JYVÄSKYLÄN YLIOPISTO
UNIVERSITY OF JYVÄSKYLÄ

Tietoturvapolitiikan kehittäminen Pohjois-Pohjanmaan sairaanhoitopiirissä

Siponen & Puhakainen tietoturvapolitiikan kehittämismallin mukaisesti

Jyväskylän yliopisto
Informaatioteknologianlaitos
Jenni Siermala
Pro Gradu -tutkielma
29.11.2015

Tiivistelmä

Tämän tutkimuksen tarkoituksena on selvittää, kuinka Siposen ja Puhakaisen tietoturvapolitiikan kehittämismallia toteutetaan ja kehitetään käytännössä. Se koostuu neljästä lähtökohdasta. Kirjallisuudesta ei löydy tietoturvapolitiikkaa, joka olisi toteutettu tämän mallin mukaisesti. Lisäksi tutkimuksessa selvitetään mallin soveltuvuutta Pohjois-Pohjanmaan sairaanhoitopiirissä (PPSHP).

Tutkimus toteutettiin laadullisena toimintatutkimuksena, joka koostui viidestä vaiheesta: määrittäminen, suunnittelu, toteutus, arviointi sekä tarkentaminen ja oppiminen. Tutkimustietoaineisto kerättiin haastatteluiden avulla (PPSHP:n tietoturvasta ja tietosuojasta vastaavia henkilöitä), tutkimalla PPSHP:n strategiaa sekä terveydenhuollon tietoturvaa ja tietosuojaa velvoittavaa lainsäädäntöä. Haastatteluiden teemat nousivat Siposen ja Puhakaisen tietoturvapolitiikan kehittämismallista. Tiedonkeruumenetelmien avulla selvitettiin Siposen ja Puhakaisen tietoturvapolitiikan kehittämismallin mukaiset vaatimukset tietoturvapolitiikalle.

Tutkimuksessa havaittiin, että tämä malli soveltuu hyvin PPSHP:n tietoturvapolitiikan toteuttamiseen ja käyttöönottoon. Tutkimuksessa syntyi yhteensä kymmenen ylä- ja alatason tietoturvapolitiikkadokumenttia, toteutettiin PPSHP:lle tietojärjestelmien luokittelu ja kehitettiin uusia prosesseja muun muassa ICT-varautumisen osalta. Näiden toimien avulla PPSHP:n tietoturva tasoa nostettiin.

Avainsanat
Tietoturva, tietoturvapolitiikan kehittämismalli, tietoturvapolitiikka

Abstract

The purpose of this study is to examine how the Siponen and Puhakainen method for the development of information security policies are executed in practice. The study consists of four premises which define the information security policies. In existing literature there are no studies handling on specifically this sort of design of information security policy put into practice. In addition, this study concentrates on evaluating the applicability of the information security policy in question to practice at Pohjois-Pohjanmaan sairaanhoitopiiri (PPSHP).

This study was carried out as a qualitative Action research cycle -study (ACR). ACR consists of five stages: diagnosing, action planning, action taking, evaluating and specifying and learning. The research data was collected by interviews (interviewing people responsible of data privacy and information security at PPSHP), investigating the strategy and the obligating information security legislation concerning healthcare. The main themes of the interviews emerged from the information security policy method for development of design by Siponen and Puhakainen. With the data collecting methods mentioned, the study was carried out to find specifications for the information security policy method by Siponen and Puhakainen.

It was found out that the design by Siponen and Puhakainen method for the development of information security policies is well applicable at the information security policy management at PPSHP. The study produced altogether ten higher and lower level information security policy documents, information system classification and provisions processes of information systems was developed. With these actions the level of information security of PPSHP was improved.

Key words:
information security, developing model of information security policy, information security policy

Alkusanat

Kiitokset Pohjois-Pohjanmaan sairaanhoitopiirin tietoturvaryhmälle luvasta toteuttaa tämän tutkimuksen Oulun yliopistollisessa sairaalassa. Erityisesti kiitän PPSHP:n hallintoylilääkäriä Juha Korpelaista, hallintolakimiestä Sari Haatajaa ja tietoturvavastaavaa Pentti Körkköä, jotka lupautuivat haastateltaviksi. Lisäksi haluan kiittää kaikkia muita PPSHP:n työntekijöitä, jotka osallistuivat tutkimukseen tietoturvapolitiikoiden kommentoinnin myötä.

Haluan myös kiittää tämän lopputyön ohjaajaa, professori Mikko Siposta. Lisäksi tutkimusprosessin aikana sain Petri Puhakaiselta kannustusta ja arvokkaita kommentteja.

Oulussa 29.11.2015
Jenni Siermala

Sisältö

Tiivistelmä 2
Abstract 3
Alkusanat 4
1. Johdanto 6
2. Tietoturvapolitiikan toteuttaminen organisaatiossa eri mallien mukaan 8
3. Siponen & Puhakainen tietoturvapolitiikan kehittämismalli 12
4. Tutkimusmenetelmät ja tutkimusympäristö 14
4.1. Tutkimusmenetelmät 14
4.2. Toimintatutkimus 15
4.3. Tutkimusaineiston kerääminen 17
4.4. Tutkimusympäristö 18
4.4.1. Organisaatiorakenne 18
4.4.2. Pohjois-Pohjanmaan sairaanhoitopiirin kuntayhtymän strategia 20
5. Tietoturvapolitiikan kehittäminen Siponen & Puhakainen tietoturvapolitiikan kehittämismallin mukaisesti 21
5.1. Tietoturvapolitiikan vaatimusten kartoitus 22
5.1.1. Lainsäädännön vaatimukset tietoturvapolitiikkaan 23
5.1.2. Tietoturvapolitiikan vaatimukset organisaation strategiasta 24
5.2. Tietoturvapolitiikoiden suunnittelu 28
5.2.1. Tieto-omaisuuden tunnistaminen 29
5.2.2. Tieto-omaisuuden luokittelu 29
5.2.3. Tietoturvapolitiikoiden suunnittelu 30
5.3. Tietoturvapolitiikoiden toteuttaminen 31
5.4. Tietoturvapolitiikoiden testaaminen 34
5.5. Tietoturvapolitiikoiden arviointi 35
6. Pohdinta 37
7. Johtopäätökset 39
Lähteet 40
Liite A. Tutkimuksessa käytetyt kysymykset 44
Liite B. Tutkimuksessa hyödynnetyt lait 45

1. Johdanto

Ruighaver, Maynar & Chang mukaan tietoturvapolitiikka tukee organisaation tietoturvakulttuuria ja tietoturvapolitiikka on yksi tietoturvakulttuurin osa-alue. Tietoturvakulttuuri heijastelee tietoturva-asenteita ja sitä, kuinka organisaation johto puuttuu tietoturva kysymyksiin. (Ruighaver, Maynard, & Chang 2007.) Organisaation tulee suunnitella tietoturvapolitiikka siten, että tieto-omaisuus on turvattu (Louw, Roussouw & Thompson 2006).

Tietoturvapolitiikka on siis tärkein osa yrityksen tietoturvakokonaisuuden suunnittelua. Siinä on kuvattu organisaation johdon tavoitteet ja käytännöt tietoturvallisuuden saavuttamiseksi. Tietoturvapolitiikassa kuvataan yleisellä tasolla organisaation kannalta tarvittava tietoturva-aste ja miten tälle asteelle päästään. Tietoturvapolitiikassa on lisäksi suuntaviivat miten organisaation tietoturvapolitiikkaa ylläpidetään ja kehitetään. Tietoturvapolitiikka on organisaation osa organisaation tieto- ja viestintäpolitiikkaa. (Hakala, Vainio & Vuorinen 2006.)

Tietoturvapolitiikka on asiakirja, joka antaa suuntaviivat organisaation tiedon suojaamiselle, kuvaa organisaation johdon sitoutumista ja tukea tiedon turvaamiselle. Tietoturvapolitiikan hyvä olla linjassa organisaation toiminnan kanssa, mukailtava organisaation tavoitteita ja tehtäviä, noudattaa organisaation liiketoiminnan linjauksia ja organisaation turvallisia toimintatapoja. (Höne & Eloff 2002). Tietoturvapolitiikan tavoitteena on vähentää riskejä, jotka kohdistuvat organisaation tietoon erilaisissa organisaation toiminnoissa. (Karyda, Kiountouzis & Kokolakis 2005).

Kun organisaatioon on luotu tietoturvapolitiikka, tulee varmistua että luotuja menetelmiä toteutetaan ja tietoturvapolitiikkaa organisaatiossa noudatetaan. Jos tietoturvapolitiikkaa ei noudateta, työntekijät eivät työskentele tehokkaasti. (Backhouse & Dhillon 2001.) Sen lisäksi organisaation tieto ja liiketoiminta voivat joutua vaaraan, jos organisaatiossa ei noudateta tietoturvallisia toimintatapoja ja tekniikoita. Ei ole myöskään mielekästä toimintaa, jos organisaatiossa työntekijät ovat tietoisia tietoturvapolitiikasta mutta eivät noudata sitä. Tietoturvakoulutus tukee työntekijöiden tietoturvapolitiikan noudattamista. (Siponen, Pahnila & Mahmood 2007.)

Tietoturvakoulutuksen tavoitteena on saada työntekijät toimimaan turvallisesti organisaation toimintaympäristössä. Tietoturvapolitiikan noudattamista organisaatiossa tukee koulutuksen lisäksi sanktiot. Organisaatiossa tulee olla toimintatapa kuinka menetellään, jos on toimittu tietoturvapolitiikan vastaisesti. (Puhakainen & Siponen 2010).

Kirjallisuus suosittelee, että tietoturvapolitiikan taustalla on viitekehys, kun tietoturvapolitiikkaa luodaan. Tietoturvapolitiikassa tulisi olla määriteltynä tietoturvaprosesseja ja organisaation pitäisi olla motivoitunut toteuttamaan ja ylläpitämään niitä. (Knapp, Morris, Marshall & Byrd 2009.)

Tässä tutkimuksessa selvitetään kuinka Siposen & Puhakaisen tietoturvapolitiikan kehittämismallia toteutetaan ja kehitetään käytännössä. Kohde organisaatio on Pohjois-Pohjanmaan sairaanhoitopiiri (PPSHP). Kirjallisuudesta ei löydy tietoturvapolitiikkaa,

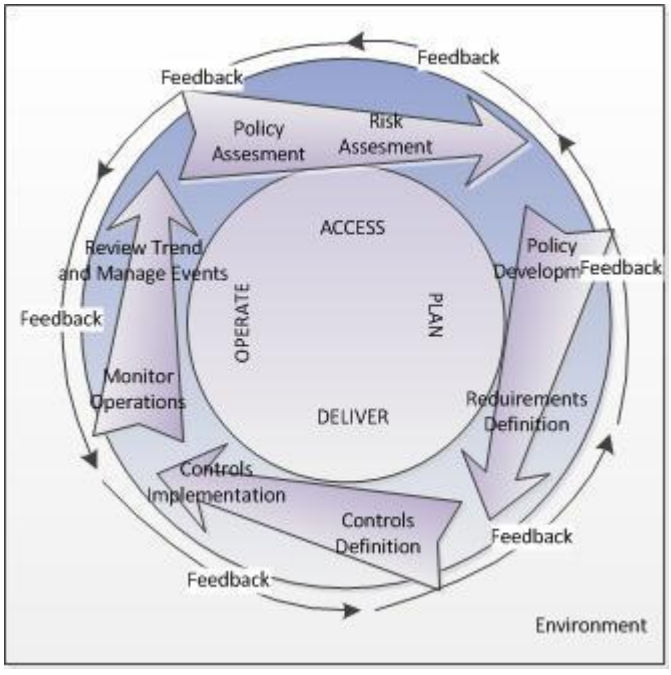
joka olisi toteutettu tämän mallin mukaisesti. Lisäksi tutkitaan mallin soveltuvuutta tässä konteksitissa.

2. Tietoturvapolitiikan toteuttaminen organisaatiossa eri mallien mukaan

Tässä luvussa tarkastellaan kirjallisuudesta selityksiä sille, miten tietoturvapolitiikka koostuu organisaatiossa, mitä tietoturvapolitiikan toteuttamisessa tulee ottaa huomioon ja erilaiset mallit sen toteuttamiselle. Tutkijat ovat kehittäneet erilaisia malleja tietoturvapolitiikan toteuttamiselle. Tässä luvussa tarkastellaan näitä malleja.

Tietoturvapolitiikka on yleensä melko korkean tason dokumentti, joka on tekniikka riippumaton. Tietoturvapolitiikassa otetaan huomioon organisaation riskit, asetetaan suunta ja menettelytavat tiedon turvaamiselle. Lisäksi tietoturvapolitiikassa määritellään sanktiot eli kuinka menetellään, jos tietoturvapolitiikan vastaisesti toimitaan. Tietoturvapolitiikan toteuttaminen perustuu tietoturvastandardeihin, menettelytapoihin ja ohjeisiin, joita ei saa sekoittaa keskenään. Tietoturvapolitiikka luodaan ja valtuutetaan organisaation edustajille, organisaatiosta riippuen oikealle taholle, se voi olla esimerkiksi henkilöstöhallinto, turvallisuus- tai tiedotusosasto. (Rees, Bandyopadhyay & Spafford 2003.)

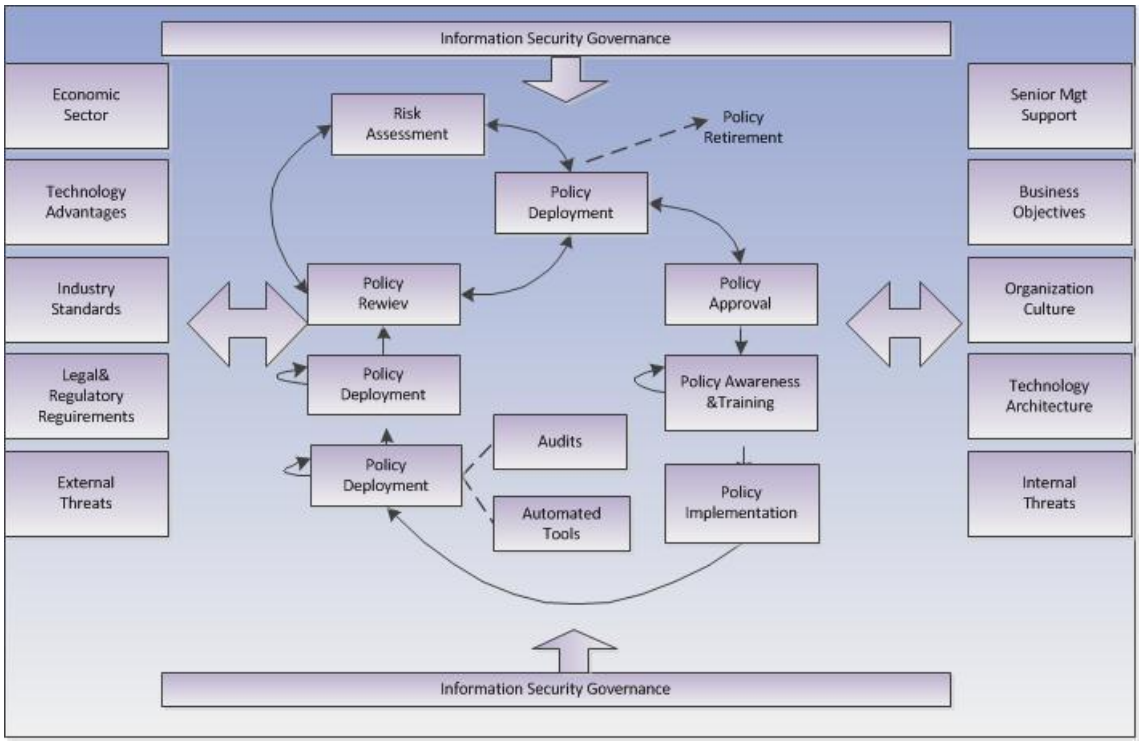
Rees ja muut (2003) ovat kehittäneet mallin, jonka nimi on Policy Framework for Interpreting Risk in E-Business Security (PFIRES). Tämän mallin tavoitteena on luoda organisaation tietoturva-asiantuntijoille ja organisaation johdolle ohje, kuinka tietoturvastrategia ja -politiikka toteutetaan ja ylläpidetään. Malli sisältää sekä uuden tuotteen kehitysmallin (new product development life cycle) että järjestelmän elinkaarimallin (systems development life cycle SDLC), näiden mukaisesti uudet teknologiat ja sovellukset toteuttavat organisaation määrittämiä tietoturvallisuuden suuntaviivoja. Kuviossa 1 on kuvattu PFIRES malli. (Rees ym. 2003.)



