Terveydenhuollon asiakastietojen käsittelyn lainmukaisuus aluetietojärjestelmäympäristössä

Antto Seppälä

Tampereen yliopisto
Tietojenkäsittelytieteiden laitos
Tietojenkäsittelyoppi / Tietojärjestelmätieteet
Pro gradu -tutkielma
Ohjaaja: Pirkko Nykänen
Joulukuu 2007

Tampereen yliopisto
Tietojenkäsittelytieteiden laitos
Tietojenkäsittelyoppi / Tietojärjestelmätieteet
Pro gradu tutkielma, 119 sivua, 7 liitesivua
Joulukuu 2007

Merkittävimpiä muutoksia viime aikojen terveydenhuollon palvelutuotannossa on ollut tavoite hoitaa potilaita yli organisaatiorajojen. Useisiin organisaatioihin perustuva hoito vaatii tietojenkäsittelyä yli rajojen. Organisaatioiden rajojen ylittävän tietojenkäsittelyn tarpeeseen on kehitetty aluetietojärjestelmiä, joiden avulla voidaan katsella potilastietoja eri organisaatioiden potilastietojärjestelmistä. Potilastietojen katselu yli organisaatiorajojen asettaa suuria vaatimuksia tietosuojalle ja tietoturvalle.

Tässä tutkimuksessa tarkastellaan aluetietojärjestelmäympäristössä tapahtuvan tietojenkäsittelyn lainmukaisuuden toteutumista. Tutkimuksen alussa esitellään terveydenhuoltoon ja potilastietojen käsittelyyn liittyvää lainsäädäntöä, jonka pohjalta rakennettiin arviointikriteeristö. Kriteeristöön kerättiin vaatimuksia ja rajoitteita, mitä lainsäädäntö asettaa terveydenhuollon tietojenkäsittelylle. Kriteeristön avulla analysoitiin kohdeympäristön tietojenkäsittelyn lainmukaisuutta. Kohdeympäristöinä tutkimuksessa olivat Pirkanmaan ja Satakunnan sairaanhoitopiirit.

Tutkimus osoitti, että aluetietojärjestelmäympäristössä tapahtuva tietojenkäsittely noudattaa pääsääntöisesti lainsäädännön asettamia vaatimuksia. Tutkimuksella kuitenkin havaittiin joitakin puutteita, joihin kohdeympäristöissä tulisi reagoida.

Avainsanat ja –sanonnat: terveydenhuolto, tietojärjestelmät, aluetietojärjestelmät, tietosuoja, tietoturva, yhteistoiminnallisuus

1. Johdanto

Terveydenhuolto Suomessa on järjestetty yleisesti organisaatiokeskeisesti, jolloin potilaan hoitoa suunnitellaan yhden toimintayksikön näkökulmasta. Organisaatiokeskeisyys ei näy pelkästään hoidon järjestämisessä, vaan myös toimintayksiköiden tietojärjestelmät ovat suunniteltu organisaation omiin tarpeisiin. Poikkeuksena ovat erilaiset sähköiset lähete-palautejärjestelmät ja aluetietojärjestelmät, joiden tavoitteena on mahdollistaa tietojen välitys eri organisaatioiden välillä. Potilaiden hoito voidaan kuitenkin nähdä saumattomana palveluketjuna, jossa useat toimijat osallistuvat hoitoon yli organisaatiorajojen. Viime aikoina Suomessa on alettu terveydenhuollon kohdalla lähestyä potilaiden hoitoa asiakaslähtöisesti. Asiakaslähtöinen ajattelutapa vaatii organisaatioiden rajojen ylittävää saumatonta tiedonkulkua [Tuori, 2003; Ohtonen, 2002].

Merkittävimpiä muutoksia viime aikojen terveydenhuollon palvelutuotannossa on ollut tavoite hoitaa potilaita yli organisaatiorajojen. Useisiin organisaatioihin perustuva hoito vaatii tietojen käsittelyä yli rajojen. Sosiaali- ja terveydenhuollossa käytössä olevat useat keskenään yhteentoimimattomat järjestelmät ovat muodostaneet merkittävän hidasteen toiminnan kehittämiselle ja verkostoitumiselle. Tämän takia palveluiden tuottajien pitää kehittää yhdessä organisaatioiden välisiä toimintaprosesseja ja näitä tukevia tietojärjestelmiä, jotta voidaan taata potilaille saumaton palveluketju. Järjestelmien keskittämisellä voidaan saavuttaa merkittäviä säästöjä, kun kehittämis- ja käyttökustannuksia on mahdollista karsia [Ekebom et al., 2003]. Keskittämisellä ei tarkoiteta pelkästään yhteisten järjestelmien hankintaa, vaan myös että uudet järjestelmät integroidaan yhteentoimiviksi jo olemassa olevien järjestelmien kanssa

Suomessa aloitettiin kansallinen Satakunnan makropilotti – hanke vuonna 1999. Tarkoituksena oli kehittää sosiaali- ja terveydenhuollon

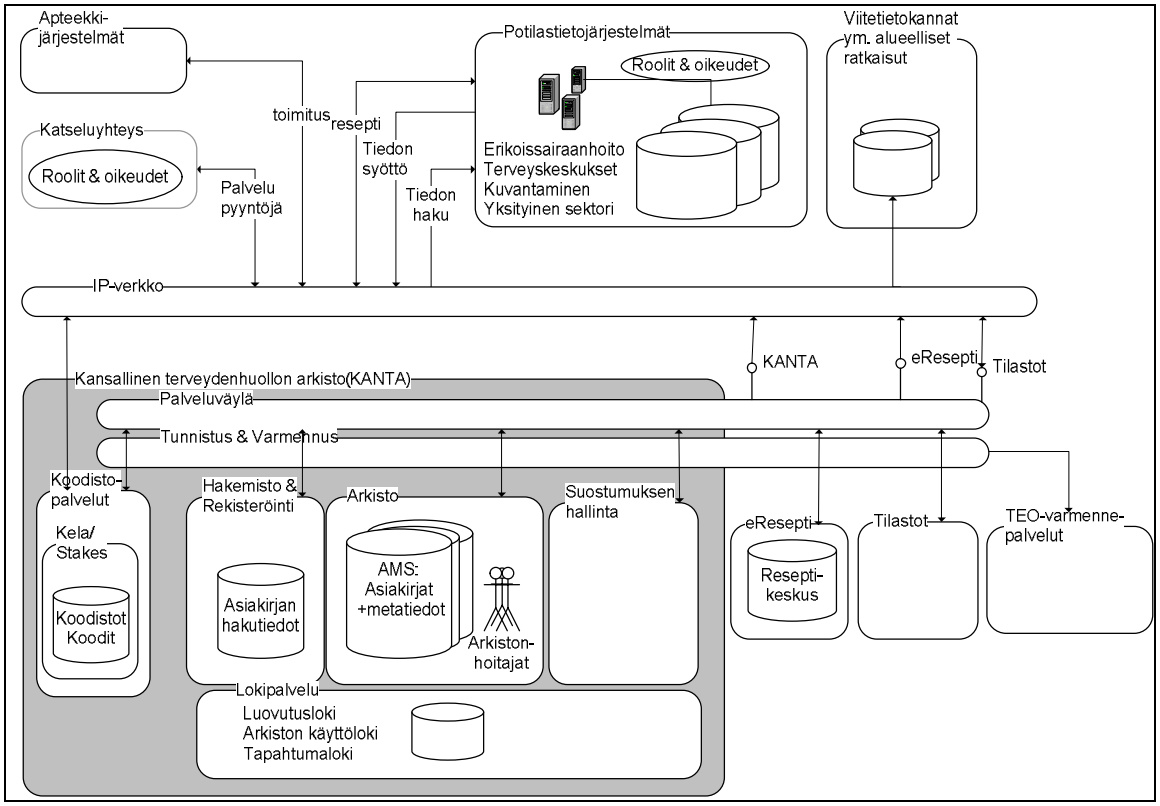
palvelujärjestelmää vastaamaan muuttuvan sektorin luomiin uusiin haasteisiin ja paineisiin, kuten väestön ikääntymiseen ja kansalaisten tietoisuuden kasvuun omista oikeuksistaan. Hankkeessa oli myös tarkoituksena kehittää teknisiä ratkaisuja, joiden avulla voidaan tarjota palveluita vanhoista tavoista poikkeavasti. [Määttä, 2000]

Yhtenä ratkaisumahdollisuutena nähtiin saumattomat palveluketjut ja niihin liittyvät tietotekniset ratkaisut. Hankkeen myötä säädettiin myös laki saumattomien palveluketjujen kokeilusta (811/2000). Saumattomia palveluketjuja tukemaan pyrittiin kehittämään aluetietojärjestelmiä, joiden tavoitteena on mahdollistaa tietojen vaihto eri terveyden- ja sosiaalihuollon toimintayksiköiden välillä. Aluetietojärjestelmissä tarkoituksena on tarjota terveydenhuollon ammattilaisille mahdollisuus katsella potilaiden tietoja toisten toimintayksiköiden potilastietojärjestelmistä [Ohtonen, 2002; Winblad et al., 2006]..

Pirkanmaan ja Satakunnan sairaanhoitopiireillä on käytössä Fiale-aluetietojärjestelmät. Aluetietojärjestelmän tarkoituksena on mahdollistaa tietojen siirto saman sairaanhoitopiirin alueella toimivien sosiaali- ja terveydenhuollon toimintayksiköiden erilaisten tietojärjestelmien välillä. Tiedon siirron avulla järjestelmät saadaan keskustelemaan keskenään ja siten voidaan saavuttaa todellista yhteistoiminnallisuutta eri organisaatioiden välillä. Yhteistoiminnallisuus mahdollistaa potilaiden hoidon yli organisaatiorajojen, ja yhtenäisten saumattomien palvelukokonaisuuksien luomisen.

