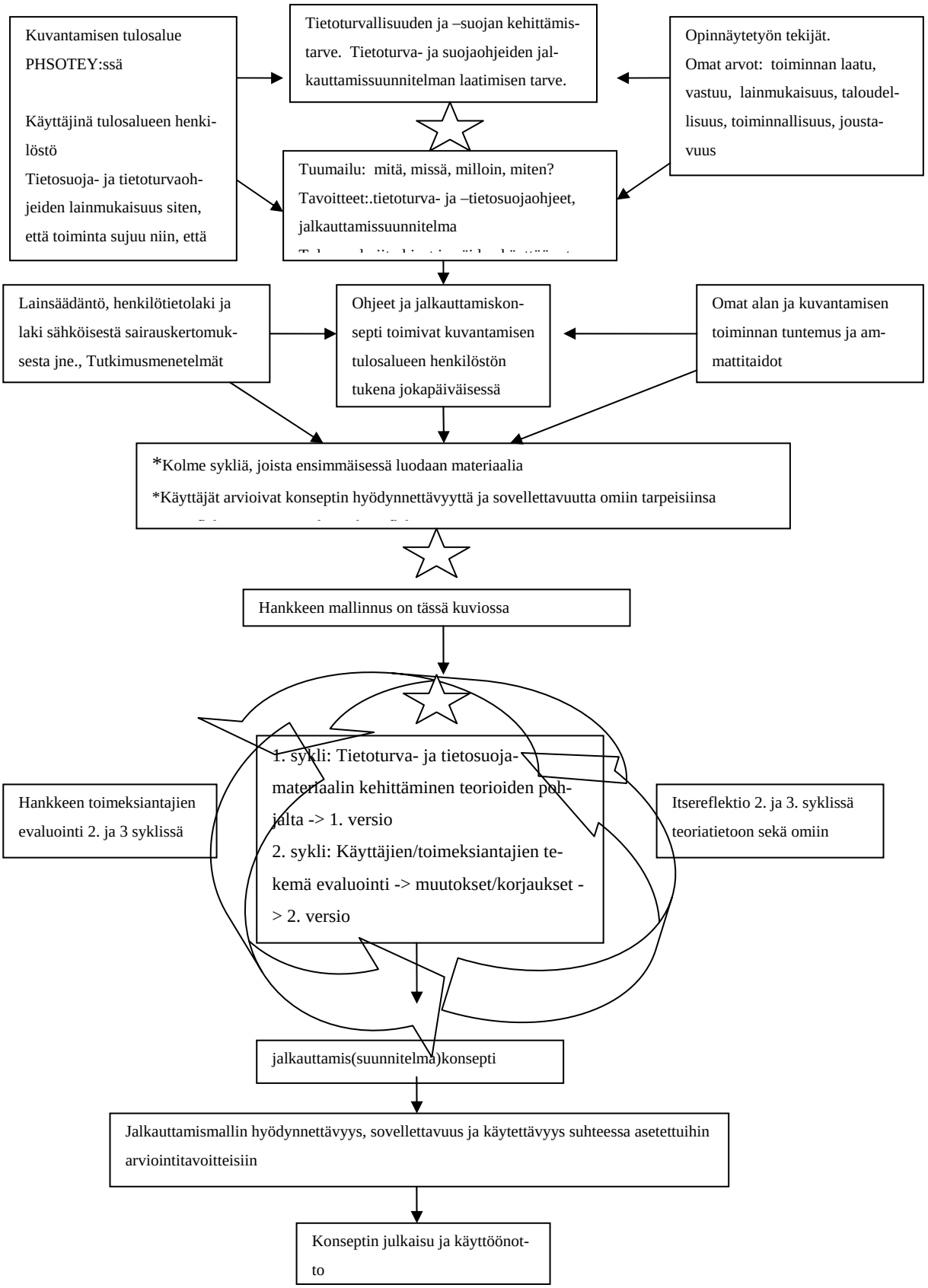
17) Millaisia tietoturva- ja tietosuojaohjeita kaipaat? *

18) Jos tarvitset apua tietoturva-asioissa, tiedätkö keneen otat yhteyttä? *

- Esimieheesi
- ATK-yhdyshenkilöön
- Tietoturva- tai tietosuojavastaavaan
- Lähimpään työkaveriin
- En tiedä

19) Tuleeko vielä jotain muuta mieleesi tietoturvasta tai tietosuojasta (esim. parannettavaa, muutettavaa tms.)?

LIITE 2



Kuvio 5. Realistisen evaluaation malli (mukaellen Anttila 2007, 88)