KUVIO 1. *PFIRES life-cycle malli (Rees ym. 2003.)*

PFIRES elinkaari mallissa on neljä päävaihetta: arvioi (Acces), suunnittele (Plan), toteuta (Deliver) ja käytä (Operate). Koska kyseessä on iteratiivinen prosessi, joka vaiheesta on palaute silmukka. Palaute on tärkeää senkin vuoksi, että voidaan varmistaa tyydyttävätkö edellisen vaiheen vaatimukset. Organisaation muutos on kuvattu jatkumona, jonka päätepisteet ovat taktinen ja strateginen. Taktinen muutos sisältää lyhyenaikavälin tähtäimellä toteutettavan saavutuksen. Tässä arvioidaan kuinka muutoksen hallinta ja arviointi tukevat muutosta. Kun taas organisaation pitkän aikavälin strategisen muutokset, useimmat organisaatiot epäonnistuvat toteuttaessaan tavoitetta, näistä kahden muutoksesta. PFIFES tukee organisaatiota muutoksessa ja on sen vuoksi hyvin organisaatio liiketoimintastrategialähtöinen. (Rees ym. 2003.)

Knapp, Morris, Marshall & Byrd (2009) ovat kehittäneet menetelmän, jonka mukaisesti tietoturvapolitiikka toteutetaan kahdessa vaiheessa. KUVIOSSA 2 on kuvattu tämä menetelmä (Knapp ja muut 2009).



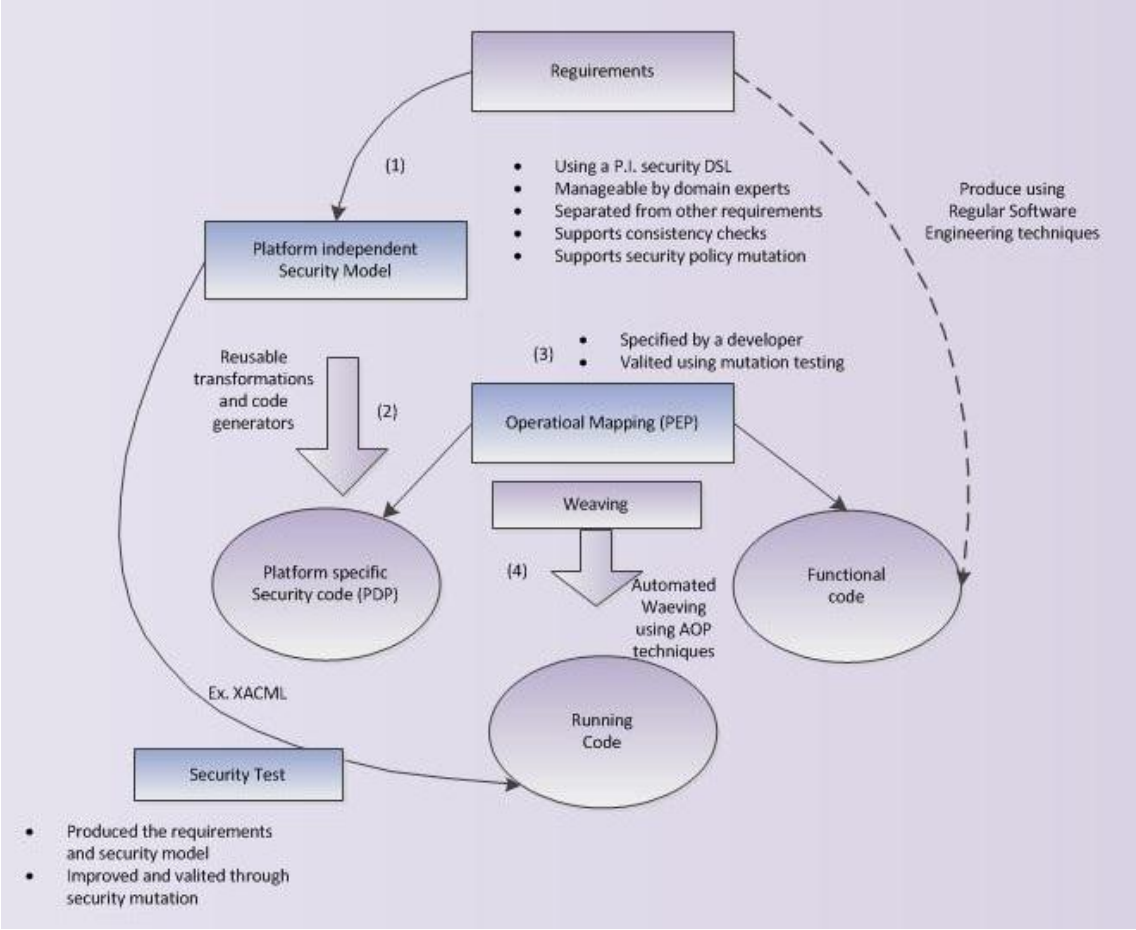
KUVIO 2. *Tietoturvapolitiikan kehittämisen vaiheet organisaatiossa. (Knapp ja muut 2009).*

Ensimmäinen vaihe toteutetaan kuvion 2 mukaisesti. Kuvion ulkokehällä olevat vaikutteet ovat merkityksellisiä ja ne tulee huomioida muodostettaessa vaatimuksia tietoturvapolitiikalle. Näitä ovat organisaation sisäisten, -ja ulkoisten vaikutteiden arvioiminen sekä tietoturvahallinnon näkemykset ja niiden vaikutus tietoturvapolitiikkaan. Ulkoiset vaikutteet syntyvät taloudesta, teknologioista, teollisuuden standardeista, lain säädännöstä ja ulkoisista uhkista. Organisaation sisältä tulevat vaikutteet puolestaan ovat johdon tuki, liiketoiminta, organisaation kulttuuri, teknologinen arkkitehtuuri ja sisäiset uhkat. (Knapp ym. 2009.)

Toinen vaihe toteutetaan kuvion 2 mukaisesti. Kuviossa keskellä tietoturvapolitiikan kehittäminen käynnistyy. Vaiheessa toteutetaan organisaation prosesseja toistuvasti, jossa tietoturvapolitiikkaa arvioidaan, organisaation riskejä arvioidaan suhteessa

tietoturvapolitiikkaan ja näiden mukaisesti tietoturvapolitiikkaa kehitetään. Tämä muodostaa yleisen prosessivirran. Vaiheet etenevät riskien arvioinnista tietoturvapolitiikan kehitykseen ja tietoturvapolitiikan arviointiin. Näissä vaiheissa voidaan nuolien mukaisesti palata takaisin, jos se on tarpeen. Tietoturvapolitiikka hyväksytään organisaatiossa, se koulutetaan organisaation henkilökunnalle ja otetaan käyttöön organisaation prosesseissa. Tietoturvapolitiikan noudattamista valvotaan. Tietoturvapolitiikkaa arvioidaan ja se voi tarvittaessa käynnistyä uudelleen toteutettavaksi. Kun tietoturvapolitiikka vanhentuu, se poistetaan käytöstä ja toteutetaan uusi dokumentti tämän kehitysprosessiin mukaisesti. (Knapp ym. 2009.)

Baudry, Fleurey Le Traon & Mouelhi (2008) ovat toteuttaneet Java sovelluksen, jonka avulla tietoturvapolitiikka määritetään, kehitetään ja testataan. Tietoturvapolitiikka määritellään ohjelmointikielien avulla (OrBAC, RBAC). Tästä muodostuu yleinen tietoturvan perusmalliin, ja sitä käytetään aikaisen vaiheen yhtenäisyystarkastuksissa. Perusmalli siirretään automaattisesti tietoturvapolitiikkaan XACML alustalle integroituun sovellukseen, jotta voidaan varmistua testitapausten laatu, kaikki ne virheet, joilla on vaikutusta tietoturvapolitiikkaan, lähetetään tietoturvapolitiikan perusmalliin ja käsitellään sen mukaisella tavalla. (Mouelhi ym. 2008.) Alla on kuvio tämän prosessin toteutumisesta.



KUVIO 3. Tietoturvapolitiikan kehittämisen malli. (Baudry ym. 2008).

Tietoturvapolitiikka on organisaatiossa tiedon turvaamisen kannalta olennaisen tärkeä. Organisaation tietoturva on kompleksinen ja sen vuoksi tietoturvapolitiikka on syytä

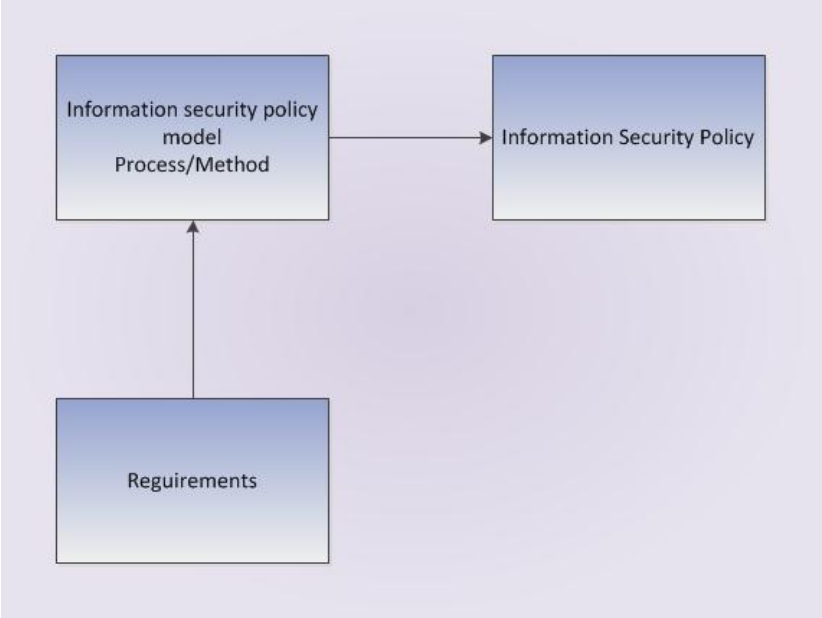
tehdä useassa tasossa (Yusufovna 2008). Myös organisaation vaatimukset tietoturvapolitiikalle ovat tärkeässä osassa, jotta voidaan suojella organisaation tieto-omaisuutta mahdollisimman tehokkaasti (Peltier 2002).

Tietoturvapolitiikka jaetaan hierarkisesti ylä- ja alatason tietoturvapolitiikkoihin, tämän avulla organisaation toimintaympäristö turvataan tehokkaasti. Ylä- ja alatason tietoturvapolitiikoissa otetaan huomioon erilaiset organisaatioon kohdistuvat vaatimukset, jotka tulevat liiketoiminnasta, lainsäädännöstä ja muusta toimintaympäristöstä. (Knapp ym. 2009). Kun organisaation toimintaympäristö ja organisaation omat vaatimukset otetaan riittävissä määrin huomioon, varmistetaan, että organisaatio toimii turvallisesti. Tietoturvapolitiikan on mukailtava organisaation toimintoja, siksi tietoturvapolitiikat jaetaan myös alatasoihin, näin saavutetaan tehokas tietoturvapolitiikka. (Baskerville & Siponen 2002.)

3. Siponen & Puhakainen tietoturvapolitiikan kehittämismalli

Siponen & Puhakainen (2015) tietoturvapolitiikan kehittämismallia sovelletaan tässä tutkimuksessa toteutettaessa tietoturvapolitiikkaa. Tämä malli on valittu sen vuoksi, että siinä toteutuu kirjallisuuden mukainen jaottelu ylä- ja alatason politiikoihin tietoturvapolitiikan kehittämismallissa otetaan organisaation vaatimusten kartoittaminen tietoturvapolitiikalle erityisen hyvin huomioon. Lisäksi kirjallisuuden mukaan tätä mallia ei ole sovellettu käytännössä. Siponen & Puhakainen tietoturvapolitiikan kehittämismallissa valitseminen tähän kontekstiin sopii hyvin. (Siponen & Puhakainen 2015.)

Kun organisaatiossa noudatetaan teoriamallia/menetelmää tietoturvapolitiikan toteuttamisessa ja otetaan huomioon organisaatioon kohdistuvat vaatimukset, lopputuloksena syntyy tehokas ja organisaation toimintoja mukaileva tietoturvapolitiikka (Baskerville & Siponen 2002). Kuvio 4 kuvaa tämän prosessin.



KUVIO 4. Tietoturvapolitiikan prosessi mukaillen Baskervilleä & Siposta. (Baskerville ym. 2002).

Kuten edellä (Luku 2) kerrottiin, tietoturvapolitiikka jaetaan hierarkisesti ylä- ja alatason tietoturvapolitiikoihin organisaation linjan mukaisesti. Ylätason tietoturvapolitiikassa määritellään organisaation johdon lausunto siitä mikä on organisaation tieto-omaisuus ja kuinka se suojataan. Lisäksi ylätason tietoturvapolitiikassa määritellään ketkä ovat vastuulliset tiedon turvaamisen kannalta. Alemman tason tietoturvapolitiikka noudattaa ylätason tietoturvapolitiikan linjauksia. Lähestymistapa kuitenkin poikkeaa. Alatason tietoturvapolitiikka määrittelee toimintatavat, kuinka organisaatiossa työskennellään tietoturvallisesta. Nämä ylä- ja alatason tietoturvapolitiikat voidaan suunnitella siten, että on malli, jonka mukaisesti tietoturvapolitiikka toteutetaan. (Baskerville ym. 2002.)

Tässä kontekstissa on tärkeää ottaa huomioon, että organisaation ominaispiirteet. Se toteutuu Siponen & Puhakainen tietoturvapolitiikan kehittämismallissa. Tietoturvapolitiikan kehittämismalli koostuu neljästä lähtökohdasta (Siponen ym. 2015.)

Lähtökohta1. Tietoturvapolitiikan kehittämisen menetelmät tulee olla johdettuna teoriasta. Kuten kaikessa tieteellisessä tutkimuksessa, se perustuu teorioihin, joka on tieteen filosofinen luonne. (Siponen ym. 2015.)

Lähtökohta 2. Tietoturvapolitiikan kehittämisen mallin tulee sisältää empiiristä tietoa, koska se on lähtökohta ja tieteen perusajatus. Sen vuoksi empiiristä tietoa pidetään tärkeänä osana tieteessä. (Siponen ym. 2015.)