Aluetietojärjestelmän avulla voidaan jakaa tietoa eri terveydenhuollon toimintayksiköiden välillä. Sen tarkoituksena on parantaa asiakkaan hoidon laatua ja nopeutta sekä helpottaa hoitohenkilökunnan tehtäviä. Myös organisaatiot pyrkivät saamaan kustannussäästöjä järjestelmän käytöllä, kun oletettavasti voidaan vähentää päällekkäisiä tutkimuksia ja testejä. [STM, 2002]

Terveydenhuollon tietojenkäsittely tulee lähivuosina Suomessa kokemaan muutoksia, koska Suomessa astui 1. heinäkuuta 2007 voimaan laki asiakastietojen sähköisestä käsittelystä. Lain avulla pyritään parantamaan terveydenhuollon organisaatioiden mahdollisuuksia hyödyntää tietotekniikkaa toiminnassaan. Merkittävin muutos koskien aluetietojärjestelmiä on kuitenkin määrittely kansallisesta arkkitehtuurista, johon alueellistenkin järjestelmien on mukauduttava. Kansallisessa arkkitehtuurissa on tavoitteena luoda valtakunnallinen tietojärjestelmäinfrastruktuuri (kuva 1.).



Kuva 1. KANTA kokonaisarkkitehtuuri [STM, 2007, s 8].

Kansallisessa arkkitehtuurissa on tarkoituksena luoda valtakunnallinen keskitetty sähköinen potilastietojen käsittely- ja arkistointijärjestelmä (KANTA). Kaikkien terveydenhuollon palveluntarjoajien on siirtymäajan jälkeen velvoitettu siirtymään arkiston käyttäjiksi. Arkistoon tallennetaan kansalaisten potilastiedot. Arkiston avulla voidaan jakaa eri

toimintayksiköiden tietoja muille organisaatioille. Kansallinen arkkitehtuuri asettaa paikallisille ratkaisuille minimivaatimukset esim. tiedon organisoimiselle ja siirrolle kansalliseen arkistoon. Arkistossa ei eri organisaatioiden tietoja yhdistetä, vaan sinne luodaan useita erillisiä rekistereitä, jotta voidaan säilyttää rekisterinpitäjyys tiedon omistajalla [STM, 2007]. Uusi tietojärjestelmäpalvelu ei siis välttämättä poista tarvetta aluetietojärjestelmille, mutta muutoksia se voi niille aiheuttaa, koska esimerkiksi toimintayksiköiden pitää rakentaa liittymät kansalliseen arkistoon.

Aluetietojärjestelmissä käsitellään asiakkaiden henkilötietoja ja välitetään niitä yli toimintayksiköiden rajojen, joten erilaiset lait ja asetukset asettavat käsittelylle vaatimuksia. Esimerkiksi potilastietojen luovutuksessa toimintayksiköstä toiseen on laissa säädetty vaatimuksia ja rajoitteita siitä, mitä ehtoja pitää täyttää ennen tietojen luovutusta. Tämä tutkimus selvittää lainsäädännöstä aiheutuvia vaatimuksia ja rajoitteita tietosuojaan ja tietoturvaan liittyen aluetietojärjestelmäympäristössä.

Tässä tutkimuksessa tutkitaan tietosuojan ja tietoturvan näkökulmasta Pirkanmaan ja Satakunnan sairaanhoitopiirien Fiale-aluetietojärjestelmiä, sekä niihin liittyvää tiedon käsittelyä ja siirtoa. Aluetietojärjestelmiä tutkitaan kahdella eri tasolla, sekä toiminnallisesta että tietojärjestelmätason näkökulmasta. Tutkimuksessa keskitytään varsinkin potilaan suostumukseen, potilastietojen käsittelyyn sekä käyttäjänhallintaan. Tutkimuksessa analysoidaan mitä vaatimuksia ja rajoitteita lainsäädäntö asettaa aluetietojärjestelmälle ja sen käyttöympäristölle. Analyysin perusteella arvioidaan tutkimuksessa esiteltävällä arviointikriteeristöllä miten hyvin tällä hetkellä aluetietojärjestelmät vastaavat lain asettamiin vaatimuksiin ja rajoitteisiin, eli miten ne täyttävät tietosuoja- ja tietoturvavaatimukset.

Tutkimuksen tuloksina esitellään arvio miten hyvin aluetietojärjestelmät täyttävät lainsäädännön vaatimukset, sekä minkälaisia muutoksia niihin mahdollisesti pitäisi tehdä. Tutkimuksessa pohditaan myös miten uusi laki asiakastietojen sähköisestä käsittelystä vaikuttaa aluetietojärjestelmiin.

2. Tietosuoja ja tietoturva

2.1. Tietosuoja

Tietosuojalla tarkoitetaan henkilötietojen suojaamista valtuudettomalta ja henkilöä vahingoittavalta käytöltä ja käsittelyltä. Tietosuojan tavoitteena on turvata tietojen luottamuksellisuuden säilyttäminen, yksityisyys ja oikeusturva. Henkilötietojen käsittelystä on säädetty monissa eri laeissa, mutta tietosuojan yleislakina voidaan pitää henkilötietolakia (1999/523). Henkilötietolakia sovelletaan silloin, kun missään muualla lainsäädännössä ei toisin säädetä [Tammisalo, 2005; Pahlman 2005; Korhonen, 2003]. Henkilötietolain tavoitteet määritellään itse lain alussa:

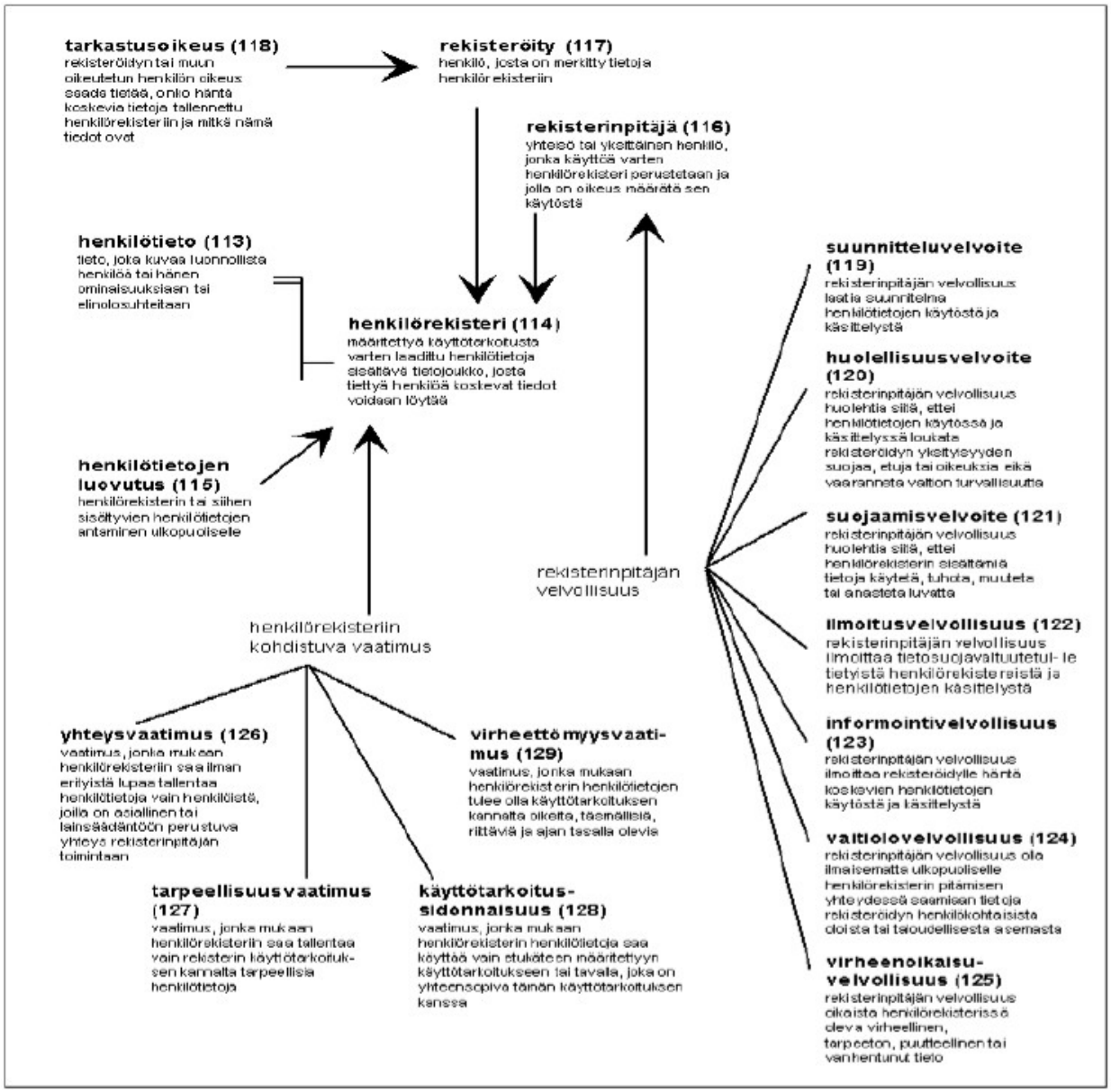
> "Tämän lain tarkoituksena on toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia henkilötietoja käsiteltäessä sekä edistää hyvän tietojenkäsittelytavan kehittämistä ja noudattamista."