Lähtökohta 3. Tietoturvapolitiikan kehityksessä täytyy ottaa huomioon organisaation ominaispiirteet. Tämä lähtökohta juontaa juurensa teorioista, joiden mukaan ei voida tuottaa yhtä tapaa toteuttaa tietoturvapolitiikkaa organisaatiossa. (Siponen ym. 2015.)

Lähtökohta 4. Menetelmän tulee sisältää toimintatavat, kuinka tietoturvapolitiikkaa ja tietoturvaprosesseja kehitetään ja ylläpidetään. Tämän lähtökohdan ajatuksena on luoda politiikka politiikan sisälle, jossa on ohjeet siitä, kuinka organisaatio suunnittelee ja ylläpitää tietoturvapolitiikkaa. Siinä määritellään myös vastuut ja kuinka tietoturvapolitiikka hyväksytään ja julkaistaan. (Siponen ym. 2015.)

Lähtökohdassa 2 määritetään, että organisaatiot ovat toisistaan erilaisia sekä niiden toimintaympäristöltään että ominaisuuksiltaan. Tämän vuoksi on tärkeää että otetaan huomioon organisaatioiden vaatimukset tietoturvapolitiikalle toteutettaessa tietoturvapolitiikkaa. (Siponen ym. 2015.)

4. Tutkimusmenetelmät ja tutkimusympäristö

Tässä luvussa esitetään tutkimusmenetelmästä, toimintatutkimuksesta ja tutkimusympäristöstä. Tutkimus toteutettiin vuosien 2012 - 2015 aikana Pohjois-Pohjanmaan sairaanhoitopiirissä.

4.1. Tutkimusmenetelmät

Toimintatutkimuksen avulla selvitetään tosielämän ongelmia teorian avulla (Chiasson, Germonprez & Mathiassen 2012). Toimintatutkimus on myös erittäin soveltuva menetelmä, kun organisaation tilannetta parannetaan tieteen keinoin (Davison, Martinsons & Ou 2012). Tutkimuksen tarkoituksena on selvittää, kuinka Siposen ja Puhakaisen tietoturvapolitiikan kehittämismallia toteutetaan ja kehitetään käytännössä. Tutkimustehtävä määrittää, millä menetelmällä tutkija saa vastauksia kysymyksiinsä (Syrjäläinen, Eronen & Värri 2007).

Aiemmin keskusteltiin kriittisesti laadullisesta (kvalitatiivinen) ja määrällisestä (kvantitatiivinen) menetelmästä, mutta Syrjäläisen ja muiden (2007) mielestä nykyään niitä ei nähdä toisiaan poissulkevana. Laadullisen tutkimuksen on ajateltu olevan eräänlaista esitietotutkimusta ja myöhemmin tehty määrällinen tutkimus on varsinaista tutkimusta. (Syrjänen ym. 2007).

Luvussa (2) kerrottiin, että kaiken tieteellisen tutkimuksen tulee perustua teorioihin, kokoelmaan selittäviä käsitteitä, se on tieteen filosofinen luonne. (Metsämuuronen 2009). Cuba ja Lincoln (2000) vertasivat tutkimuksen tekemisen paradigmoja keskenään. Paradigmat voi selittää siten, että ne ovat perususkomuksia, malleja tai selityksiä tutkittavasta ilmiöstä, jolla ei ole teorianomaista hyväksyntää. Paradigmat perustuvat ontologisiin (oppi olevaisesta), epistemologisiin (oppi tiedosta ja sen olemuksesta) ja metodologisiin (oppi tiedon hankinnan menetelmistä) (Metsämuuronen 2009.)

Tutkimustoiminnan näkökulmia näihin paradigmoihin Cuba ja Lincoln (2000) ovat positivismi (objektiivisuus, toistettavuus on totuus), postpositivismi (objektiivisuus, toistettavuus saattaa olla totuutta), kriittinen teoria (subjektiivisuus eli tutkijan arvot vaikuttavat lopputulokseen, tutkijan ja tutkittavan dialogilla hankitaan tieto) ja konstruktivismi (todellisuus on suhteellista, subjektiivisuus, tiedon hankinta perustuu tulkintaan). Kriittinen teoria ja konstruktivismi ovat tyypillisiä laadulliselle tutkimukselle. (Metsämuuronen 2009.)

Laadullisesta tutkimuksesta käyty kriittinen keskustelu perustuu siihen, että sillä ei ole omaa paradigmaa tai teoriaa, kokoelmia selittäviä käsitteitä (Metsämuuronen 2009), mutta sillä on **taustateoria** (aineistoa tarkastellaan sen avulla) ja **tulkintateoria** (ohjaa tutkijan valintoja siitä, mitä aineistosta etsii) (Eskola ym. 2000). Anttilan (2006) mukaan kvalitatiiviselle tutkimukselle on neljä laadullista tavoitetta: ilmiöiden ymmärtäminen, niiden selittäminen ja tulkinta sekä soveltaminen käytäntöön.

Hirsijärvi, Remes & Sajavaara (2012) sekä Tuomi (2007) ovat koonneet ominaispiirteitä laadullisella tutkimuksella:

- Tutkimus on kokonaisvaltaista tiedonhankintaa, aineisto kerätään todellisissa tilanteissa, tiedon keruun kohteena ovat ihmiset
- Suositaan aineiston hankintaa, joissa tiedonantajien ”ääni” ja näkökulmat tulevat esiin, metodit ovat laadukkaita
- Tiedonantajat tai tietolähteet valitaan tarkoituksen mukaisesti, ei satunnaisotoksella
- Tiedon keruu ja tutkimus toteutetaan joustavasti ja suunnitelmia voi muuttaa
- Aineistoa tarkastellaan monitahoisesti ja yksityiskohtaisesti, ei vaan teorian ja hypoteesin testaamista
- Tuloksia ei yleistetä, vaan käsitellään ainutlaatuisina ja aineistoa tulkitaan sen mukaan

Edellä mainitut Hirsjärven ja muiden (2012) sekä Tuomen (2007) esittämät yhteiset piirteet vaikuttivat siihen, miksi tässä tutkimuksessa valittiin laadullinen tutkimus. Siinä painottui muun muassa se, että tiedonantajien ”ääni” ja näkökulmat saadaan kuuluumaan PPSHP:n sairaanhoitopiirin tietoturvapolitiikkaan liittyvissä vaatimuksissa.

Tutkimukseen valittiin toimintatutkimus, koska tarkoituksena oli kehittää ja toteuttaa tietoturvapolitiikkaa Siponen ym. (2015) tietoturvapolitiikan kehittämismallin mukaisesti. Tietoturvapolitiikka oli käytännössä, tutkimuskohteen organisaatiossa, todettu ongelma tai sitä pyrittiin kehittämään paremmaksi (Metsämuuronen 2009), ja Kanasen (2009) mukaan tuloksena voi olla esimerkiksi uuden tuotekonseptin kehitys. Seuraavaksi kerrotaan toimintatutkimuksesta enemmän.

4.2. Toimintatutkimus

Tämän tutkimuksen tutkimusmenetelmäksi on valittu toimintatutkimus, sillä jaottelussa toimintatutkimus on lähempänä kvalitatiivista kuin kvantitatiivista tutkimusta (Kananen 2009).

Toimintatutkimuksesta (action research cycle, ARC) on esitetty erilaisia määritelmiä kirjallisuudessa. Metsämuurosen (2009) mukaan se tarkoittaa pienimuotoista interventiota, joka tehdään todellisessa maailmassa (Metsämuuronen 2009), mutta se on ajallisesti haastavaa (Vilkka 2006). Toimintatutkimuksen avulla siis selvitetään tosielämän ongelmia teorian avulla, ja kehitetään olemassa olevaa käytäntöä (Metsämuuronen, 2009; Ciasson, Germonprez & Mathiassen 2012). Toisin sanoen toimintatutkimuksen tarkoituksena on saada aikaan muutos työelämän ongelmiin (Kananen 2009). Toimintatutkimuksen avainsanoja ovat auttaa muuttamaan todellisuutta, reflektiivisyys eli tutkitaan aikaansaamia muutoksia, käytännönläheisyys ja ihmisten osallistuminen (Heikkinen & Jyrkämä 1999).

Toimintatutkimus on lähtökohdiltaan toimintatieteeseen liittyvää, joka tähtää organisaatioiden toiminnan tutkimiseen ja kehittämiseen käytännössä (Mäntylä 2007). Kuuselan (2005) mukaan tutkija voi toimia yhdessä yhteisön, esimerkiksi organisaation, jäsenten kanssa (Kuusela 2005), edellä mainitusta on noussut myös kritiikkiä, koska

tutkija on osa yhteisöä, ja voi siten tehdä muutosehdotuksia sekä toteuttaa niitä. Lisäksi tiedonantajien ja tutkijan välillä ei ole tasavertaista dialogia. Tutkijalle voi tulla tutkimuksen aikana rooliristiriita siitä, minkä verran hän saa osallistua toimintatutkimukseen. Tutkijan on pidettävä huoli koko tutkimuksen ajan, asiantuntijan roolissa, ettei ohjaa interventioita yksin. (Kuula 1999; Kananen 2009.)

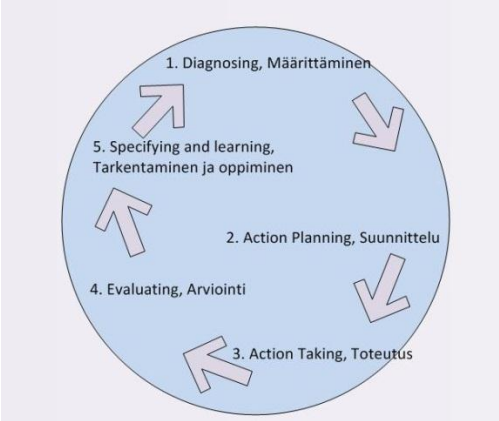
Kritiikkiä on aiheuttanut myös toimintatutkimuksen tutkimuskohde, joka on johonkin tilanteeseen sidottu tietty ryhmä, otos on rajallinen eikä edustava, ei pystytä kontrolloimaan muuttujia eikä tuloksia voida yleistää. Joskus on voinut käydä, ettei teoriaa ja käytäntöä ole voitu yhdistämään toisiinsa, ja tutkijat eivät ole kyenneet hyödyntämään toisten saamia tuloksia. (Metsämuuronen 2009.)

Edellä mainituista arvosteluista huolimatta Kananen (2009) tuo toimintatutkimuksesta esille etuja. Työyhteisöllä on toimivat suhteet ”tutkittavaan ilmiöön”, tässä tutkimuksessa tietoturvapolitiikka. He voivat paremmin testata toimintamalleja ilman ulkopuolista apua, ja toimintatutkimus tukee työelämän muutosprosesseja, jolloin hierarkkisuus voi vähetä, kun pyritään matalampiin organisaatiorakenteisiin. Lisäksi verkostoituminen lisääntyy, elinikäistä oppimista tapahtuu ja tiimityöskentely sekä itseohjautuvuus lisääntyvät eri organisaatioissa. (Kananen 2009.)

Toimintatutkimuksen vaiheita esitetään monella tavalla. Perusajatus niillä kaikilla on sama: ongelman määrittely esimerkiksi arkipäivän tilanteesta nouseva, ratkaisun esitys muun muassa neuvotellen asiasta kiinnostuneiden kanssa, ratkaisun kokeilu ja arviointi esimerkiksi ongelman muokkaaminen ja uudelleen määrittely ja uuden ratkaisun testaaminen. Tärkeää on muistaa arviointikriteerien määrittely. (Kananen 2009; Metsämuuronen 2009.)

Tämä toimintatutkimus toteutettiin iteratiivisen prosessin mukaan. Tämän avulla voitiin tarkastella syntyvää tietoturvapolitiikkaa, ja arvioida toteutuiko sille asetetut vaatimukset. Tietoturvapolitiikka tullaan toteuttamaan vaiheittain, jolloin voidaan tarkastella tietoturvapolitiikan sopivuutta kyseiseen organisaatioon ja vaadittuun kontekstiin.

Baskerville (1999) määrittää toimintatutkimukseen vaiheet, joita voidaan toteuttaa iteratiivisesti. Vaiheet ovat: diagnosing (1), action planning (2), action taking (3), evaluating (4) specifying learning and learning (5). Kuviossa 5 on kuvattuna vaiheet. (Baskerville 1999.)



KUVIO 5. Toimintatutkimuksen (ARC) vaiheistus mukaillen Baskervilleä (1999)

Iteratiivisen prosessin mukaisesti lopputuloksen arviointi on keskeinen vaihe. (Baskerville 1999.)

Tämä tutkimus toteutettiin toimintatutkimusmenetelmänä iteratiivisen vaiheistuksen mukaisesti. Sen avulla voitiin tarkastella syntyvää tietoturvapolitiikkaa ja arvioida toteutuiko sille asetetut vaatimukset. Oli myös perusteltua käyttää toimintatutkimusta tutkimusmenetelmänä, koska siinä yhdistettiin organisaation toimintaympäristö ja tietoturvapolitiikan kehittämismalli. Kappaleessa 4/5 selitetään prosessia enemmän.

4.3. Tutkimusaineiston kerääminen

Tässä tutkimuksessa aineisto hankittiin haastattelulla ja tutkimalla organisaation strategiaa ja terveydenhuollon tietoturvaa ja tietosuojaa velvoittavaa lainsäädäntöä. Haastattelut tiedonkeruumenetelmänä laadullisessa tutkimuksessa on yleinen menetelmä, erityisesti tiedon tutkimus- ja kehittämistöissä (Myers & Newman 2007).

Tässä tutkimuksessa käytettiin teemahaastattelua. Siinä on etukäteen mietityt teemat ja niihin liittyvät tarkentavat kysymykset, joilla ei ole tarkasti määriteltyä kysymysten muotoa ja esittämisjärjestystä (Metsämuuronen 2009).

Haastattelu mahdollistaa perustellumman tiedonkeruun, koska tutkija osallistuu yhteistyössä tiedonkeruu prosessiin (Schultze & Avital 2011). Turner määrittää kolme haastattelu menetelmää, joita ovat vapaamuotoinen keskusteleva haastattelu (informal conversational interview), ohjaava lähestyminen yleiseen haastatteluun (general interview guide approach) ja yhdenmukainen avoin haastattelu (standardized open-ended interview) (Turner 2010).

Vapaamuotoisessa keskustelevassa haastattelussa tutkija esittää kysymyksiä, jotta hän ymmärtäisi paremmin tutkimuskohdettaan. Tutkijalla ei tarvitse olla etukäteen valmisteltuja strukturoituja kysymyksiä. Kun tutkija puolestaan haluaa ohjata haastateltavaa, hän valitsee ohjaavan lähestyminen yleiseen haastatteluun. Tällöin tutkija saa strukturoituihin kysymyksiin vastaukset mutta haastattelussa on tilaa myös keskustelevampaan haastatteluun. Tällöin haastattelijalla on mahdollisuus esittää jatkokysymyksiä haastateltavalle. Yhdenmukainen avoin haastattelu on tarkoin strukturoitu siten, että kysymykset ovat yhdenmukaisia mutta vastaukset voidaan antaa avoimesti. Tämän menetelmän avulla tutkija saa tarkentavaa tietoa tutkimuksen kohteesta. (Turner 2010.)