Henkilötiedon käsite on määritelty henkilötietolaissa. Sillä tarkoitetaan luonnollista henkilöä kuvaavia merkintöjä, jotka voidaan tunnistaa häntä tai hänen perhettään koskeviksi. Henkilötietolakia on noudatettava aina henkilötietoja käsiteltäessä, ellei jossain toisessa laissa muutoin säädetä. Henkilötietolaissa on määritelty yleiset säännökset henkilötietojen keräämisestä, tallentamisesta, käytöstä, luovuttamisesta, siirrosta ja muusta käsittelystä. Henkilötietolaista nousevat esiin käsittelyä koskevat yleisperiaatteet. Niitä ovat huolellisuusvelvoite, suunnitteluvelvoite ja käyttötarkoitussidonnaisuus sekä tarpeellisuus- ja virheettömyysvaatimus. [Pahlman, 2005; HetiL, 1999; Pajukoski, 2004]

Henkilötietoja kerättäessä muodostuu henkilörekisteri. Henkilörekisterin määritelmä on, että se sisältää tietojoukon, joka muodostuu henkilötiedoista ja niitä käsitellään automaattisen tietojenkäsittelyn avulla tai ne on järjestetty siten että tiettyä henkilöä koskevat tiedot ovat helposti löydettävissä. Vastuu henkilötietojen käsittelyn lainmukaisuudesta on rekisterinpitäjällä. Rekisterinpitäjällä tarkoitetaan tahoa, jonka tarkoituksiin henkilörekisteri perustetaan ja joka vastaa henkilötietojen käsittelyn lainmukaisuudesta. Rekisterinpitäjä voi olla henkilö, yhteisö, laitos tai säätiö [HetiL, 1999].

Rekisterinpitäjälle on henkilötietolaissa säädetty erilaisia vastuita ja velvoitteita. Rekisterinpitäjän tulee huolehtia tietojen laadusta ja virheettömyydestä sekä salassa pidettävien ja arkaluontoisten tietojen suojaamisesta ulkopuolisilta. Henkilötietoja kerätessään rekisterinpitäjän on informoitava rekisteröityä tietojen käsittelystä. Tästä syystä rekisterinpitäjän tulee laatia rekisteriseloste, josta selviää rekisterinpitäjä, tietojen käsittelytarkoitus, tietojen säännönmukaiset luovutuskohteet, kuvaus rekisteröityjen ryhmästä sekä kuvaus rekisterin suojauksen periaatteista. Rekisteriseloste tulee olla jokaisen saatavilla, vaikka rekisterissä olevat tiedot olisivatkin salassa pidettäviä. [HetiL, 1999; Pajukoski, 2004; Pahlman, 2005]

Rekisterinpitäjän tulee myös määritellä kuka vastaa rekisterinpidosta sekä miten toteutetaan rekisteröidyn oikeudet. Näitä oikeuksia ovat tarkastus-, tietojen saanti- ja korjausoikeus. Rekisterinpitäjän tulee myös tehdä henkilöstölleen tietosuojaohjeet, joissa käsitellään henkilötietojen käyttöä ja tietojärjestelmien toimintaperiaatteita. Näiden ohjeistuksien noudattamisen toteutumista tulee myös valvoa. Kuvaan 2 on koottu henkilörekisterinpidon vaatimuksia ja käsitteitä. [HetiL, 1999; Pajukoski, 2004; Pahlman, 2005]



Kuva 2. Henkilörekisteriin liittyviä käsitteitä [Hyppönen et al., 2005, s 52].

2.1.1. Tietosuoja terveydenhuollossa

Terveydenhuollossa asiakas- ja potilassuhde perustuu tiedon luottamuksellisuuteen ja salassapitoon. Tietosuojan tavoitteena on turvata potilaan yksityisyys, edut ja oikeusturva sekä rekisterinpitäjän oikeusturva ja luoda henkilötietojen hyvä käsittelytapa kaikkiin eri käsittelyn vaiheisiin. Tietosuojassa ei siis ole ensisijaisesti kyse tietojen konkreettisesta suojauksesta,

vaan asiakkaan yksityisyyden suojasta sekä luottamuksellisesta potilassuhteesta. Niitä käytännön toimia, joilla toteutetaan tietosuoja, kutsutaan tietoturvaksi [Reponen, 2006; Pahlman, 2005; Pajukoski, 2004, Ylipartanen, 2004].

Lait ja erilaiset asetukset muodostavat hierarkkisen järjestyksen, jossa ylemmän asteen normi syrjäyttää alemman asteisen. Mikäli normit ovat samantasoiset, niin uudempi syrjäyttää vanhemman. Lisäksi erityissäännökset syrjäyttävät yleissäännökset. Tämä järjestys koskee myös Suomen tietosuojalainsäädäntöä, jonka perusteet on määritelty jo Euroopan Unionin tasolla. Tietosuojasta on säädetty EU-tasolla henkilötietodirektiivissä (Euroopan parlamentin ja neuvoston direktiivi (95/46/EY) yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta). Suomi on täyttänyt henkilötietodirektiivin vaatimukset säätämällä henkilötietolain (523/1999), joka astui voimaan 1.6.1999. [Pahlman, 2005]

Terveydenhuollossa tärkeässä roolissa oleva salassapito voidaan jakaa kahteen kokonaisuuteen, asiakirjasalaisuuteen ja vaitiolovelvollisuuteen. Asiakirjasalaisuudella tarkoitetaan salassa pidettävien tietojen antamista näyttämällä tai luovuttamalla salassa pidettäviä asiakirjoja sivullisen henkilön nähtäväksi tai käytettäväksi. Vaitiolovelvollisuudella tarkoitetaan muita tapoja ilmaista salassa pidettäviä tietoja. Terveydenhuollon asiakirjat ovat julkisuuslain (621/1999) perusteella salassa pidettäviä tietoja. Terveydenhuollon salassapidosta on säännöksiä myös potilaslaissa (785/1992, muutos 653/2000), erikoissairaanhoitolaissa (1062/1989, muutos 652/2000), laissa terveydenhuollon ammattihenkilöistä (559/1994) sekä laissa yksityisestä terveydenhuollosta (1521/1990). Potilaan tietoja saa luovuttaa sivullisille ainoastaan potilaan suostumuksella tai johonkin lakiin perustuvalla syyllä. [Pahlman, 2005; Pajukoski, 2004; Ylipartanen, 2004]

2.1.2. Potilasasiakirjojen laatiminen, säilyttäminen ja käsittely

Potilasasiakirjalla tarkoitetaan terveydenhuollossa käytettyä potilaan hoitoon liittyvää asiakirjaa tai teknistä tallennetta, joka sisältää tietoja potilaan terveydentilanteesta. Potilaslain 2 §:n 5 kohdassa [PotL, 1992] määritellään potilasasiakirja seuraavasti:

> *”potilasasiakirjoilla* potilaan hoidon järjestämisessä ja toteuttamisessa käytettäviä, laadittuja tai saapuneita asiakirjoja taikka teknisiä tallenteita, jotka sisältävät hänen terveydentilaansa koskevia tai muita henkilökohtaisia tietoja. ”

Potilasasiakirjoja ovat siten kaikki terveydenhuollon rekisterinpitäjän hallussa olevat potilaan hoitoon liittyvät tallenteet, asiakirjat, kortistot ja tulosteet, jotka sisältävät tietoja potilaan terveydentilasta ja joita käytetään potilaan hoidon suunnittelussa, toteuttamisessa tai järjestämisessä. Potilasasiakirjoja ovat mm. potilaskertomukset, lähetteet, kuvat ja laboratoriotutkimukset. Potilasasiakirjojen tehtävänä on parantaa potilaan hoidon jatkuvuutta ja tiedonvälitystä, myös silloin kun hoito tapahtuu eri toimintayksiköissä. Asiakirjoihin tehtävien merkintöjen tulee olla tarpeellisia, virheettömiä ja riittäviä. [Pahlman, 2005; PotL, 1992]

> Terveydenhuollossa potilasasiakirjojen huolellinen laadinta on sekä potilaan että hoitohenkilökunnan oikeusturvan kannalta keskeistä. Potilasrekisteri rakentuu potilaiden terveys- ja henkilötiedoista, joten sitä koskee henkilötietolain määräykset henkilörekisterin ylläpitämisestä. Terveydenhuollossa rekisterinpitäjänä toimii toimintayksikkö, jonka tarpeisiin asiakirjoja pidetään ja jolla on oikeus määrätä niiden käytöstä. Potilaan asemasta ja oikeuksista terveyden- ja sairaanhoitoa järjestettäessä säädetään potilaslaissa (785/1992). Sosiaali- ja terveysministeriö on antanut erillisen asetuksen potilasasiakirjojen laatimisesta (99/2001), jossa

määritellään tarkemmin potilasasiakirjojen luomiseen ja säilyttämiseen liittyviä asioita [Pahlman, 2005, Ylipartanen, 2004].