Haastatteluissa selvitettiin tietoturvapolitiikan vaatimukset. Haastattelun kysymykset nousivat Siponen ym. (2015) tietoturvapolitiikan kehittämismallista (LIITE A). Haastattelussa selvitettiin organisaation liiketoiminnasta kohdistuvat vaatimukset ja organisaation liiketoimintaympäristöstä nousevat vaatimukset. Lisäksi haastatteluiden avulla selvitettiin organisaation tieto-omaisuus. Haastatteluita toteutettiin koko iteratiivisen prosessin ajan, kun ylä- ja alatason tietoturvapolitiikoita testattiin. Haastattelut myös analysoitiin ylä- ja alatason tietoturvapolitiikan mukaisesti. Haastatteluiden vastaukset analysoitiin sisältöanalyysin mukaisesti ja haastattelut teemoitettiin (Eskola & Suoranta 1998).

4.4. Tutkimusympäristö

Tutkimus toteuttiin PPSHP:ssä. Jokainen kunta kuuluu sairaanhoitopiiriin ja sairaanhoitopiirin omistajana ovat nämä kunnat, jotka muodostavat kuntayhtymän. Sairaanhoitopiirin kuntayhtymä solmii perussopimuksen, jossa on määritelty, kuinka omistus jaetaan ja kuinka päätökset tehdään. Sairaanhoitopiirin vastuulla on tuottaa julkista terveydenhoitoa alueensa kunnille, jotka rahoittavat sairaanhoitopiirin toiminnan julkisilla verovaroilla.

Pohjois-Pohjanmaan sairaanhoitopiiriin kuuluu 29 kuntaa. Kuvassa 1 on PPSHP:n sairaanhoitopiirin jäsenkunnat.

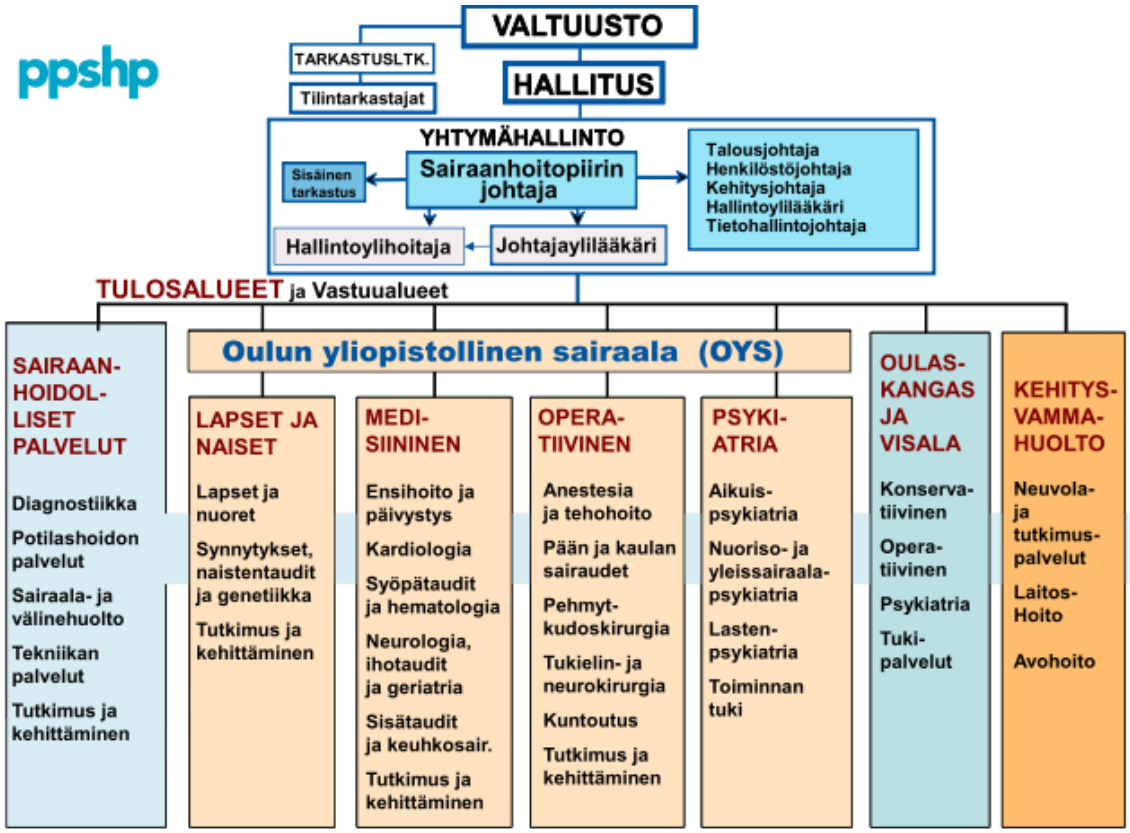
KUVA 1. *PPSHP:n jäsenkunnat.*

4.4.1. Organisaatiorakenne

PPSHP:n tehtävä on järjestää ja tuottaa erikoissairaanhoidon palveluja. Sairaanhoitopiiriin kuuluu Oulun yliopistollinen sairaala ja sen vuoksi organisaatiolla on opetus ja tutkimustoimintaa.

PPSHP:n organisaatiorakenne koostuu seuraavista toimintayksiköistä: Sairaanhoidolliset palvelut, Oulun yliopisto sairaala, Oulaskankaan ja Visalan sairaalat

sekä Tahkokankaan kehitysvamma huolto. Hallinto pitää sisällään talous- ja henkilöstöhallinnon sekä tietohallinnon. Kuviossa 6 on PPSHP:n organisaatiorakenne.



KUVIO 6. *PPSHP:n organisaatiorakenne.*

Kaikista toimintayksiköissä on organisaation toiminnan kannalta kriittistä tietoa, joka tulee ottaa huomioon toteutettaessa tietoturvapolitiikkaa. Lisäksi Siponen ym. (2015) tietoturvapolitiikan kehittämismallin mukaisesti organisaation on kyettävä toteuttamaan strategiaansa turvallisesti (Siponen ym. 2015). Tämän vuoksi kappaleessa 4.4.2 on kuvattuna tärkeimmät kohdat PPSHP:n strategiasta.

4.4.2. Pohjois-Pohjanmaan sairaanhoitopiirin kuntayhtymän strategia

PPSHP ja Oulun yliopistollinen sairaalan tavoite on tuottaa ja järjestää kansallisia terveyspalveluja alueellaan ja tarjota erikoissairaanhoidon palveluja korkeatasoisesti kaikissa tilanteissa koko Pohjois-Suomen alueelle. Toiminta perustuu arvoille ja eettisille periaatteille, joita ovat: ihmisarvot, vastuullisuus, oikeuden mukaisuus ja uudistuskyky ja avoimuus.

PPSHP työskentelee yhteistyössä eri organisaatioiden kanssa. Se kehittää palveluverkostoja perusterveydenhuollon ja muiden sairaanhoitopiirien kanssa. Palveluketjut muodostetaan sosiaalipalveluiden, konsultointiin kehittämisen ja etäpalveluiden työnjaon järkevöittämiseksi.

PPSHP toteuttaa toiminnassaan yhteistyötä eri organisaatioiden kanssa. Se kehittää palveluketjuja yhteistyössä perusterveydenhuollon ja muiden sairaanhoitopiirien kanssa. Palveluketjut toteutetaan järkevän työnjaon järjestämiseksi, kehittäen konsultointitoimintaa sekä etäyhteysratkaisuja toiminnan tukemiseksi. Yhteistyö eri organisaatioiden välillä toteutetaan mittaamalla kuinka hyvin palvelut on järjestetty väestön tarpeiston näkökulmasta. Rahoituksen hallinnan onnistuminen mitataan luottamuksellisen yhteistyön onnistumisella ja taloudellisen tuloksen sekä kuntalaisten kansallisen yhdenvertaisuuden toteutumisella. PPSHP on innovatiivinen organisaatio. Se osallistaa yliopistosairaalan kehityksen, korkeatasoiset palvelut ja pohjoisen Suomen kuntalaiset.

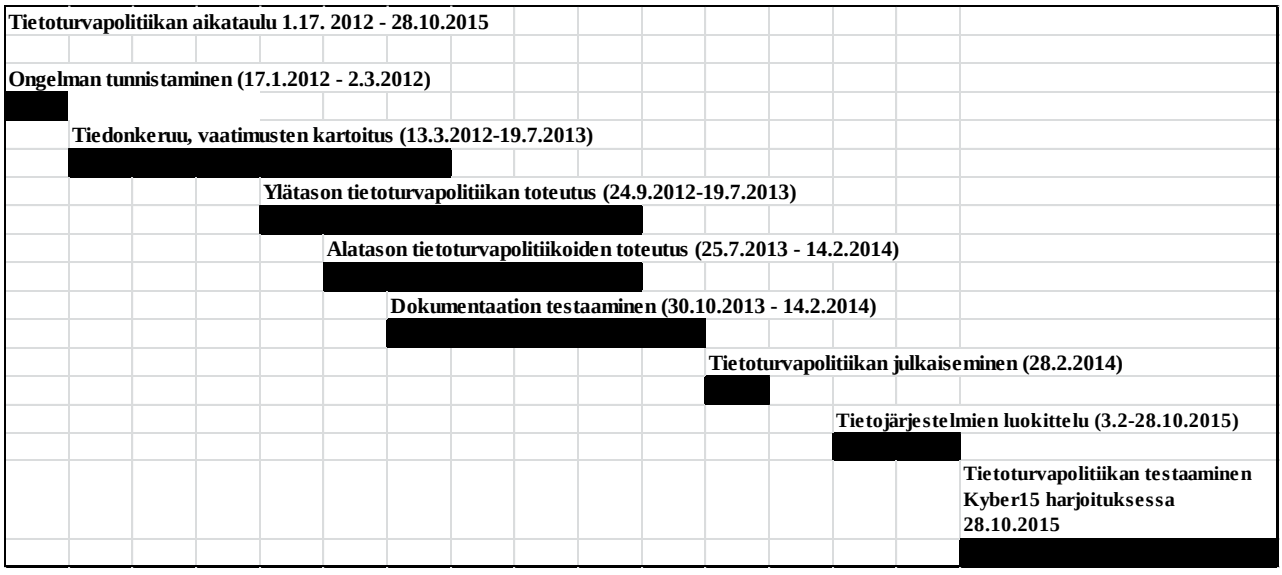
PPSHP edistää ilmapiiriä, jossa on korkeatasoinen asiantuntemus ja se heijastaa toimintaa sekä tukee strategisia tavoitteita Sairaanhoitopiirissä. Sairaanhoitopiirissä on turvallinen ja terve toimintaympäristö. Henkilökunta osallistetaan toiminnan ohjaukseen, suunnitteluun ja kehittämiseen kaikilla toiminnan tasoilla.

5. Tietoturvapolitiikan kehittäminen Siponen & Puhakainen tietoturvapolitiikan kehittämismallin mukaisesti

Tietoturvapolitiikka toteutettiin vuoden 2013 aikana. Tietoturvapolitiikka toteutettiin Siponen ym. (2015) tietoturvapolitiikan kehittämismallin mukaisesti toimintatapaustutkimusmenetelmää käyttäen. Vaiheistuksen mukaiset toimet toteutettiin ja tässä tutkimuksessa se eteni seuraavasti: Tunnistettiin organisaation ominaispiirteet ja vaatimukset tietoturvapolitiikalle. Kun edellä mainitut vaatimukset oli tunnistettu, luetteloitiin organisaation tieto-omaisuus ja luokitellaan se organisaation toiminnan kannalta kriittisyyden mukaisesti. Näiden toimien jälkeen tietoturvapolitiikat toteutettiin ja testattiin. Politiikoiden toteuttamisessa ja testaamisessa hyödynnettiin organisaation työntekijöitä ja kuunneltiin heidän kannanottonsa. Testaamisen tarkoituksena oli toteuttaa sellaiset tietoturvapolitiikat, jotka ovat ymmärrettäviä ja luettavia. Viimeisessä vaiheessa arvioitiin tietoturvapolitiikat. (Siponen ym. 2015.)

Siponen ym. (2015) tietoturvapolitiikan kehittämismallin mukaiset vaiheet toteutettiin PPSHP:ssä käytännössä, joten työn toteutukseen käytetty aika oli 2012-2015. Taulukosta 1 on luettavissa työn toteutuksen aikataulu.

TAULUKKO 1: *Toteutuksen aikataulu*



Tässä tutkimuksessa sovellettiin toimintatutkimusmenetelmän mukaista vaiheistusta ja Siponen ym. (2015) tietoturvapolitiikan kehittämismallia. Kuviossa 7 on kuvattuna miten edellä mainitut on yhdistetty.

KUVIO 7. *Tietoturvapolitiikan toteuttaminen toimintatapausvaiheistuksen mukaisesti.*

Koko iteratiivisenprosessin ajan arvioitiin, että lopullinen tavoite täyttyy, eli organisaation tärkein tieto-omaisuus voidaan turvata, ilman että siitä se aiheuttaa työntekijöille suurta haittaa ja organisaatio voi toteuttaa strategiaansa ilman tietoturvapoikkeamia.

5.1. Tietoturvapolitiikan vaatimusten kartoitus

Toimintatapaustutkimusmenetelmän vaiheessa 1. Diagnosin, Määrittäminen (kuviossa 7) tunnistettiin Siponen ym. (2015) mukaisesti vaatimukset tietoturvapolitiikalle. Vaatimukset ovat: **organisaation sisäisiä**, esimerkiksi organisaation strategiasta peräisin, sekä **organisaation ulkopuolelta** peräisin olevia vaatimukset, esimerkiksi lainsäädännöstä nousevat vaatimukset organisaatiolle. Vaiheessa 1. Diagnosin, Määrittäminen tunnistettiin myös organisaation ominaispiirteet, organisaation tärkeimmät toiminnot ja tieto-omaisuus. Näiden tietojen keräämistä varten tutkimuksessa haastateltiin organisaation avainhenkilöitä ja tutustuttiin organisaation strategiaan. Ulkoisia vaatimuksia tietoturvapolitiikkaan kerättiin tutustumalla terveydenhuollon tietoturvaa ja tietosuojaa velvoittavaan lainsäädäntöön (Liite B).

Terveydenhuollon organisaatiorakenne on erityinen ja poikkeaa muista organisaatiosta, erityisesti organisaatiorakenteen ja johtamisen osalta. Lisäksi henkilökunta noudattaa

tiukasti arvoja, perinteitä ja käyttäytymistä, jotka periytyvät henkilökunnan keskuudessa. (Seren & Baykal 2007). Julkinen terveydenhuollon organisaatio on voittoa tavoittelematon organisaatio, joka rahoitetaan julkisilla verovaroilla. Lisäksi julkisella terveydenhuollolla on aina enemmän kysyntää kuin tarjontaa, joka on organisaatiolle erityinen piirre.

PPSHP on julkinen terveydenhuollon organisaation, jonka toimintaa säätelee terveydenhuoltoa säätelevät lait ja valvovat viranomaiset. Lisäksi kunnat, jotka kuuluvat Pohjois-Pohjanmaan kuntayhtymään valvovat sairaanhoitopiirin toimintaa. Nämä on määritelty organisaation strategiassa, joiden huomioonottaminen on vaatimuksena toteutettaessa tietoturvapolitiikkaa (Siponen ym. 2015).

5.1.1. Lainsäädännön vaatimukset tietoturvapolitiikkaan

Laki säätelee voimakkaasti terveydenhuollon viranomaisen toimintaa ja sitä, kuinka organisaatiot käsittelevät tietoaan. Lainsäädäntöä tarkasteltaessa nousee esille kaksi tiedon luokkaa: potilasasiakirjat ja viranomaisen asiakirjat. Potilasasiakirjoja tai potilastietoa syntyy kun organisaatiossa hoidetaan potilaita. Viranomaisen asiakirjoja tai viranomaistietoa syntyy kun organisaatio toteuttaa viranomaisen tehtävää organisaatiossa.

Potilasasiakirjat ovat salassa pidettävää tietoa. Tämä on kirjattu useaan eri lakiin ja mikään laki ei sulje toistaan pois. Esimerkiksi Laki potilaan asemasta ja oikeuksista (785/1992) määrittää, että terveydenhuollon ammattihenkilöt, jotka osallistuvat potilaan hoitoon tai potilaan hoitoon osallistuvat eivät saa ilman lupaa paljastaa yksityisen ihmisen tai perheen salaisuutta, jonka hän on asemansa tai tehtävän perusteella saanut tietoon. Salassapitovelvollisuus säilyy ammatinharjoittamisen jälkeenkin. (Laki potilaan asemasta ja oikeuksista (785/1992).)

Julkisen viranomaisen asiakirjat ovat julkisia, jos asiaa ei ole määritelty salaiseksi. Näin määritellään laissa Laki Viranomaisen toiminnan julkisuudesta (621/199). Hyvä hallintotapa velvoittaa julkisia viranomaisia toimimaan avoimesti ja julkisesti, jotta voidaan seurata, miten julkisin varoin rahoitettua toimintaa hoidetaan. Laki Viranomaisen toiminnan julkisuudesta määrittää, mitkä tiedot voidaan määrittää salaiseksi ja kuinka pitkäksi aikaa. (Laki viranomaisen toiminnan julkisuudesta (621/199).)

Tätä tutkimusta varten tutustuttiin 29 lakiin, jota velvoittavat julkista terveydenhuollon viranomaista tietoturvan ja tietosuojan osalta. Tietoturvapolitiikkaan velvoittava lainsäädäntö on liitteessä B.

5.1.2. Tietoturvapolitiikan vaatimukset organisaation strategiasta

Tunnistettaessa niitä vaatimuksia tietoturvapolitiikalle, jotka nousevat ia organisaation sisältä. Siponen ym. (2015) tietoturvapolitiikan kehittämismallin mukaisesti on tärkeää, että organisaatio toteuttaa liiketoimintastrategiaa ilman tietoturvaongelmia (Siponen ym. 2015). Sen vuoksi tässä tutkimuksessa tutustuttiin organisaation strategiaan. Lisäksi organisaation johtoa haastateltiin, jotta saatiin kattava kuva organisaation strategiasta.

Haastatteluja toteutettiin tässä vaiheessa seitsemän kappaletta seitsemän. Haastateltavia valittaessa tavoitteena oli saada riittävä edustus organisaation johdosta, jotka ovat tekemisissä tietoturvan- ja tietosuojan parissa. PPSHP:ssä on vähän henkilöitä, jotka edustavat tätä joukkoa. Sen vuoksi haastateltavien määrää voidaan pitää riittävänä. Yhtä organisaation edustajaa haastateltiin kolme kertaa, jotta saatiin esiin riittävä tieto tietoturvapolitiikan vaatimuksista. Kolme haastattelua jouduttiin aikataulullisista syistä toteuttamaan sähköpostihaastatteluna, koska kasvokkain tapahtuvaan haastatteluun ei ollut mahdollisuutta. Kuitenkin haluttiin ottaa näiden henkilöiden asiantuntemus huomioon tietoturvapolitiikan vaatimuksia kartoitettaessa. Kysymykset ovat liitteessä B. Haastattelussa oli tilaa myös keskustelulle, näin saatiin kattavasti esiin haastateltavan asiantuntemus tietoturvapolitiikalle.

Seuraavassa esimerkkejä haastatteluista, joissa nousevat esiin organisaation ominaispiirteet, tärkeimmät toiminnot ja tieto-omaisuus. Seuraavassa eräs haastateltava kuvaa organisaation toimintaympäristön vaatimuksia tietoturvapolitiikalle:

> *”Meillähän on lakisääteinen perustehtävä. Meillä on periaatteessa useampikin laki mikä siinä taustalla on, … terveydenhuoltolaki,.. erikoissairaanhoitolaki. Meidän perustehtävä on taata kolme pääprosessia,.. potilaidenhoito, ja tutkimus ja koulutus”*

> *”…sitten meillä on vastuuta myös erikoisvastuualueesta.. Meidän lisäksi neljän sairaanhoitopiirin alueella täällä pohjoisessa toimiva kokonaisuus. Keski-pohjanmaa, Kainuu ja Lappi, meillä on aika paljon toimintoja, jotka on keskitetty tänne... Meillä on vielä kansallisia erityistehtäviä muutamia ja jotka on keskitetty tänne Ouluun, jonkun muun yliopistollisen sairaalan rinnalle, että niistä tämä kokonaisuus muodostuu. Me ollaan nykyisen lainsäädännön mukaan yhä enemmän, koordinoiva, yhä enemmän vastuuta omasta alueesta, että ja erityisvastuualueesta on myös vähän enemmän kuin aikaisemmin. Sellaisessa pelikentässä me täällä toimitaan. Varsinaista liiketoimintasuunnitelmaahan ei terveydenhuollon julkiselle organisaatiolle laadita.. se on strategia.”*

Kaikki haastateltavat yhtyivät edellä mainittujen organisaation pääprosesseihin mutta kaksi haastateltavaa mainitsivat haastattelussa opetuksen ja koulutuksen, kosta organisaatiossa on yliopistollinen sairaala:

> *”Meidän päätehtävä on varmistaa kolme pääprosessia potilaan hoito, tutkimus ja koulutus.”*

”Luonnollisesti perustehtävä lähtee sairaanhoitopiirille annetusta lakisääteisestä tehtävästä, joka on potilaan hoitoon liittyvät tehtävät. Sen lisäksi meillä on koulutukseen ja tutkimukseen liittyvät tehtävät. ”

”Kaikki toiminnot lähtevät potilaan hoidosta. Se on meidän tulos ja kaikki tähtää siihen.”

Haasteellista oli saada tieto organisaation strategian pääkohdista. Kaksi haastateltavaa ja nostivat seuraavia pääkohtia esiin.

”Yhteistyö on tärkeä, koska Sairaanhoitopiiri organisaationa ei tule tästä kasvamaan ja joudumme hoitomaan yhä sairaampia potilaita, sen vuoksi joudumme luopumaan joistain tehtävistä.”

”Mitä tulee tehtävien vastuun jakoon, eri organisaatioiden välillä, me olemme tekemisissä lainsäädännöllisten velvoitteiden kanssa. Yleistettäessä todetaan että yhteistyö perusterveydenhuollon ja erikoissairaanhoidon kesken on rajattua, koska meillä on tiukka lainsäädäntö. Siitä kuitenkin voidaan löytää vaihtoehtoja yhteistyölle, jos sille on halua.”

Kaikki haastateltavat nimesivät potilastiedon organisaation tärkeimmäksi tiedoksi. Haastatteluissa kaikilla haastateltavilla oli oma näkemyksensä potilastiedon salassa pitoon, eheyteen ja saatavuuteen.

”M*eillähän on lainsäädäntö, joka tätä hallitsee ja ohjaa ja sitä tulkitaan tietosuojavaltuutetun toimesta ja tietysti oikeuslaitoksen toimesta. Kaikkein kriittisintähän on tähän potilaan hoitoon liittyvät tiedot… Ja ne ovat kategoriassa yksi jos näin päin tätä tietoa ajatellaan. …Tietysti sen tiedon saatavuus on turvattava kaikissa olosuhteissa ja kovin pitkään ei pystytä toimimaan ilman noita järjestelmiä ja tietoja. No sitten toiminnan.. muut ohjauksellliset tiedot, ole tietoturvan ja tietosuojan kannalta ollenkaan niin kriittisiä, että talous tiedot ei ole niin, kriittisiä. Ollaan julkinen organisaatio, ne tiedot ovat aikalailla julkisia. Mielellään me omistajien kanssa niitä asioita käsitellään, hyvin mielellään, sehän on poliittisen teon päätöksen pohjana.*

“Lähtökohtana on, että julkisen viranomaisen tiedot ovat julkisia ja potilastiedon ovat salassa pidettäviä.”

“Kyllähän se potilaan hoidon kannaltahan se on korvaamatonta. Täytyy sanoa, että tiedon täytyy olla saatavilla kokoajan. Muuten se toiminto vaarantuu nopeasti. Kyllähän se riippuu tilanteesta. Joskus se ei vaikuta ja joskus se voi vaikuttaa paljonkin. Tuota niin, siihen päätöksen tekoon, jota joudutaan tekemään potilaan osalta. Jos kaikki tiedot eivät ole käytössä voi olla riski että tehdään vääriä päätöksiä potilaan osalta. Sillä tavalla, korkeassa luokassa”

*”*S*anoisin, että se muuttuu yhä tärkeämmäksi ja tärkeämmäksi. Myös yhteiskunnan muutoksen myötä, mutta myös ihmiset aivan erilailla, he*

myös tiedostavat oikeuksiaan. Ainahan potilastietojen turvaaminen ja suojaaminen on ollut tärkeää. Mutta se asenneilmasto on muuttunut siihen suuntaan, että yksityisyyttä suojataan yhä enemmän ja ihmiset ovat tietoisia oikeuksistaan. Meillä on myös lainsäädännön velvoite… Sitten pitää muistaa, että ihmiset, jotka tulee meille ovat jollainlailla haavoittuvassa asemassa. Sellainen ihminen, joka on haavoittuvassa asemassa ja miten syvälle nämä potilastiedot menee se on se ensiarvoisen tärkeää. Sitten pitää myös suojella meidän omaa imagoa. Mutta sitten myös miten meidän palvelu koetaan. Tietosuoja on myös sitä."

"Yksi olennainen syy tiedon oikeellisuuteen on potilasturvallisuus. Toki lainsäädäntö tuo eheys ja oikeellisuus vaatimuksia mutta ne kaikki tukevat sitä potilasturvallisuutta, että potilaita hoidetaan oikein ja ne saavat oikeanlaisen hoidon…"
"Lainsäädännöllä ja meidän omalla toiminnalla pyritään turvaamaan potilasturvallisuus ja joskus tulee lieve ilmiöitäkin. Mutta me ollemme julkinen organisaatio ja meidän kuuluu nekin asiat hoitaa"

"On mitä asetuksessa määrätään, miten oikeita niiden pitää olla… Keskushallinnon asiakirjoille ei ole salassapitovelvoitetta, nehän ovat julkisia, samoin hallituksen ja viranhaltija päätösten, joissa se asia on julkinen. Sitten jos asia on salainen, nämä asiakirjatkin ovat salaisia. Henkilöstöhallinnon tiedoissa on salaisia ja julkisia asiakirjoja"

Haastatteluista esiin nousseet vaatimukset tietoturvapolitiikalle on analysoitu. Sivulla 27 taulukossa 2 on esillä tärkeimmät vaatimukset, jotka nousevat PPSHP:n strategiasta. Taulukossa kuvataan vaatimus strategiasta, kuinka se vaikuttaa tietoturvapolitiikkaan ja viimeisessä sarakkeessa kerrotaan mitä toimia vaatimus aiheuttaa toteutuakseen.

TAULUKKO2. *Strategiasta nousevat vaatimukset organisaation tietoturvapolitiikalle.*

PPSHP:n strategia	**Vaatimus tietoturvapolitiikalle**	**Vaatimuksen toteutus organisaatiossa**
Tehokas terveydenhuolto kaikissa tilanteissa	Toiminnan jatkuvuus kaikissa tilanteissa	Turvataan tietojärjestelmien käytettävyys, tunnistetaan riskit, turvataan kriittiset toiminnot varamenettelyjärjestelyllä.
Alueellinen yhteistyö muiden organisaatioiden kanssa	Turvataan organisaation kriittinen tieto	Solmitaan salassapitosopimukset yhteistyö organisaatioiden kanssa, velvoitetaan PPSHP:n henkilökunta tiedon salassapidon osalta.
Kumppanuus alueen organisaatioiden kesken	Luodaan yhtenäiset tietoturvaperiaatteet alueelle	Kumppanuusorganisaatiot velvoitetaan toimimaan yhteisten tietoturvaperiaatteiden mukaisesti.
Vastuunjako alueen organisaatioiden kesken	Määritellään organisaatioiden vastuut	Tunnistetaan tiedon omistajat ja heidän vastuut.
Vetovoimainen työpaikka ja osaava henkilöstö	Toteutetaan uusia toimintamalleja ja palveluita	Turvataan kaikki toiminnot ja palvelut väärinkäytökseltä tai luvattomalta käytöltä. Vain ne henkilöt saavat ottaa käyttöön uusia toimintoja ja palveluita, joiden työtehtävät sitä vaativat. PPSHPssä huolehditaan että, järjestelmien toimintaa ja käyttöä valvotaan aktiivisesti.

PPSHP:n strategiassa määritellään, että organisaation tehtävänä on turvata ja varmistaa kansallinen terveydenhuolto sen jäsenkunnille ja tarjota kaikissa tilanteissa korkealaatuista erikoissairaanhoitoa koko Pohjois-Suomelle. Kaikki haastattelemani henkilöt totesivat, että potilastieto on organisaation kriittisin tieto, jonka on oltava saatavilla kaikissa tilanteissa. Tämä vaatimus toteutetaan PPSHP:ssä siten, että tietojärjestelmät ovat käytettävissä niille henkilöille, jotka sitä tietoa tarvitsevat. Tunnistetaan tietojärjestelmiin ja potilastietoa sisältäviin aineistoihin kohdistuvat riskit. Lisäksi toimintojen jatkuvuus on turvattu kaikissa tilanteissa. Nämä vaatimukset on todettu myös lainsäädännössä. (Henkilötietolaki (523/1999) ja Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007.)

Alueellinen yhteistyö muiden organisaatioiden kanssa mainittiin haastattelussa. Kun tämä vaatimus huomioidaan tietoturvapolitiikassa, se edellyttää että yhteistyötä tekevät organisaatiot tunnistavat heidän kriittisen tiedon ja suojaavat sen. Vaatimuksen käyttöönotto edellyttää, että yhteistyötä tekevät organisaatiot solmivat salassapitosopimukset ja kouluttavat henkilökunnan salassapidon osalta. Tämän avulla turvataan että yhteistyöorganisaatiot myös tunnistavat kriittisen tiedon, jos sitä joudutaan käsittelemään yhteistyötä tehtäessä.

Kumppanuus ja yhteistyö alueen organisaatioiden kesken nousi esiin haastattelussa ja se on myös luettavissa organisaation strategiassa. Kumppanuus perustuu luottamukselle ja luottamus rakennetaan siten, että organisaatiot voivat luottaa siihen että toimitaan yhteisten pelisääntöjen mukaisesti. Myös Terveydenhuoltolaissa määritellään että Sairaanhoitopiirin organisaatioiden potilasrekisterit muodostavat yhteisen potilasrekisterin, jonka rekisterin pitäjänä toimii jokainen terveydenhuollon organisaatio oman rekisterinsä osalta. (Terveydenhuoltolaki 1326/2012). Tällöin yhteiset pelisäännöt potilastiedon rekisterien ylläpitoon ja potilastiedon turvaamiseen on olennaisessa osassa.