Potilaslain mukaan terveydenhuollon ammattihenkilön tulee merkitä potilasasiakirjoihin potilaan hoidon järjestämisen, suunnittelun, toteuttamisen ja seurannan kannalta tarpeelliset tiedot [PotL, 1992]. Potilasasiakirjoihin saa tehdä ainoastaan hoidon kannalta välttämättömiä merkintöjä. Merkintöjen tulee olla selkeitä ja ymmärrettäviä, ja niiden alkuperä tulee pystyä todistamaan. Asiakirjoihin merkittävien tietojen tulee olla myös virheettömiä ja ne pitää tehdä viivytyksettä. Osa potilasasiakirjoista tulee ammattilaisen allekirjoittaa omakätisesti tai varmennetulla digitaalisella allekirjoituksella, kuten esimerkiksi lähetteissä ja lausunnoissa. [PotL, 1992; Pahlman, 2005]

Potilasasiakirjoista keskeisin on potilaskertomus. Potilasasiakirja-asetuksessa säädetään, että jokaisesta potilaasta on pidettävä jatkuvaa potilaskertomusta. Potilaskertomukseen kerätään potilaan hoidon yhteydessä luodut erilaiset asiakirjat, kuten lähetteet ja röntgenlausunnot. Potilaan jokaisesta avohoitokäynnistä, osastohoitojaksosta ja terveydenhuollon ammattilaisen käynnistä potilaan luona on tehtävä merkintä potilaskertomukseen. Potilasasiakirja-asetuksessa myös säädetään, että potilaskertomuksen tulee olla alkuperäinen. Tämä tarkoittaa sitä, että merkintöjä ei saa poistaa tai korvata. Tietojärjestelmille tämä asettaa haasteen, että pitää pystyä turvaamaan potilaskertomuksen alkuperäisyys ja eheys [STM, 2001; Pahlman, 2005].

Terveydenhuollon toimintayksiköiden tulee suunnitella ja toteuttaa potilasasiakirjajärjestelmänsä siten, että sen rakenne ja tietosisältö vastaa potilasasiakirjojen käyttötarkoitusta. Potilasasiakirjajärjestelmiä rakennettaessa tulee tarkoin huomioida käyttöoikeudet. Käyttöoikeuksien on vastattava henkilökunnan tehtäviä ja vastuita sekä tietojen siirtämis- ja luovutustarpeita. Potilasasiakirjat tulee laatia ja säilyttää siten, että niiden eheys ja käytettävyys voidaan turvata läpi niiden elinajan. [STM, 2001]

Potilasasiakirjojen säilyttäminen on suuri haaste terveydenhuollon toimintayksiköille, koska säilytysajat ovat pitkiä ja tietojen eheys sekä luottamuksellisuus on turvattava. Vastuu potilasasiakirjojen säilyttämisestä on lähtökohtaisesti sillä terveydenhuollon toimintayksiköllä, jonka toiminnassa asiakirjat ovat syntyneet. Mikäli potilaan tietoja halutaan siirtää toiseen toimintayksikköön, niin pääsääntöisesti tulisi luovuttaa asiakirjasta ainoastaan kopio. [STM, 2001]

Potilasasiakirja-asetuksessa säädetään, että potilaskertomuksen tietoja on säilytettävä 10 vuotta potilaan kuoleman jälkeen tai jos siitä ei ole tietoa niin 100 vuotta potilaan syntymästä ja 10 vuotta hoidon päättymisen jälkeen. Eri potilasasiakirjoille on säädetty eripituisia säilytysaikavaatimuksia ja nämä selviävät potilasasiakirja-asetuksen liitteestä. Potilasasiakirjojen säilytyksessä toimintayksiköiden tulee varmistua, että potilasasiakirjat välttyvät tuhoutumiselta, vahingoittumiselta ja asiattomalta käytöltä. Säilytyksen jälkeen toimintayksiköiden on huolehdittava tietojen asianmukaisesta hävittämisestä välittömästi ja varmistuttava ettei tiedot päädy sivullisten tietoon. [STM, 2001; Pahlman, 2005; Ylipartanen, 2004]

Potilasasiakirjojen käsittelyä ohjaavat velvoitteet ja vaatimukset tulevat henkilötietolaista, koska potilasasiakirjat muodostavat henkilörekisterin. Toki terveydenhuollon erityislait ja säädöksetkin asettavat vaatimuksia ja velvoitteita tietojen käsittelylle, kuten esimerkiksi potilaslaki ja potilasasiakirja-asetus. Potilastietojen käsittelyä koskevat lait ovat voimassa huolimatta siitä, tapahtuuko tietojen käsittely paperilla vai sähköisessä muodossa. Henkilötietolain periaatteista voidaan katsoa tulevan seuraavat oleelliset vaatimukset terveydenhuollon tietojenkäsittelylle [Itälä ja Ruotsalainen, 2004]:

- etukäteissuunnittelun vaatimus
- huolellisuus- ja suojaamisvelvoite
- virheettömyys-, eheys-, ja luotettavuusvaatimus
- käyttötarkoitussidonnaisuus
- tarpeellisuusvaatimus

- yhteysvaatimus.

Otettaessa käyttöön tietojärjestelmiä on terveydenhuollon organisaatioiden otettava huomioon, että henkilötietolaissa sekä viranomaisten toiminnan julkisuudesta annetussa laissa on määritelty henkilötietojen käsittelylle *etukäteissuunnittelun* vaatimus [Itälä ja Ruotsalainen, 2004; HetiL, 1999]. Henkilötietojen kerääminen ja käsittely on suunniteltava huolellisesti etukäteen. Suunnittelulla tarkoitetaan, että tietojen käyttötarkoitus on määritelty. Lisäksi tulee määritellä tietojen käsittelyyn liittyvien menettelyjen kuvaukset käsittelyn eri vaiheissa sekä arvioida toimintaan sisältyvät tietosuojariskit [Pajukoski, 2004; HetiL, 1999]. Potilasasiakirja-asetuksessa täsmennetään vielä, että terveydenhuollon toimintayksikön tulee rekisterinpitäjänä suunnitella potilasasiakirjajärjestelmänsä siten, että se vastaa rakenteeltaan ja tietosisällöltään potilasasiakirjojen käyttötarkoitusta. [Pahlman, 2005]

Henkilötietolaissa on henkilötietojen käsittelylle *huolellisuus- ja suojaamisvelvoite*. Potilasasiakirjoissa käsitellään ihmisten arkaluontoisia tietoja, jotka ovat salassa pidettäviä. Potilassuhde on siis luottamuksellinen ja potilaalla on oikeus yksityisyyden suojaan, joten potilasasiakirjoja on käsiteltävä (mm. laatiminen, säilyttäminen, käyttäminen sekä luovuttaminen) huolellisesti [Itälä ja Ruotsalainen, 2004]. Huolellisuusvaatimukseen liittyy myös, että rekisterinpitäjän on ohjeistettava henkilötietojen käsittely. Lisäksi organisaatiossa on määriteltävä käyttöoikeudet. Potilasasiakirja-asetuksessa on nimenomaisesti vielä säädetty, että terveydenhuollon toimintayksikön johtajan on rekisterinpitäjän ominaisuudessa annettava kirjalliset ohjeistukset potilasasiakirjojen käsittelystä ja menettelytavoista. [Pahlman, 2005; STM, 2001]

Potilaan hoidon turvaamiseksi ja hoitohenkilökunnan oikeusturvan takaamiseksi rekisterinpitäjän velvollisuus on huolehtia käsiteltävien tietojen *virheettömyydestä, eheydestä ja luotettavuudesta*. Henkilörekisterinpitäjän tulee varmistua, että ei käsitellä tietoja jotka ovat virheellisiä, epätäydellisiä tai vanhentuneita [HetiL, 1999; Ylipartanen, 2004]. Henkilötietolain perusteella

tietoja luovutettaessa luovuttajan on huolehdittava luovutettavien tietojen virheettömyydestä ja tiedon saajan on varmistettava luovutettujen tietojen alkuperä ja muuttumattomuus [Itälä ja Ruotsalainen, 2004]. Potilasasiakirja-asetuksen mukaan toimintayksiköllä on velvollisuus huolehtia potilasasiakirjojen käytettävyydestä ja muuttumattomuudesta. Lisäksi potilasasiakirjat on laadittava ja säilytettävä sellaisia välineitä ja menetelmiä hyödyntäen, että tietojen eheys ja käytettävyys voidaan varmistaa. [Pahlman, 2005, Ylipartanen, 2004]

Käyttötarkoitussidonnaisuudella tarkoitetaan henkilötietolaissa, että kerättyjä tietoja käytetään tai luovutetaan ainoastaan siihen tarkoitukseen kuin ne on alun perin kerätty [HetiL, 1999; Itälä ja Ruotsalainen, 2004; Ylipartanen, 2004]. *Tarpeellisuusvaatimuksella* tarkoitetaan, että kaikkien potilasasiakirjojen merkintöjen on oltava potilaan hoidon kannalta tarpeellisia. Potilaslaissa ja potilasasiakirja-asetuksessa on säädetty, että potilasasiakirjoihin tulee merkitä hyvän hoidon järjestämisen, suunnittelun, toteuttamisen ja seurannan turvaamiseksi tarpeelliset tiedot. [Ylipartanen, 2004; Itälä ja Ruotsalainen, 2004]

Yhteysvelvoitteella tarkoitetaan, että potilasasiakirjaa käsittelevällä henkilöllä on oltava hoitosuhde tai muu asiallinen yhteys potilaaseen. Potilaslaissa on määritelty, että terveydenhuollon toimintayksikössä potilasasiakirjoja saa käsitellä ainoastaan ne henkilöt, jotka osallistuvat potilaan hoitoon tai siihen liittyviin tehtäviin, asianomaisessa toimintayksikössä tai sen toimeksiannosta. Lisäksi potilasasiakirja-asetuksessa todetaan, että tietoja saa käsitellä ainoastaan siinä laajuudessa kuin työtehtävät tai vastuu edellyttää. Asetuksessa edellytetään myös, että rekisterinpitäjän on valvottava ATK:lla toimivien järjestelmien käyttöä riittävillä teknisillä menetelmillä, kuten esimerkiksi lokitiedostojen avulla. Potilaan suostumuksella tietoja voidaan kuitenkin luovuttaa. [Pahlman, 2005]

2.1.3. Potilastietietojen luovutus ja suostumus

Potilastiedot ovat lain mukaan salassa pidettäviä tietoja, koska tavoitteena on suojata potilaan yksityisyyttä. Salassapidosta voidaan pääsääntöisesti poiketa ainoastaan potilaan suostumuksella tai lainsäädäntöön perustuvalla syyllä. Laissa sosiaali- ja terveydenhuollon saumattoman palveluketjun kokeilusta (811/2000) suostumus määritellään, että se perustuu asiakkaalle annettuun riittävään tietoon ja on vapaaehtoinen, yksilöity, tietoinen ja todennettavissa oleva tahdonilmaisu, jolla rekisteröity hyväksyy henkilötietojensa käsittelyn.