Haastattelussa todettiin, että PPSHP:llä on erityisvastuualue, johon kuuluvat seuraavat sairaanhoitopiirit: Keski-pohjanmaa, Kainuu, Lappi ja Länsi-Pohja. Toimintoja voidaan jakaa näiden organisaatioiden kesken. Jaettaessa toimintoja tulee mahdollisuus keskittää toimintoja tehokkaammin. Tiedon turvaamisen osalta, on huomioitava, että organisaatioiden vastuut on määritelty. Toteutettaessa tämä organisaatiossa tiedolle määritellään omistajat ja vastuut.

PPSHP:n strategiassa ja haastattelussa mainittiin, että Pohjois-Pohjanmaan sairaanhoitopiiri on vetovoimainen työpaikka ja sillä on osaava henkilöstö. Henkilökunta vanhenee ja organisaatio haluaa pitää olemassa olevat työntekijät motivoituneina työntekijöinä. PPSHP:n tavoitteena on myös uusien asiantuntijoiden pitävän organisaatiota vetovoimaisena ja mielekkäänä työpaikkana. Tämä vaatimus velvoittaa esimerkiksi organisaatiota rakentamaan uusia toimintamalleja ja palveluita. Toteutettaessa tämä tietoturvapolitiikassa turvataan kaikki toiminnot ja palvelut väärinkäytökseltä tai luvattomalta käytöltä. Vain ne henkilöt saavat ottaa käyttöön uusia toimintoja ja palveluita, kenen työtehtävät sitä vaativat. PPSHPssä huolehditaan että, tietojärjestelmien toimintaa ja käyttöä valvotaan aktiivisesti.

5.2. Tietoturvapolitiikoiden suunnittelu

Toimintatutkimuksen vaiheessa 2 kuviossa 7, joka on sivulla 22 Action Planning (Suunnittelu), tunnistetaan Siponen ym. (2015) tietoturvapolitiikan kehittämisen mallin mukaisesti organisaation liiketoiminnan kannalta kriittisin tieto-omaisuus. Tässä vaiheessa myös luokitellaan tieto. (Siponen ym. 2015.)

Toimintatutkimuksen vaiheessa 2 myös suunnitellaan ylä- ja alatason tietoturvapolitiikat. Ylä- ja Alatason tietoturvapolitiikoiden suunnittelu toteutetaan organisaation tarpeiden mukaisesti. (Siponen ym. 2015.)

5.2.1. Tieto-omaisuuden tunnistaminen

Siponen ym. (2015) tietoturvapolitiikan kehittämisen mallin mukaisesti tulee varmistua siitä, että organisaation strategian mukaiset tavoitteet täyttyvät ja tieto-omaisuus suojataan sille kohdistuvia uhkia vastaa. (Siponen ym. 2015.) Tässä tutkimuksessa tieto-omaisuus tunnistettiin haastattelussa. Lisäksi PPSHP:n tietohallinnossa käynnistettiin projekti 2015, jonka lopputuloksena syntyi tietojärjestelmien luokittelu. Projekti koostui projektiryhmästä ja ohjausryhmästä.

Projektissa hyödynnettiin tämän tutkimuksen haastatteluaineistoa. Koska tieto on tietojärjestelmissä, projektin tehtävänä oli kartoittaa tietojärjestelmät ja luokitella ne PPSHP:n toiminnan kannalta kriittisyyden mukaan. Projektin ohjausryhmä koostui PPSHP:n tietohallinnon edustajista ja projekti ryhmä koostui PPSHP:n edustajista ja OAMK:n opiskelijoista.

5.2.2. Tieto-omaisuuden luokittelu

Haastatteluiden ja tietojärjestelmien luokitteluprojektin mukaisesti tietojärjestelmät luokiteltiin seuraavasti taulukon 3 mukaisesti.

TAULUKKO 3. *Tietojärjestelmien luokittelu PPSHP:n krittisten toimintojen mukaisesti.*

Potilaanhoito
Toiminnan turvaaminen
Infrasturktuuri
Tukitoiminnot

Potilaanhoito sisältää organisaation strategian mukaiset liiketoimintaprosessit eli potilaan hoitoon liittyvät tietojärjestelmät. Toiminnan turvaamiseen sisältyvät haastattelussa esiin nousseet hallinnolliset asiakirjat ja muu toiminnan ylläpitoon liittyvät tietojärjestelmät, esimerkiksi palkka- ja henkilöstöhallinnon tietojärjestelmät. Infrastrktuuri -luokassa ovat esimerkiksi sovellusten virtuaalisointiin, tietoverkon palveluihin sisältyvät tietojärjestelmät ja erilaiset valvontajärjestelmät. Tukitoiminnot sisältävät esimerkiksi erilaiset toiminnanohjaus- ja koulutusjärjestelmät.

PPSHP jatkoi projektin jälkeen työtä luokittelemalla luokissa olevat tietojärjestelmät kriittisyyden mukaan ja määritteli, mitä vaatimuksia kriittiselle tietojärjestelmän toiminnalle asetetaan.

Kriittisyys luokat olivat 1-4, joista luokan 1 tietojärjestelmät ovat kaikkein kriittisimpiä ja luokan 4 tietojärjestelmät vähiten kriittisiä PPSHP:n toiminnan kannalta. Taulukossa 4 on kuvattuna määreet tietojärjestelmälle asetetuista vaateista.

TAULUKKO 4. *Tietojärjestelmien krittisyysluokkien määritykset.*

Kritti-syys asteet	Järjestelmän sallittu alhaalla olo	Potilas tietoa	Liike- ja ammat ti-salaisu uksia	Varame nettelyt yksiköis sä	Testi-ympä ristö	Järjestel-mä vikasieto inen	Päivystys-aikanen valvonta	Järjestel mä-toimittaja n tuki päivystys aikana
1	Alle 3 tuntia	✓	✓	✓	✓	✓	✓	✓
2	3-12 tuntia	✓	✓	✓			✓	✓
3	12-24 tuntia	✓	✓	✓				
4	useita päiviä							

Taulukossa kriittisyysaste kuvaa tietojärjestelmän kriittisyyttä. Järjestelmän sallittu alhaalla oloaika kertoo sen, kuinka kauan PPSHP:n toimii ilman tietojärjestelmää. Potilastietoa ja Liike- ja ammattisalaisuudet sarake kertoo sisältääkö tietojärjestelmä organisaation strategian kannalta kriittistä tietoa. Varamenettelyt sarake kertoo minkä luokan tietojärjestelmälle on suunniteltava varamenettelyt, jotta organisaation toiminta ei vaarannu vaikka järjestelmä on pois käytöstä.

Testiympäristö -sarake tarkoittaa, että PPSHP velvoittaa toteuttamaan tämän luokan tietojärjestelmälle erillisen testiympäristön, jotta erilaiset huoltotoimet voidaan testata ennen niiden toteuttamista varsinaiseen tuotantoympäristöön. Järjestelmän vikasietoisuus -sarakkeen mukaan velvoitetaan toteuttamaan järjestelmään jo se asennusvaiheessa erilaisia komponentteja, jotka lisäävät järjestelmän vikasietoisuutta, esimerkiksi kahdennusta ja klusterointia. Päivystysaikainen valvonta ja Järjestelmätoimittajan tuki päivystysaikana -sarakekeet määrittävät tuetaanko tietojärjestelmän toimintaa myös virka-ajan ulkopuolella. Lisäksi nämä seikat on huomioitava erilaisissa järjestelmän toimintaan solmittavissa sopimuksissa. Näiden velvoitteiden täyttäminen lisää PPSHP:n tiedon saatavuutta, eheyttä ja käytettävyyttä.

5.2.3. Tietoturvapolitiikoiden suunnittelu

Toimintatapaustutkimuksen mukaisesti vaiheessa 2 kuviossa 7 sivulla 22 tietoturvapolitiikat suunnitellaan ylä- ja alatason tietoturvapolitiikoihin. Siponen ym. (2015) tietoturvapolitiikan kehittämismallin mukaisesti ylä- ja alatason tietoturvapolitiikoiden tarkoitus on turvata organisaation strategiset tavoitteet, tämä toteuttaa Siponen ym. (2015) tietoturvapolitiikan kehittämisen mallin kolmannen tason: *Tietoturvapolitiikan kehityksessä täytyy ottaa huomioon organisaation ominaispiirteet. Tämä lähtökohta juontaa juurensa teorioista, joiden mukaan ei voida tuottaa yhtä tapaa toteuttaa tietoturvapolitiikkaa organisaatiossa.* Ylätason tietoturvapolitiikalla

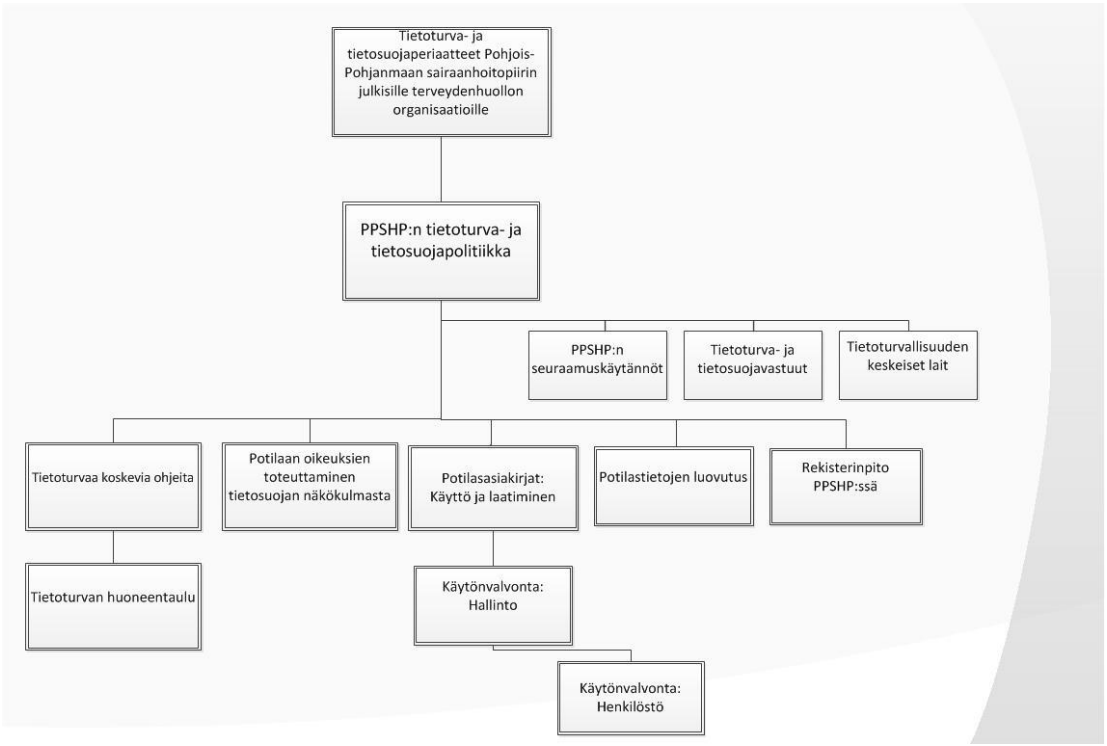
saavutetaan organisaation strategisten tavoitteiden toteutuminen ja alatason politiikat toteutetaan organisaation mukaisesti, jotta strategiset tavoitteet toteutuvat organisaation jokaisella tasolla. (Siponen ym. 2015).

Suunniteltaessa tietoturvapolitiikoita strateginen tavoite: Kumppanuus alueen organisaatioiden kesken edellyttää yhteisten pelisääntöjen toteuttamista tietoturvan- ja tietosuoja osalta. Tämä dokumentti edellytti sairaanhoitopiirin alueen yhteistä tietoturva- ja tietosuoja periaatetta. Tämän avulla alueen organisaatiot toteuttavat yhteisiä pelisääntöjä käsitellessään Terveydenhuoltolaissa (1326/2012) määritetyn yhteisen potilasrekisterin tietoja. Seuraavassa luvussa käsitellään tarkemmin strategisten tavoitteiden täyttyminen tietoturvapolitiikoissa.

5.3. Tietoturvapolitiikoiden toteuttaminen

Toimintatapaustutkimuksen mukaisesti 3 kuviossa 7 sivulla 22 vaiheessa toteutetaan tietoturvapolitiikat. Ylätason tietoturvapolitiikat Siponen ym. (2015) tietoturvapolitiikan kehittämismallin mukaisesti turvataan organisaation strategiset tavoitteet ja organisaation toiminta ilman toiminnan uhkaavia tietoturvahaasteita. Tietoturvapolitiikassa määritellään kuinka tietoturvapolitiikka ja sen periaatteet otetaan käyttöön organisaatiossa. Käyttöönotto vaihtelee organisaation mukaisesti. Tietoturvapolitiikoiden testaaminen on tärkeä elementti, joka täyttää ensimmäisen lähtökohdan. (Siponen ym. 2015).

Strategisten tavoitteiden olivat: Tehokas terveydenhuolto kaikissa tilanteissa, alueellinen yhteistyö muiden organisaatioiden kanssa, kumppanuus alueen organisaatioiden kesken, vastuunjako alueen organisaatioiden kesken ja vetovoimainen työpaikka ja osaava henkilöstö. Lisäksi haastatteluissa nousi esiin että organisaation kriittiset tiedot olivat potilastieto, organisaation liike- ja ammattisalaisuudet sekä tutkimus ja kehitystyöhön liittyvä tieto. Kuviossa 8 sivulla 32 on kuvattuna toteutetut ylä- ja alatason tietoturvapolitiikat.



KUVIO 8. *Ylä- ja alatason tietoturvapolitiikat Pohjois-Pohjanmaan sairaanhoitopiirissä.*

PPSHP:n tietoturvapolitiikat koostuvat seuraavista dokumenteista ylätason politiikoista: tietoturva- ja tietosuojaperiaatteet Pohjois-Pohjanmaan sairaanhoitopiirin julkisille terveydenhuollon organisaatioille, PPSHP:n tietoturva- ja tietosuojapolitiikka, PPSHP:n seuraamuskäytännöt, tietoturva- ja tietosuojavastuut, tietoturvallisuuden keskeiset lait

Alatason tietoturvapolitiikat ovat: tietoturvaa koskevia ohjeita, tietoturvan huoneentaulu, potilaan oikeuksien toteuttaminen tietosuojan näkökulmasta, potilasasiakirjat: käyttö ja laatiminen, käytönvalvonta: hallinto, käytönvalvonta: henkilöstö, potilastietojen luovutus ja rekisterinpito PPSHP:ssä

PPSHP:n strategisena tavoitteena oli *Kumppanuus alueen organisaatioiden kanssa*. Tämä tavoite toteutuu luomalla yhteiset tietoturvapelisäännöt alueen organisaatioiden kanssa. Tämä on ylätason tietoturvapolitiikka nimeltään Tietoturva- ja tietosuojaperiaatteet Pohjois-Pohjanmaan sairaanhoitopiirin julkisille terveydenhuollon organisaatioille. Tässä ylätason tietoturvapolitiikassa toteutuu myös Terveydenhuoltolain (1326/2012) määrittämä sairaanhoitopiirin alueen yhteisen potilasrekisterin velvoitteet terveydenhuollon organisaatioille.

PPSHP:n tietoturva- ja tietosuojapolitiikka sisältää seuraavat liitteet: PPSHP:n seuraamuskäytännöt, Tietoturva- ja tietosuojavastuut ja Tietoturvallisuuden keskeiset lait. Nämä ylätason tietoturvapolitiikat on johdettu alatason tietoturvapolitiikoihin, joissa on otettu huomioon PPSHP:n kriittisen tiedon suojaaminen organisaation kaikilla tasoilla.