Potilaslakiin on määritelty perussäännökset potilaan tietojen luovuttamista varten. Sen mukaan pääsääntö on, että terveydenhuollon ammattilainen tai muu toimintayksikössä työskentelevä henkilö ei saa luovuttaa potilasasiakirjoihin sisältyviä tietoja sivulliselle ilman potilaan tai hänen laillisen edustujansa kirjallista suostumusta. Sivullisella tässä tarkoitetaan henkilöä, joka ei osallistu potilaan hoitoon tai siihen liittyviin tehtäviin asianomaisessa terveydenhuollon toimintayksikössä. [PotL, 1992; Sorvari, 2004, Ylipartanen, 2004]

Potilaan suostumukselta edellytetään etukäteisyyttä sekä vapaaehtoisuutta, lisäksi suostujaa on informoitava tiedon luovuttajasta, kenelle tiedot luovutetaan, mitä tietoa luovutetaan sekä miksi tietoa luovutetaan. Koska suostumuksen tulee olla yksilöity, niin potilaan saapuessa sairaalaan ei häneltä voida pyytää yleistä suostumusta, koska hän ei voi tietää mitä luovutettuja tietoja suostumus koskee [Sorvari, 2004, Ylipartanen, 2004].

Suostumus voi myös olla suullinen tai asiayhteydestä ilmenevä, mikäli se on tarpeellista potilaan hoidon järjestämiseksi. Käytännössä asiayhteydestä ilmenevällä suostumuksella tarkoitetaan esimerkiksi päännyökkäystä, kun potilaalle on kerrottu tietojen luovuttamiseen liittyvät tiedot. Terveydenhuollon ammattihenkilön on kuitenkin tehtävä potilasasiakirjoihin merkintä potilaan yksilöidystä suostumuksesta. Hoitoon hakeutuminen ei ole suostumus hoidon yhteydessä syntyneiden tietojen luovuttamiselle. [Pahlman, 2005, Ylipartanen, 2004] Poikkeuksina pääsääntöön on tilanteet, jossa potilas ei voi esimerkiksi tajuttomuuden tai muun vastaavan syyn vuoksi antaa

suostumustaan tai kun täysi-ikäinen henkilö ei pysty päättämään hoidostaan esimerkiksi kehitysvamman tai mielenterveyshäiriön takia [Pajukoski, 2004, Ylipartanen, 2004; PotL, 1992].

Erikoissairaanhoitolain 10 b §:n perusteella tietoja voidaan luovuttaa ilman potilaan suostumusta hänen hoitoon liittyvissä tilanteessa. Tämä mahdollistaa sen, että erityissairaanhoidon toimintayksikön tuottaessa palveluita, esimerkiksi laboratorio- ja röntgenpalveluita tai muita vastaavia erityispalveluita, sairaanhoitopiirinsä muille toimintayksiköille, niin erityissairaanhoitoyksikkö voi toimia palvelussa syntyneiden tietojen rekisterinpitäjänä. Tällöin tietoja voidaan käyttää potilaan saapuessa myöhemmin erikoissairaanhoidon yksikköön potilaiksi. Palveluja tilaavalla toimintayksiköllä on oikeus luovuttaa palveluja tuottavalle yksikölle sen palvelun toteuttamisessa tarvittavat tiedot ilman potilaan suostumusta. Lisäksi palvelun tuottajalla on oikeus luovuttaa palvelun tilaajalle palvelun tuottamisessa syntyneet tiedot. [Pahlman, 2005]

Potilastietoja luovutettaessa luovuttaja vastaa, että luovutus on laillinen ja tietosuoja on huomioitu riittävällä tarkkuudella. Luovuttajan tulee myös varmistua vastaanottajan tietojen käyttötarkoituksesta ja luovuttamisen asianmukaisesta perusteesta. Mikäli luovutuspyyntöä ei ole perusteltu tai rajattu riittävällä tarkkuudella tulee luovuttajan pyytää tarkennukset tiedon pyytäjältä ennen luovutusta [Pahlman, 2005; Ylipartanen, 2004]. Luovutuspyynnössä tulee ilmetä seuraavat asiat:

- selvitys pyytäjän oikeudesta tietojen saantiin
- potilaan täydellinen nimi ja henkilötunnus tai syntymäaika
- yksilöitynä tiedot/asiakirjat, joita pyytäjä haluaa
- tietojen käyttötarkoitus
- tarvittaessa selvitys siitä, miten tietojen suojaus järjestetään sekä
- pyytäjän nimi ja osoite, johon tiedot toimitetaan [Ylipartanen, 2004].

Henkilötietolain perusteella tiedon luovuttajalla on vastuu, että luovutettavat tiedot ovat virheettömiä ja etteivät ne joudu sivullisten käsiin. Riitatilanteessa tietoja luovuttaneella on lähtökohtaisesti näyttövelvollisuus, siitä että luovutus on tapahtunut lainmukaisesti. Luovutuksen saajan velvollisuuksiin kuuluu varmistua tietojen alkuperästä sekä muuttumattomuudesta. Potilasasiakirja-asetuksen mukaan molempien osapuolien on tehtävä potilasasiakirjoihin luovutuksesta merkintä [Itälä ja Ruotsalainen, 2004; Ylipartanen, 2004; STM 2001; HetiL, 1999]. Toimintayksikön terveydenhuollosta vastaavan johtajan tulee antaa tarkat ohjeistukset potilasasiakirjojen luovuttamisesta sekä valita siitä vastaavat henkilöt. Potilastietoja voidaan luovuttaa sähköisesti, mikäli riittävästä salauksesta on huomioitu. [Pahlman, 2005]

Potilaan terveystietoja voidaan luovuttaa hoitoon liittymättömissä tilanteissa, mikäli luovutuksen katsotaan muiden henkilöiden edun, yleisen edun tai muiden painavien syiden takia olevan perusteltua. Tällöin luovutuksesta on säädetty nimenomaisesti laissa. Näitä lainsäännöksiä on Suomessa melko runsaasti, esimerkiksi tietoja voidaan luovuttaa tutkimuskäyttöön ja lääkärillä on velvollisuus ilmoittaa ajo-oikeuksista vastaavalle poliisille todetessaan potilaan terveydentilan muutoksen rikkovan ajokorttiluvan myöntämisen edellytyksenä olevia terveysvaatimuksia. [Pahlman, 2005]

2.2. Tietoturva

Tietoturvallisuudella tarkoitetaan tiedoista, tietojärjestelmistä, tietoliikenteestä sekä henkilöistä aiheutuvien riskien hallintaa. Tietoturvan tavoitteena on taata tiedon luottamuksellisuus, eheys, oikeellisuus sekä kiistämättömyys koko niiden käsittelyn ja säilytyksen ajan. Tietoturvallisuus on toiminnallinen kokonaisuus, jonka perustana ovat organisaation turvallisuuskulttuuri ja ihmisten toiminta. Tietoturvallisuus on laaja käsite, joka ei koske pelkästään teknisiä ratkaisuja, kuten laitteistoa ja sovelluksia, vaan siihen oleellisesti kuuluvat myös ihmisten toiminta ja turvatoiminnan yleiset järjestelyt. [VAHTI, 2004a]

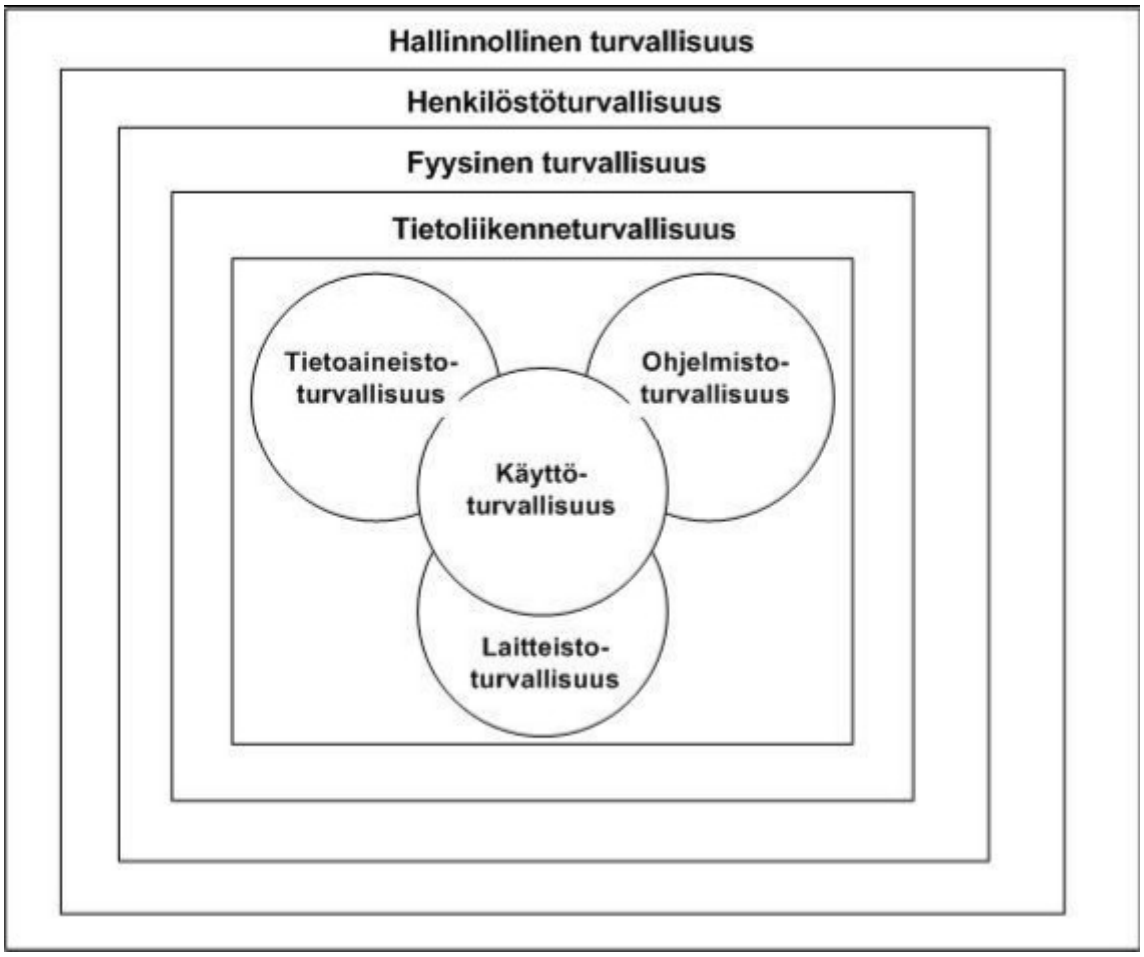
Organisaation tieto ja tietojärjestelmät ovat sen toiminnan ja toimintakyvyn kannalta olennainen osa. Tietoturvallisuuden lähtökohtana on turvata tiedon käytettävyys, eheys ja luottamuksellisuus. Tärkeiden tietojärjestelmien kohdalla näiden kolmen ominaisuuden vaaliminen on elinehto, koska ilman niitä järjestelmiä ei voida käyttää missään kriittisessä sovellusalueessa [Paavilainen, 1998].

Kaikista järjestelmien ja käyttäjien tekemistä toimista on jäätävä sellainen tieto järjestelmään, että myöhemmin voidaan todeta mitä ja milloin on tehty ja kenen toimesta. Organisaation tulee rakentaa kontrollit, joilla pystytään seuraamaan tietojärjestelmien ja käyttäjien toimintaa. Kontrollit tukevat tietoturvasta vastaavien henkilöiden toimintaa ja ylläpitävät prosessien käyttämien tietojen turvallisuutta [Tammisalo, 2005]. Tammisalon [2005] raporttia voidaan pitää ISO/IEC 17799: 2005 "Code of Practice for Information Security Management" (http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39612) standardin suomalaistettuna versiona.

Tietoturvallisuus voidaan jakaa usealla eri tavalla. Valtion tietoturvapäätöksissä käytetään jakoa seitsemään eri turvallisuuden osaan. Nämä osat ovat:

- hallinnollinen tietoturvallisuus
- henkilöstöturvallisuus
- fyysinen turvallisuus
- tietoliikenneturvallisuus
- laitteistoturvallisuus
- ohjelmistoturvallisuus
- tietoaineistoturvallisuus
- käyttöturvallisuus [VAHTI, 2004a].

Kuvassa 3. on nähtävillä eri turvallisuuden osien suhteet toisiinsa. Näistä osista kokonaisuutena muodostuu tietoturvallisuus [Reponen, 2006].



Kuva 3. Tietoturvallisuuden eri osien suhteet toisiinsa [Jokinen, 1999, s 178].

Hallinnollisella tietoturvalla tarkoitetaan keinoja, joiden tähtäimenä on parantaa organisaation tietoturvallisuutta. Lähtökohtana toimii organisaation tietoturvapolitiikka, johon määritellään tietoturvatoiminnalle suuntaviivat ja turvallisuutta parantavat toimenpiteet. Hallinnollisella tietoturvalla pyritään analysoimaan eri riskit, jotka kohdistuvat tietojärjestelmiin, sekä luomaan organisaatioon toimintatavat, joilla pyritään ehkäisemään tietoturvariskien muodostuminen [Paavilainen, 1998].

Toimintatavat ja erilaiset tietoturvakäytännöt tulee tiedottaa koko henkilöstölle, ja varmistaa, että ne on tunnistettu ja niitä noudatetaan. Organisaation tulee määritellä tietoturvallisuuden kehittämiseen ja

toteuttamiseen liittyvät tehtävät ja vastuualueet, sekä varata riittävät resurssit tietoturvatyölle. Suojattavat tietojärjestelmät ja käytetyt tietoturvaratkaisut pitää dokumentoida kokonaisuudessaan. Oleellinen osa hallinnollista tietoturvaa on myös henkilökunnan jatkuva koulutus sekä tietoturvatavoitteiden ja –periaatteiden tehokas tiedottaminen organisaation sisällä. Organisaation tietoturvatoimintaa tulee seurata, valvoa ja mitata säännöllisesti. [Tammisalo, 2005; VAHTI, 2004b].

Henkilöstöturvallisuudella tarkoitetaan henkilöstöön liittyvien tietoriskien hallintaa. Henkilöstöön liittyviä riskejä voidaan hallita henkilöstön soveltuvuuden, toimenkuvien, sijaisuuksien, tiedonsaanti- ja käyttöoikeuksien, turvallisuuskoulutuksien ja valvonnan avulla [VAHTI, 2004b]. Henkilöstöturvallisuus on erittäin tärkeässä osassa organisaation turvallisuutta suunniteltaessa, koska henkilöstö on yksi tärkeimmistä yrityksen voimavaroista samalla ollen suurin turvallisuutta uhkaava tekijä. Henkilöstöturvallisuuteen kuuluu sekä omien työntekijöiden että vierailijoiden valvonta [Paavilainen, 1998]. Tarkoituksena on estää inhimillisen toiminnan aiheuttamat tietoturvavahingot, kuten inhimilliset virheet, väärinkäytökset ja varkaudet. Työntekijöistä aiheutuvia riskejä voidaan kontrolloida tekemällä uusille työntekijöille taustatarkistuksia, varmistamalla heidän sopivuutensa työnkuvaan sekä järjestämällä ennalta suunniteltu perehdyttämiskoulutus. [VAHTI, 2004b]

Fyysinen turvallisuus sisältää henkilöiden, laitteiden, aineistojen, toimitilojen ja varastojen yms. suojaamisen erilaisilta vahingoilta ja tuhoilta. Fyysisellä turvallisuudella ehkäistään riskejä, joita voi aiheutua valtuudettomasta pääsystä organisaation tiloihin, tietoihin ja tietojärjestelmiin tai fyysisestä ympäristöstä kuten vesivahingot ja virransyöttöongelmat [Tammisalo, 2005].

Tietoliikenneturvallisuudella tarkoitetaan toimia, joiden tavoitteena on turvata organisaation tietoliikenne ja varmistaa välitettävien tietojen luottamuksellisuus, eheys ja käytettävyys. Paavilainen [1998] listaa neljä päämäärää tietoliikenneturvallisuudelle. Tarkoituksena on varmistaa:

- sanomien alkuperäisyys, koskemattomuus ja luottamuksellisuus
- lähettäjä ja vastaanottaja sekä todentaa heidät
- tietoliikennelaitteiden fyysinen turvallisuus
- väärinreitityksen estäminen.

Tietoliikenneturvallisuuteen kuuluvat kaikki asiat, jotka liittyvät tietoliikenteeseen, verkkojen rakentamiseen ja suunniteluun. Siihen vaikuttavat käytettävät protokollat, salausmenetelmät, verkkotopologiat sekä tietoturvatuotteet, kuten reitittimet ja palomuurit [Paavilainen, 1998].

Laitteistoturvallisuuden tavoitteena on taata organisaation tietojenkäsittely- ja tietoliikennelaitteiden käytettävyys ja toimivuus. Tarkoituksena on suojata laitteistot siten, että mahdollisuudet niiden varastamiseen ja vahingoittumiseen on estetty [VAHTI, 2004b]. *Ohjelmistoturvallisuudella* tarkoitetaan toimia, jotka kohdistuvat käyttöjärjestelmiin sekä organisaation käyttämiin muihin ohjelmistoihin. Organisaatioiden pitää huomioida sovelluksien koko elinkaaren liittyvät tietoturvakysymykset. Ohjelmistojen hankinnat, kehitystyöt, käyttöönotot, ylläpitotoimet ja alasajot tulee olla huolella suunniteltuja tietoturvallisia prosesseja [VAHTI, 2004b]. Kaikki organisaatioiden ohjelmistoihin liittyvät muutos-, ylläpito- ja kehitystyöt on dokumentoitava huolellisesti [Tammisalo, 2005].