Dokumentit hyväksyttiin organisaatiossa hyväksymiskäytännön mukaisesti. Ylätason tietoturvapolitiikat käsiteltiin PPSHP:n tietoturvaryhmässä ja ylätason tietoturvapolitiikat hyväksyttiin ja allekirjoitettiin 17.1.2014. Dokumenttien julkaisu

toteutettiin PPSHP:n julkaisumenetelmällä. Alatason tietoturvapolitiikat tarkastellaan organisaation vastuuhenkilöiden toimesta ja julkaistaan sen jälkeen henkilökunnan saataville. Lisäksi uudet tietoturvapolitiikat koulutetaan tämän avulla jokainen työntekijä ymmärtää tietoturvakäyttäytymisen oman työnsä kannalta.

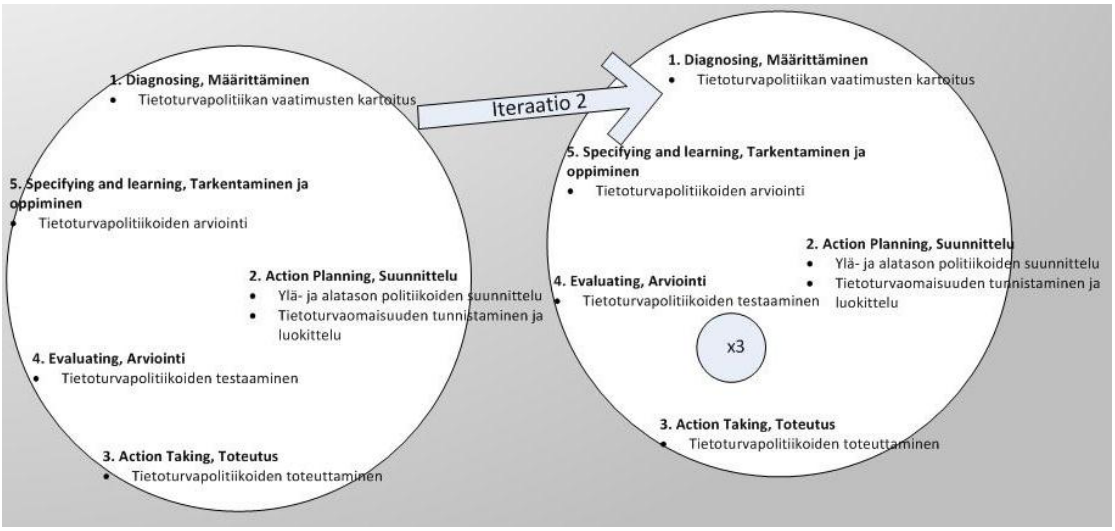
Tietoturvapolitiikat muodostavat jatkumon. Esimerkiksi Tietoturva- ja tietosuojaperiaatteet Pohjois-Pohjanmaan sairaanhoitopiirin julkisille terveydenhuollon organisaatioille velvoittaa, että tietojärjestelmissä oleva tieto on oikeellista. PPSHP:n tietoturva- ja tietosuojapolitiikka määrittää, että PPSHP valvoo tietojärjestelmissä olevien tietojen käyttöä. Lisäksi Potilastiedon käyttö ja laatiminen dokumentissa on määriteltynä miten kuinka potilasasiakirja laaditaan, millä oikeuksilla potilasasiakirjan saa avata ja kuinka potilasasiakirjojen käytönvalvonta suoritetaan tarkemmalla tasolla.

Tässä tietoturva- ja tietosuoja politiikassa liitteineen täyttyy Siponen ym. (2015) tietoturvapolitiikan kehittämisen mallin lähtökohta 4, jossa määritellään kuinka tietoturvapolitiikkaa ja tietoturvaprosesseja kehitetään ja ylläpidetään. Tässä tietoturvapolitiikassa määritellään vastuut ja kuinka tietoturvapolitiikka hyväksytään ja julkaistaan. (Siponen ym. 2015.)

5.4. Tietoturvapolitiikoiden testaaminen

Toimintatapaustutkimuksen mukaisesti vaiheessa 4 kuviossa 7 sivulla 22 tietoturvapolitiikat testataan. Tietoturvapolitiikoiden testaamisen tarkoitus on selvittää, ymmärtääkö kohderyhmä tietoturvapolitiikan. Tietoturvapolitiikat testattiin käyttäjäryhmittäin. Siten, että henkilöstö, jolle tietoturvapolitiikka oli suunnattu, he lukivat tietoturvapolitiikat ja tietoturvapolitiikoihin toteutettiin tarvittavat muutokset.

Kuten edellä on kerrottu, tässä kontekstissa toteutuu kaksi ylätason tietoturvapolitiikkaa. Ensimmäinen ylätason tietoturvapolitiikka on Pohjois-Pohjanmaan sairaanhoitopiirin alueen yhteinen tietoturva- ja tietosuojaperiaate. Kaikkia organisaatioita velvoittaa Terveydenhuoltolaki (1326/2012), joka velvoittaa, että samaan sairaanhoitopiiriin kuuluvat muodostavat yhteisen potilasrekisterin ja jokainen organisaatio vastaa siitä oman rekisterinsä osalta. Tämä siis tarkoittaa, että samaan sairaanhoitopiiriin kuuluvat kunnat tallentavat salassa pidettävää tietoa yhteiseen rekisteriin. Toteutettaessa tietoturvapolitiikkaa luotiin Pohjois-pohjanmaan sairaanhoitopiirin alueelle yhtenäinen tietoturva- ja tietosuoja periaate. Dokumentti testattiin yhdessä PPSHP:n tietoturva- ja tietosuojapolitiikan kanssa, joka on kyseisen organisaation ylätason tietoturvapolitiikka. Vaatimus käynnisti toisen iteraation kierroksen. Iteraatiot kuvattu alla Kuviossa 9.



KUVIO 9. Tutkimuksen iteraatiot

Ylätason tietoturvapolitiikkoiden kommentit pyydettiin sähköpostilla aikatauluongelmien vuoksi. Lisäksi ylätason tietoturvapolitiikoita katselmoitiin PPSHP:n tietoturvaryhmässä. Näissä kokouksissa ei ollut lupaa käyttää nauhuria mutta muutokset dokumentteihin kirjattiin kokousten muistioon. Ylätason tietoturvapolitiikat testattiin. Tässä vaiheessa ylätason tietoturvapolitiikkaan kommentoitiin, toteutuvatko lainsäädännöstä tulevat vaatimukset riittävästi.

Alatason tietoturvapolitiikat testattiin haastatteluiden avulla. Alla on taulukko alapolitiikan testauksesta.

TAULUKKO 5. *PPSHP:n alapolitiikat.*

Alapolitiikka	Haastateltavia
Potilaanoikeuksien toteuttaminen: Tietosuojan näkökulmasta	3
Potilasasiakirjojen käyttö ja laatiminen	4
Potilastiedon käytön valvonta: hallinto	3
Potilastiedon käytön valvonta: henkilöstö	3
Rekistereidenpito PPSHP:ssä	3
Tietoturvaa koskevia ohjeita	2
Tietoturvan huoneentaulu	2
Potilastietojen luovutus	2

Alapolitiikoiden viitemateriaalina käytettiin Terveyden ja hyvinvointilaitoksen laatimaa opasta nimeltään Potilasasiakirjojen laatiminen ja käsittely: Opas terveydenhuollolle. Lisäksi tarkasteltiin, että näissä alatason tietoturvapolitiikoissa toteutuvat ylätason tietoturvapolitiikat.

Haastateltavat kommentoivat ansiokkaasti alatason tietoturvapolitiikoita. Muutaman dokumentin nimi muuttui kuvaavammaksi. Esimerkiksi alapolitiikka Rekistereidenpito PPSHP:ssä oli alun perin nimeltään Rekisterihallinto. Haastateltava kuvasi haastattelussa, että nimi muistuttaa yksikköä kuten tietohallinto. Uusi dokumentin nimi on selkeästi kuvaavampi. Samoin alapolitiikka Potilaanoikeuksien toteuttaminen: tietosuojan näkökulmasta, tämä dokumentti oli ennen haastatteluita vain Potilaan oikeuksien toteuttaminen. Haastateltava kertoi, että potilaalla on muitakin oikeuksia, esimerkiksi oikeus hyvään hoitoon. Tämän vuoksi alatason politiikan nimeksi tuli Potilaan oikeuksien toteutuminen: tietosuojan näkökulmasta.

PPSHP:ssä tietoturvaan ja tietosuojaan nimetyt vastuuhenkilöt, tässä tutkimuksessa syntyneet alatason tietoturvapolitiikat jätettiin vastuullisille. Heille annettiin esimerkit tämän tutkimuksen myötä, kuinka kyseiset dokumentit voitaisiin päivittää. PPSHP:ssä on käytössä tietoturvakoulutusympäristö, johon nämä dokumentit sopivat.

5.5. Tietoturvapolitiikoiden arviointi

Toimintatapaustutkimuksen mukaisesti vaiheessa 5 taulukko 7 sivulla 22 arvioidaan tietoturvapolitiikat. Siponen ym. (2015) tietoturvapolitiikan kehittämismallin mukaisesti tietoturvapolitiikoiden arviointi on tärkein elementti. Tässä havaitaan kohtaako määritelty tavoite ja toteutuuko tietoturvapolitiikoiden vaatimukset ylä- ja alatasoilla (Siponen ym. 2015.)

PPSHP osallistui 28.10.2015 valmiusharjoitukseen, jossa organisaation haavoittuvuus kohdistui kyber-turvallisuuteen. PPSHP joutui tässä kuvitteellisessa harjoituksessa

useiden kohdistettujen kyber-hyökkäysten kohteeksi. Ennen harjoitusta ylä- ja alatason tietoturvapolitiikat oli toteutettu. Lisäksi PPSHP:ssä oli tunnistettu organisaation liiketoiminnan kannalta kriittiset tietojärjestelmät. Harjoitus toteutettiin organisaation johdon tasolla. Harjoituksessa testattiin seuraavia elementtejä: PPSHP:n ylä- ja alatason tietoturvapolitiikoiden avulla suojataan kriittisin tieto ja PPSHP on kykenevä toteuttamaan liiketoimintaansa myös kyber-hyökkäyksen aikana.

6. Pohdinta

Tässä tutkimuksessa oli tarkoitus selvittää, kuinka Siposen ja Puhakaisen tietoturvapolitiikan kehittämismallia toteutetaan ja kehitetään käytännössä. Kirjallisuudesta ei löydy tietoturvapolitiikkaa, joka olisi toteutettu tämän mallin mukaisesti. Lisäksi tutkitaan mallin soveltuvuutta tässä konteksitissa.

Terveydenhuollon organisaatio on toisaalta selkeä organisaatio tämän kaltaiselle tutkimukselle, koska sille asetetaan ulkoa tietyt vaatimukset tiedon suojaamiselle. Toisaalta kyseessä on julkinen viranomainen, jota velvoittaa viranomaistoiminnassa julkisuus. Nämä eivät kuitenkaan ole toisistaan poissulkevia seikkoja, vaan ne tukevat toisiaan.

Lainsäädännöllä on suuri vaikutus terveydenhuollon tiedon käsittelyyn ja palvelujen järjestämiseen. Tehokkaiden palvelujen järjestämisen tukena on tietoturvan ja tietosuojan näkökulma, jotta terveydenhuollon palvelut voidaan tehokkaasti ja turvallisesti toteuttaa, on tarpeen turvata salassa pidettävä tieto. Näkemykseni mukaan tietoturvapolitiikka on mahdollistaja, jonka avulla organisaatiossa voidaan toteuttaa uusia toimintamalleja ja tekniikoita.

PPSHP:n strategia painottaa, että terveydenhuollon palveluita voidaan järjestää tehokkaasti ja jakaa vastuuta eri organisaatioiden kesken. Tässä tutkimuksessa nousi esille, että on tärkeää tunnistaa ja luokitella organisaation tieto-omaisuus. Lisäksi tutkimuksessa nousi esille, että niiden organisaatioiden kesken, jotka tekevät yhteistyötä, on keskeistä jakaa yhtenäiset periaatteet tietoturvan osalta. Tämä lisää luottamusta organisaatioiden kesken ja mahdollistaa yhteistyön ja jopa kumppanuuden, kuten PPSHP:n strategiassa mainittiin.

Tiedon luokittelu on haastava prosessi ja tässä tutkimuksessa havaittiin, että yhteisen konsensuksen löytyminen siinä on haasteellista. Kuitenkin työssä on apuna riskienhallinnan työkalut eli tarkastellaan asiaa siitä näkökulmasta, että mikä tiedon merkitys on organisaation toiminnan kannalta, vahingoittuuko organisaation toiminta, jos kyseessä oleva tieto ei ole saatavilla.

Tietoturvapolitiikan toteuttaminen ylä- ja alatasolla turvaa sen, että organisaation kriittisimmän tiedon saatavuus on turvattu kaikissa tilanteissa, niille jotka tietoa tarvitsevat. Tässä tutkimuksessa syntyi yhteensä kymmenen ylä- ja alatason tietoturva- ja tietosuojapolitiikkaa. Lisäksi tutkimuksessa toteutettiin tietojärjestelmien luokittelu ja synnytettiin organisaation uusia prosesseja mm. ICT-varautumisen osalta. Tutkimus on kaikkinensa nostanut organisaation tietoturvatasoa. Lisäksi asiakasrajapintaa on hyödynnetty tutkimuksessa, näin on saatu merkittävää tietoa uusien politiikoiden ja prosessien toimivuudesta käytännössä. Tutkimuksessa on testattu uusia dokumentteja ja prosesseja valmiusharjoituksessa, jossa organisaatioon kohdistuu kuvitteellinen kyber-hyökkäys. Harjoituksessa todettiin uusia kehityskohteita mutta myös, että organisaatiossa ollaan oikealla tiellä tietoturvan osalta.

Siponen ym. (2015) tietoturvapolitiikan kehittämismallissa oli neljä lähtökohtaa. *Ensimmäisen lähtökohdan* mukaan tietoturvapolitiikan kehittämisen menetelmät tulee olla johdettuna teorioista. Toteutettaessa tämän lähtökohdan todetaan, että

organisaatiossa tietoturvapolitiikka on toteutettu tavalla, joka on tutkittu. Haasteen tuo se, että löydetään oikea teoria taustalle.
Toinen lähtökohta oli puolestaan, että tietoturvapolitiikan kehittämisen mallin tulee sisältää empiiristä tietoa. Se sisältää ajatuksen, että mallia on testattu käytännössä ja todettu mallin edut ja haitat. Tämä tutkimus vastaa osaltaan lähtökohtaan kaksi. *Lähtökohdassa kolme* todetaan, että tietoturvapolitiikan kehityksessä tulee ottaa huomioon organisaation ominaispiirteet. Tämän mukaisesti tietoturvapolitiikan kehittämisen mallia voidaan soveltaa eri toimialoilla ja erilaisissa organisaatioissa. Siponen ym. (2015) tietoturvapolitiikan kehittämisen malli on siis mukautettavissa organisaation mukaisesti.
Neljäs lähtökohta määrittää, että tietoturvapolitiikan kehittämisen menetelmissä määritellään toimintatavat kuinka tietoturvapolitiikkaa kehitetään ja ylläpidetään. Lisäksi määritellään tietoturvavastuut ja kuinka tietoturvapolitiikka hyväksytään ja julkaistaan. Tämä on tärkeä osa tietoturvapolitiikan kehittämisen mallia, koska organisaatiot muuttuvat sisäisesti ja niiden toimintaympäristöt muuttuvat. Lähtökohta neljän mukaisesti organisaatiot voivat mukautua toimintaympäristöönsä mutta samalla suojata liiketoiminnan kannalta kriittisimmän tiedon.

Pohdittaessa Siponen ym. (2015) tietoturvapolitiikan kehittämismallin soveltuvuutta tässä kontekstissa todetaan, että lähtökohdan kolme mukaisesti tietoturvapolitiikasta voitiin toteuttaa tietoturvapolitiikka, jonka avulla kohdeorganisaation vaatimukset huomioiden toteutettiin toimiva tietoturvapolitiikka. Perustelen väitettä vielä sillä, että Siponen ym. (2015) tietoturvapolitiikan kehittämismallin mukaisesti tietoturvapolitiikassa otetaan huomioon organisaatiolle asetetut vaatimukset ja tietoturvapolitiikka koostuu ylä- ja alatason tietoturvapolitiikoista. Näiden avulla organisaatioon toteutettiin kaksi ylätason tietoturvapolitiikkaa ja riittävästi alapolitiikoita.

Ylätason tietoturvapolitiikoiden avulla turvattiin lain säädännöstä tuleva vaatimus, että saman sairaanhoitopiirin julkiset terveydenhuollon organisaatiot potilastietorekisterit kuuluvat samaan rekisteriin, mutta jokainen organisaatio vastaa siitä omalta osaltaan. Lisäksi kohdeorganisaation strategiassa tunnistettiin että alueen organisaatiot ovat kumppaneita keskenään. Kumppanuuden avulla turvataan organisaatioiden keskittyminen ja varmistetaan toimivat hoitoketjut. Siponen ym. (2015) tietoturvapolitiikan kehittämismallin mukaan voitiin huomioida organisaatiolle asetetut vaatimukset ja kohde organisaation ominaispiirteet otettiin huomioon riittävästi toimivan tietoturvapolitiikan toteuttamisessa.

Työskentelin kohdeorganisaatiossa tutkimuksen ajan ja se mahdollisti työn. Lisäksi koin, että saan tukea organisaatiosta työn eteenpäin viemisessä. Haasteita toki oli, esimerkiksi siinä, että kesken työn organisaatiossa tapahtui henkilövaihdoksia ja suunnitelmia oli muutettava matkan varrella.

7. Johtopäätökset

Tässä tutkimuksessa saatiin vastaus siihen, että Siposen ja Puhakaisen tietoturvapolitiikan kehittämismalli on toimiva tässä kontekstissa eli PPSHP:ssä. Tässä tutkimuksessa organisaation ominaispiirteet ja kohdeorganisaatiolle asetetut vaatimuksen huomioitiin toteutettaessa tietoturvapolitiikkaa. Lisäksi kehitettiin yhtenäiset tietoturva- ja tietosuoja periaatteet koko sairaanhoitopiirin alueelle. Jatkokehityksen kannalta tulisi varmistua siitä, että sairaanhoitopiirin terveydenhuollon organisaatiot täyttävät nämä periaatteet.

Tässä tutkimuksessa selvitettiin myös, että organisaation kriittisin tieto säilyy organisaatiossa ja organisaatio voi toimia, vaikka sen toimintaa yritettäisiin haavoittaa kohdennetuilla kyber-hyökkäyksillä. Tutkimuksessa jäi kuitenkin selvittämättä se, että turvataanko henkilöstön tietoturvakäyttäytyminen uusien tietoturvapolitiikoiden myötä, sillä organisaation on turvattava henkilöstön riittävä tietoturva- ja tietosuoja osaaminen. Tietoturvakoulutuksien avulla nostetaan henkilöstön tietoturvaosaamista ja turvataan tietoturvakäyttäytyminen.

Terveydenhuollon palvelujen järjestäminen on uudistuksen kohteena. Jatkokehityksen kannalta on tarpeen arvioida, ovatko tässä tutkimuksen keskiössä olevat sairaanhoitopiirin alueet ja niiden organisaatiot, kun uusi sosiaali- ja terveydenhuollon palvelujen järjestäminen tulee voimaan. Tulee myös arvioida sitä, kuinka näiden organisaatioiden toimintaympäristö muuttuu. Nämä edellä mainitut seikat asettavat mahdollisesti uusia vaatimuksia näiden organisaatioiden tietoturvapolitiikoille. Samanaikaisesti EU:n tasolla ollaan uudistamassa EU:n tietosuoja-asetusta, joka tuo uusia lakiuudistuksia kansalliselle tasolle. On tarpeen tarkastella, että tuovatko ne mukanaan uusia vaatimuksia terveydenhuollon tietoturvalle ja tietosuojalle.

Lähteet

Anttila, Pirkko 2006. Ilmaisu, teos, tekeminen ja tutkiva toiminta. Hamina: Akatiimi.

Backhouse J., & Dhillon G. 2001. “Current Directions in IS Security Research: Toward Socio-Organizational Perspectives,” Information Systems Journal (11:2), pp. 127-153.

Baskerville R. 1999. Investigating Information Systems with Action Research. Communications of AIS Vol 2 (19) pp.1-27.

Baskerville R. & Siponen M., 2002. "An information security meta-policy for emergent organizations", Logistics Information Management, Vol. 15 Iss: 5/6, pp.337 – 346

Mouelhi, Fleurey, Baudry & Le Traon. 2008. A Model-Based Framework for Security Policy Specification, Deployment and Testing. Model Driven Engineering Languages and Systems. Lecture Notes in Computer Science Vol 5301, 2008, pp 537-552.

Ciasson M., Germonprez M. & Mathiassen L. 2012. Style Composition in Action Research Publication. Mis Quartely Vol 36 (2), pp. 347-363.

Davison M., Martionsons M. & Ou C.X.J. 2012. The Roles of Theory in Canonical Action Research. MIS Quartely Vol 36 pp 1-24.

Eskola, J. & Suoranta, J. 1998. Johdatus laadulliseen tutkimukseen. 2. p. Tampere : Vastapaino

Hakala M., Vainio M. & Vuorinen O. 2006. Tietoturvallisuuden käsikirja. Porvoo: Docendo

Heikkinen H., Roivio E. & Syrjälä L. 2006. Toiminnasta tietoon. Vantaa: Dark.

Heikkinen, H.L. T. & Jyrkämä J. 1999. Mitä on toimintatutkimus? Teoksessa Heikkinen, H. L. T., Huttunen, R. & Moilanen, P. (toim.) Siinä tutkija missä tekijä. Toimintatutkimuksen perusteita ja näköaloja. Jyväskylä: Atena kustannus, 25–62.

Hirsjärvi, S. & Hurme, H. 2010. Tutkimushaastattelu. Teemahaastattelun teoria ja käytäntö. Helsinki: Gaudeamus.

Hirsjärvi, S., Remes, P. & Sajavaara, P. 2012. Tutki ja kirjoita. Helsinki: Kustannusosakeyhtiö Tammi.

Henkilötietolaki (523/1999) saatavissa: http://www.finlex.fi/fi/laki/ajantasa/1999/19990523?search%5Btype%5D=pika&search%5Bpika%5D=Henkil%C3%B6tietolaki. Viitattu 29.11.2015.

Höne, K. & Eloff, J.H.P. 2002. Information security policy – what do international information security standards say?, Computers & Security Volume (21:5), pp 402–409.

Kananen, J. 2009. Toimintatutkimus yritysten kehittämisessä. Jyväskylän ammattikorkeakoulun julkaisuja -sarja. Jyväskylä: Jyväskylän ammattikorkeakoulu.

Knapp, K. J., Morris, R. F, Marshall, Jr.T.E & Byrd T. A. 2009. Information security policy: An organizational-level process model. Computers & Security. July 10.

Karyda, M., Kiountouzis, E. & Kokolakis, S. 2005. Information systems security policies: a contextual perspective. Computers & Security (24), pp. 246-260

Kuula, A. 1999. Toimintatutkimus: kenttätyö ja muutospyrkimyksiä. Tampere: Vastapaino.

Kuusela P.2005. Realistinen toimintatutkimus? Työturvallisuuskeskus. Edita.

Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007) Saatavissa: http://www.finlex.fi/fi/laki/ajantasa/2007/20070159?search%5Btype%5D=pika&search%5Bpika%5D=Laki%20sosiaali%20ja%20terveydenhuollon%20asiakastietojen%20s%C3%A4hk%C3%B6isest%C3%A4%20k%C3%A4sittelyst%C3%A4%20. Viitattu 29.11.2015.

Laki potilaan asemasta ja oikeuksista (785/1992). Saatavissa: http://www.finlex.fi/fi/laki/ajantasa/1992/19920785?search%5Btype%5D=pika&search%5Bpika%5D=Laki%20potilaan%20asemasta%20ja%20oikeuksista%20. Viitattu 29.11.2015.

Laki terveydenhuollon ammattihenkilöistä (559/1994). Saatavissa: http://www.finlex.fi/fi/laki/ajantasa/1994/19940559?search%5Btype%5D=pika&search%5Bpika%5D=Laki%20terveydenhuollon%20ammattihenkil%C3%B6ist%C3%A4%20. Viitattu 29.11.2015.

Laki viranomaisen toiminnan julkisuudesta (621/199). Saatavissa: http://www.finlex.fi/fi/laki/ajantasa/1999/19990621?search%5Btype%5D=pika&search%5Bpika%5D=Laki%20viranomaisen%20toiminnan%20julkisuudesta%20. Viitattu 29.11.2015.

Louw, L. Solms & R., Thomsom. 2006. Cultivating an organizational Information security culture. Computer Fraud & Security. Vol (10) pp 7-11.

Maynard, S.B., Ruighaver A.B & Chang, S. 2007. Organisational security culture: Extending the end-user perspective. Computers&Security Vol (26) 1. pp56-62.

Metsämuuronen, J. 2009. Tutkimuksen tekemisen perusteet ihmistieteissä. Helsinki: International Methelp.

Myers M.D & Newman M. 2007. The qualitative interview in IS research: Examining the craft. Information and Organization. Volume 17, Issue 1, 2007, sivu 2–26.

Mäntylä, R. 2007. Kertovan muutosselonteon menetelmä. Teoksessa Avauksia laadullisen tutkimuksen analyysiin, toim. Syrjäläinen, E. Eronen, A. & Värri, V.-M., 40–61. Tampere: Tampere University Press.

Nigam, A. & Siponen, M. 2011. Designing Information System Security Policy Methods: A Meta-Theory Approach. Sprouts. (11) 150.

Peltier TR. 2002. Information security policies, procedures and starndards: guidline for effective information security management. Aeuerbach CRC press LLC.9.

Rees. J., Bandyopadhyay &Spafford E. H. 2003. PFIRES: A Policy Framework for Information Security. Communication of ACM 46 (7) 101-106.

Rees J., Bandyopadhyay S. & Spafford E. H. 2003. PFIRES: a policy framework for information security. ACM. 46 (7) 101-106.

Seren S. & Baykal U. 2007 Relationships Between Change and Organizational Culture in Hospitals. Journal of Nursing Scholarship. 39 (2) 191–197.

Siponen, M., Pahnila, S. &Mahmood, A. 2007. Employees' Behavior towards IS Security Policy Compliance. System Science. HICSS

Siponen, M. &Puhakainen, P. 2010. Improving employees' compliance through Infromation systems security training: An action research study. MIS Quarterly 34 (4) 757-778.

Schultze U. & Avital M. 2011. Designing interviews to generate rich data for information system research. Information and Organization. 21 (1) 1–16.

Syrjäläinen, Eija, Eronen, Ari & Värri, Veli-Matti 2007. Johdanto. Teoksessa Syrjäläinen, Eija, Eronen, Ari & Värri, Veli-Matti (toim.) Avauksia laadullisen tutkimuksen analyysiin. Tampere: Tampereen University Press, 7–10.

Terveydenhuoltolaki (1326/2012). Saatavissa: http://www.finlex.fi/fi/laki/ajantasa/2010/20101326?search%5Btype%5D=pika&search%5Bpika%5D=Terveydenhuoltolaki%20. Viitattu 29.11.2015

Tuomi, J. 2007. Tutki ja lue. Johdatus tieteellisen tekstin ymmärtämiseen. Helsinki: Kustannusosakeyhtiö Tammi.

Tuomi, J. & Sarajärvi, A. 2009. Laadullinen tutkimus ja sisällönanalyysi. Helsinki: Kustannusosakeyhtiö Tammi.

Turner D.W. 2010. Qualitative Interview Design: A Practical Guide for Novice Investigators. 15 (3) 754-760.

Vilkka, H. 2006. Tutki ja havainnoi. Helsinki: Kustannusosakeyhtiö Tammi.

Yusufovna S. F. (2008) Advanced Security Policy Implementation for Information Systems. (56) IEEE Computer Society.

Julkaisemattomat lähteet

Siponen, M. & Puhakainen, P. 2015. New Methods For the Development of Information Security Policies. Unpublished manuscript.

Liite A. Tutkimuksessa käytetyt kysymykset

Mitkä ovat PPSHP:n keskeisimmät toiminnot?

Mikä PPSHP:n strategiassa on toiminnan kannalta tärkeintä?

Mitkä ovat PPSHP:n toimintojen tärkeimmät tiedot ja tietojärjestelmät?

Kuinka kriittisiä edellä mainitut tietojen salassapito, oikeellisuus ja saatavuus ovat?

Onko tiedoilla ehdoton oikeellisuus vaatimus, miksi? Jos vaatimusta ei ole, millaisia virheitä sallitaan?

Liite B. Tutkimuksessa hyödynnetyt lait

Potilastietojen käsittelyn tulee täyttää EU:n tietosuojadirektiivin ja kansallisen lainsäädännön asettamat vaatimukset tietoturvallisuudelle ja yksityisyyden suojalle. Vaatimustenmukaisuus saadaan selville tietosuoja- ja tietoturvakartoituksen avulla. Terveydenhuollossa potilastietojen käsittelyn ennakkosuunnittelu on erityisen korostuneessa asemassa. Täten lainmukaisuus tulee tarkistaa jo tietojärjestelmien suunnitteluvaiheessa.

Alla on esitetty keskeisimmät potilastietojen käsittelyä säätelevät lait ja asetukset:
Arkistolaki 1994/831
Asetus terveydenhuollon ammattihenkilöistä 1994/564
Erikoissairaanhoitolaki 1989/1062
Esitutkintalaki 1987/449
Hallintolaki 2003/434
Henkilökorttilaki 1999/829
Henkilötietolaki 1990/523
Kuntalaki 1995_365
Laki kuolemansyyn selvittämisestä 1973/459
Laki lääketieteellisestä tutkimuksesta 1999/488
Laki potilaan asemasta ja oikeuksista 1992/785
Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä 2007/159
Laki sähköisestä asioinnista viranomaistoiminnassa 2003/13
Laki terveydenhuollon ammattihenkilöistä 1994/559
Laki sähköisestä lääkemääräyksestä 61/2007
Laki terveydenhuollon valtakunnallisista henkilörekistereistä 1989/556
Laki vahvasta tunnistamisesta ja sähköisestä allekirjoituksesta 2009/617
Laki viranomaisten toiminnan julkisuudesta 1999/621
Laki väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista 2009/166
Lastensuojelulaki 2007/417
Mielenterveyslaki 1990/1116
Poliisilaki 1995/493
Rekisterihallintolaki 1996/166
Sosiaali- ja terveysministeriön asetus potilasasiakirjoista 2009/298
Tartuntatautilaki 1986/583
Terveydenhuoltolaki 2010/1326
Työterveyshuoltolaki 2001/1383