Tietoaineistoturvallisuudella tarkoitetaan toimia, joiden tavoitteena on turvata asiakirjojen, tiedostojen ja muiden tietoaineistojen käytettävyys, eheys ja luottamuksellisuus. Organisaatioiden kaikki tieto, joka on toiminnan kannalta merkittävää, on suojattava sekä dokumentoitava. Organisaation tiedot ja tietojärjestelmät on suojattava siten, että työntekijöillä on pääsy vain niihin tietoihin, jotka ovat välttämättömiä heidän työtehtäviensä kannalta [VAHTI, 2004b; Tammisalo 2005].

Käyttöturvallisuuden tavoitteena on parantaa tietotekniikan käytön, käyttöympäristön, tietojenkäsittelyn ja ylläpidon turvallisuutta. Tietojärjestelmien käyttöä ja tilaa on valvottava suunnitelmallisesti, jotta mahdollisiin vikatilanteisiin voidaan reagoida riittävällä nopeudella.

Seurantatietoja voidaan käyttää hyväksi järjestelmien suunnittelutyössä [VAHTI, 2004b; Tammisalo, 2005].

2.2.1. Tiedon eheys, luottamuksellisuus ja saatavuus

Organisaatioiden tietovarannot sijaitsevat monimuotoisessa ympäristössä, joka koostuu erilaisista liiketoimintaprosesseista, teknologioista, lainsäädännöllisistä vaatimuksista, toiminta-alueen paineista sekä turvallisuusuhkista. Tietoa liikkuu erilaisten järjestelmien välillä tietoverkkojen, tietokantojen, sekä palvelimien avulla, tavoitteena on täyttää organisaation toiminnan tarpeet. Tietovarantojen monimutkaisuus asettaakin paineita tiedon saatavuudelle ja käytettävyydelle, eheydelle sekä luottamuksellisuudelle. Tietoturvan tavoitteena onkin turvata näiden tekijöiden olemassaolo. [Sullivan, 2004]

Tiedon saatavuudella tarkoitetaan, että tietovarannot ovat saatavissa aina ajasta ja paikasta riippumatta. Tietovarantojen saatavilla olo tulee turvata myös erilaisissa poikkeus- ja häiriötilanteissa. Tämä vaatii huolellista suunnittelua ja testausta. Yhden komponentin rikkoutuminen tai erilaisten tietoturvahyökkäysten kohteeksi joutuminen, ei saa vaarantaa koko tietojärjestelmän toimintaa, joten huolto- ja ylläpitotoiminnot on kyettävä suorittamaan käyttöä häiritsemättä [VAHTI, 2004b]. Saatavuus sisältää myös sen, että tiedot on tallennettu sellaisessa muodossa, että ne ovat luettavissa ja ymmärrettävissä. Tällöin pitää taata, etteivät käytetyt tallennusformaatit ole vanhentuneet ja ettei tiedon tallennusmuoto aiheuta tulkintaongelmia [Tammisalo, 2005].

Tiedon eheyden turvaamisella tarkoitetaan, että tiedot ovat täydellisiä ja muokkaamattomia. Organisaatioissa monet eri sovellukset voivat käsitellä samaa tietoa, joten eheyden takaaminen on usein ongelmallista ja se vaatii laajaa ymmärrystä organisaation tietovarannoista ja tietovirroista [Sullivan, 2004]. Tiedot eivät saa vahingossa muuttua tai korruptoitua tietojärjestelmien

tai niiden osien vioittumisen takia. Tietoja täytyy myös turvata väärentämiseltä. Tiedon eheyden rikkoutumisen havaitseminen on usein erittäin vaikeaa ja se aiheuttaa mahdollisesti erittäinkin suuria haittavaikutuksia. Tämän takia tiedon eheyden turvaaminen katsotaankin yhdeksi suurimmista tavoitteista tietoturvassa. [Paavilainen, 1998; Tammisalo, 2005; Tammisalo, 2007]

Eheyden vaatimus antaa tiedoille kolme uutta ominaisuutta alkuperäisyys, kiistämättömyys ja koskemattomuus. Alkuperäisyyden takaamiseksi pitää organisaation pystyä varmistamaan, että tieto on tullut sieltä mistä sen väitetäänkin tulleen. Tiedon kiistämättömyyden takaamiseksi on olemassa menetelmiä, joilla voidaan asiakirjan tekijä kiistämättömästi todentaa, ja joilla tietoihin voidaan liittää tekoajan tai muuttumishetken aikaleima, kuten esimerkiksi sähköinen allekirjoitus. Tietojärjestelmien sisäisen tiedonkäsittelyn ja tiedon siirtojen eheyden ylläpitoon ja käytettävän tiedon oikeellisuuden tarkistamiseen on olemassa erilaisia menetelmiä. Näillä keinoilla voidaan varmistaa tiedon koskemattomuus, ettei sitä ole missään vaiheessa muokattu tai muutettu. Täyttämällä nämä kolme tiedon ominaisuutta, voidaan organisaatiossa turvata tiedon eheys. [Paavilainen, 1998; Tammisalo, 2005, Tammisalo, 2007]

Organisaatioiden tietoturvan tavoitteena on myös tietojen luottamuksellisuuden turvaaminen. Luottamuksellisuudella tarkoitetaan, että tiedot ovat vain niihin oikeutettujen henkilöiden ja organisaatioiden saatavilla, eikä niitä paljasteta muille [Paavilainen, 1998]. Tietojärjestelmissä usein käsitellään arkaluontoisia tai salassa pidettäviä tietoja. Luottamuksellisuuden säilyttämiseksi organisaatioiden tulee kehittää turvaluokitukset eri tiedoilleen [VAHTI, 2004a]. Tietoja käyttävillä henkilöillä pitää olla riittävät valtuudet niiden käsittelemiseen. Organisaation tietovarannot pitää luokitella, jotta voidaan oikeille henkilöille antaa valtuudet tietyn tiedon käsittelemiseksi. Tämän lisäksi kaikki henkilöt on tunnistettava ja todennettava, jotta voidaan määritellä heidän oikeudet ja valtuudet tietojärjestelmään. Organisaation tulee myös määritellä tietojen käsittelytavat ja –säännöt [Tammisalo, 2005].

2.2.2. Tietoturva ja lainsäädäntö

Lainsäädäntö asettaa terveydenhuollon toimintayksiköille vaatimuksia ja velvoitteita liittyen tietojenkäsittelyn tietoturvallisuuteen. Lähtökohtaisesti kaikki potilasrekistereihin tallennetut tiedot ovat salassa pidettäviä, joten toimintayksiköiden on huolehdittava tietojen riittävästä suojaamisesta. Henkilötietolain 32 pykälässä on vaatimus rekisterinpitäjälle henkilötietojen suojaamisesta:

> "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 huomioon käytettävissä olevat tekniset mahdollisuudet, toimenpiteiden aiheuttamat kustannukset, käsiteltävien tietojen laatu, määrä ja ikä sekä käsittelyn merkitys yksityisyyden suojan kannalta."

Laissa viranomaistoiminnan julkisuudesta pykälässä 18 säädetään hyvästä tiedonhallintatavasta. Hyvällä tiedonhallintatavalla asetetaan viranomaiselle velvollisuus huolehtia tietojen käsittelystään. Tavoitteena on, että viranomaiset huolehtivat toimintaansa liittyvien asiakirjojen ja tietojärjestelmien saatavuudesta, käytettävyydestä, laadusta –eli eheydestä sekä asianmukaisesta suojauksesta. Lisäksi viranomaisen tulee tietojen käsittelyssään pyrkiä ottamaan huomioon tietoihin liittyvät erilaiset intressit, kuten asiakirjojen julkisuus ja salassapito, arkistointi ja säilytys, henkilötietojen suoja ja tietojen käyttörajoitukset sekä tietoturvallisuus. Julkisuuslaki koskee ainoastaan julkisia terveydenhuollon toimijoita ja se ei siis vaikuta yksityisiin terveydenhuollon toimintayksiköihin. [JulkL, 1999; Korhonen, 2003; Ylipartanen, 2004]

Julkisuuslaissa [JulkL, 1999] listataan viisi erityistä velvoitetta viranomaiselle hyvän tiedonhallintatavan toteuttamiseksi. Viranomaisen tulee:

1. pitää luetteloa käsiteltävistä ja käsitellyistä asioista, sekä huolehtia julkisten asiakirjojen vaivattomasta saatavuudesta;
2. laatia ja pitää saatavilla kuvaukset tietojärjestelmistä sekä niistä saatavissa olevat julkiset tiedot;
3. selvittää tietojärjestelmien käyttöönottoa sekä hallinnollisia ja lainsäädännöllisiä uudistuksia valmisteltaessa suunniteltujen toimenpiteiden vaikutus asiakirjojen julkisuuteen, salassapitoon ja suojaan sekä tietojen laatuun samoin kuin ryhtyä tarpeellisiin toimenpiteisiin tietoon liittyvien oikeuksien ja tiedon laadun turvaamiseksi sekä asiakirjojen ja tietojärjestelmien sekä niihin sisältyvien tietojen suojan järjestämiseksi;
4. suunnitella ja toteuttaa asiakirja- ja tietohallinto, tietojärjestelmät sekä tietojenkäsittelyt siten, että tiedot arkistoidaan tai hävitetään asianmukaisesti, tietojen suoja, eheys ja laatu turvataan asianmukaisin menettelytavoin ja tietoturvallisuusjärjestelyin, huomioiden tietojen merkitys, käyttötarkoitus, uhkatekijät sekä tietoturvallisuustoimenpiteistä aiheutuvat kustannukset;
5. huolehtia siitä, että henkilökunnalla on riittävä tieto käsiteltävien asiakirjojen julkisuudesta sekä tietojen antamisessa että käsittelyssä sekä asiakirjojen ja tietojärjestelmien suojaamisessa noudatettavista menettelyistä ja tietoturvallisuusjärjestelyistä, samoin kuin että hyvän tiedonhallintatavan noudattamiseksi luotujen sääntöjen ja ohjeistuksien toteutumista valvotaan.

Hyvästä tiedonhallintatavasta on julkisuuslain lisäksi säädetty asetuksessa viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (1030/1999). Asetuksen ensimmäisessä pykälässä velvoitetaan viranomainen tekemään suunnitelma, miten hyvä tiedonhallintatapa toteutetaan ja samalla selvittämään ja arvioimaan asiakirjansa ja tietojärjestelmänsä, sekä niihin

talletetut tiedot ja niiden merkitykset. Samalla on myös huomioitava, miten toteutetaan arkaluontoisten ja salassa pidettävien tietojen suojaaminen, tietojen käyttötarkoituksia koskevat rajoitukset ja tietojen käytettävyys, eheys sekä laatu. Lisäksi viranomaisen on selvitettävä ja arvioitava tietoihin ja tietojärjestelmien turvallisuuteen kohdistuvat uhat sekä millä keinoin uhkia voidaan vähentää ja poistaa. [JulkA, 1999]

Asetuksen toisessa pykälässä viranomainen velvoitetaan luokittelemaan erityissuojattavat tietoaineistot. Erityissuojattavilla tietoaineistoilla tarkoitetaan asiakirjoja ja niihin sisältyviä tietoja, joiden luovuttamista on rajoitettu lainsäädännössä tai niitä saa käyttää vai määrättyyn tarkoitukseen. Erityissuojattavia tietoaineistoja varten viranomaisen tulee toteuttaa asianmukaiset toimenpiteet, joita ovat [JulkA, 1999]:

- tietoaineistojen ja tietojenkäsittelytilojen riittävä valvonta ja suojaus
- tietojärjestelmiin pääsy on valvottu, sekä luvaton tunkeutuminen niihin on estetty käytettävissä olevilla keinoilla
- ainoastaan asianmukaiset henkilöt pääsevät käyttämään, käsittelemään ja muuttamaan tietoaineistoja, sekä käyttöoikeuksien rajaus on tehty asianmukaisesti ja käytön valvonta on riittävää
- tietoja aineistoista saavat luovuttaa ainoastaan ne henkilöt, keiden tehtäviin asia kuuluu
- tietoverkoissa siirrettävä tieto on salattava tarpeen mukaan.

Lisäksi asetuksessa [JulkA, 1999] määritellään, että organisaatioiden on annettava henkilökunnalleen toimintaohjeet liittyen tietojenkäsittelyn jokaiseen vaiheeseen sekä määriteltävä asiakirjojen luovuttamiseen liittyvät vastuut.

Suomen lainsäädäntö asettaa terveydenhuollon yksiköille velvollisuuden suunnitella, turvata ja valvoa tietojenkäsittelyään läpi tietojen elinkaaren, riippumatta siitä tapahtuuko käsittely sähköisesti vai manuaalisesti. Erilaisten velvoitteiden ja rajoituksien tarkoituksena on turvata sekä ammattilaisen, että potilaan oikeusturvaa. Tietoturvallisuudessa on aina varmistuttava, että voidaan toteuttaa sekä rekisteröidyn oikeudet että rekisterinpitäjän velvollisuudet. [Ylipartanen, 2004]

2.2.3. Tietoturva terveydenhuollossa

Terveydenhuolto on tietokeskeistä toimintaa, jossa useat eri organisaatiot tuottavat jatkuvasti suuria määriä tietoa. Tuotettava tieto on pääsääntöisesti salassa pidettävää ja rakenteeltaan monimuotoista. Tiedon käsittelyä varten on kehitetty organisaatioihin erilaisia tietojärjestelmiä, jotka pääasiallisesti toimivat omissa suljetuissa ympäristöissään. Tiedon ollessa sähköisessä muodossa on se alttiimpaa erilaisille tietoturvaloukkauksille, koska tietoon voi päästä käsiksi ajasta ja paikasta riippumatta. [Tammisalo, 2007; Grimson et al., 2000]

Terveydenhuollon tietojärjestelmät ovat tällä hetkellä suuren muutoksen ja kehityksen kohteena. Potilaita hoidetaan useilla eri osastoilla ja organisaatioissa, mistä voi aiheutua ongelmia, koska potilastiedot eivät välttämättä liiku potilaan mukana. Tiedon liikkumisen varmistamiseksi terveydenhuollon tietojärjestelmistä pyritään rakentamaan yhteistoiminnallisia integroituja kokonaisuuksia. Yhteistoiminnallisuuden tavoitteena on saada eri organisaatioiden ja hoitoyksiköiden yhteistyö parantumaan luomalla järjestelmistä toimivia kokonaisuuksia [Nordberg, 2004]. Yhteistoiminnallisuus on Suomessa nostettu keskeiseksi tavoitteeksi jo vuonna 1996 julkaistussa suomalaisen sosiaali- ja terveydenhuollon tietoteknologian hyödyntämisstrategiassa. Yhteistoiminnallisuuden takaamiseksi on Suomessa pyritty tekemään yhteisiä linjauksia käytettävistä standardeista, joiden avulla yhteistoiminnallisuus voidaan toteuttaa [STM, 2003].

Integroitujen järjestelmien avulla voidaan parantaa potilaiden hoidon laatua sekä lisätä tehokkuutta. Tietojärjestelmien yhteistoiminnallisuus parantaa tiedon liikkuvuutta, mutta samalla aiheuttaa suuria paineita tietoturvalle, koska potilaiden arkaluontoiset tiedot liikkuvat vapaammin hoitoyksiköiden välillä. Terveydenhuollon organisaatioille syntyykin suuri vastuu järjestelmien tietoturvan ja tiedon laadun turvaamiseksi, koska kaiken tiedon liikkumisen

tulee tapahtua lainmukaisesti, tietoturvallisesti ja siten että potilaan yksityisyyttä ja itsemääräämisoikeutta kunnioitetaan. [Blobel and Pharow, 2000; Grimson et al., 2000].

Hustonin [2001] mielestä tekniset kysymykset liittyen terveydenhuollon tietojärjestelmiin on pystytty suurelta osin ratkaisemaan, tämän takia Huston [2001] nostaakin terveydenhuollon tietojärjestelmien kannalta tärkeäksi ei-tekniset haasteet. Suurimmiksi haasteiksi nousevat lainsäädännölliset kysymykset liittyen tiedon liikkumiseen organisaatioiden välillä ja vastuiden määrittäminen osallistuvissa organisaatioissa liittyen tiedon suojaamiseen ja ylläpitämiseen, hoitohenkilökunnan koulutus sekä tietoturva vastuiden määritteleminen.

Terveydenhuollon tietojärjestelmien kohdalla tietoturva on erittäin merkittävä tekijä, koska käsiteltävät tiedot ovat usein arkaluonteisia ja henkilökohtaisia, joten niiden käsittely ja turvallisuus on laissa määriteltyä. Nordbergin [2004] mielestä viisi suurinta haastetta terveydenhuollon tietoturvalle integroidussa ympäristössä ovat:

- kommunikaatio yli organisaatiorajojen ja tietoturva-alueiden välillä on välttämätöntä
- käyttäjien roolit ja vastuut ovat erilaisia
- potilaan yksityisyys on erittäin tärkeää
- hoitohenkilökunnalla tulee olla kaikki tarvittava tieto oikeaan aikaan oikeassa paikassa
- tiedon suojaaminen ja turvallisuus on kyettävä takaamaan.

Nordberg [2004] jakaa terveydenhuollon tietoturvan pääasialliset haasteet kahteen osaan: ohjelmisto- ja tietoliikenneturvallisuuteen. Ohjelmistoturvallisuuden tavoitteena on parantaa järjestelmien käyttäjien tunnistamista, roolien määrittelyä ja pääsynhallintaa. Tietoliikenneturvallisuudella pyritään turvaamaan järjestelmien ja käyttäjien välisten sanomien ja yhteyksien turvallisuus.

Bakker [2003] esittää, että terveydenhuollon tietojärjestelmien kohdalla erityisesti tiedon käytettävyys ja eheys ovat keskeisiä tietoturvakysymyksiä. Tietojärjestelmien käytettävyys terveydenhuollossa on erittäin tärkeää, koska potilaiden hoito on jatkuvaa työtä ilman taukoja. Tämän takia järjestelmien pitää toimia käytännössä aina. Terveydenhuollon organisaatioiden tuleekin varautua erilaisiin poikkeustilanteisiin. Tiedon eheys on potilaiden hoidon ja turvallisuuden kannalta erittäin tärkeää. Mikäli järjestelmissä olevat tiedot ovat korruptoituneet tai niihin on tallennettu väärää tietoa esimerkiksi näppäilyvirheen takia, voivat seuraukset olla kohtalokkaita. Lisäksi luotettavuus on nostettava erittäin tärkeään rooliin terveydenhuollossa, koska käsiteltävät tiedot ovat hyvinkin henkilökohtaisia ja tallennetut tiedot on suojattava valtuudettomalta käytöltä. Terveydenhuolto alueena on erittäin heterogeeninen ja monimutkainen, joten se aiheuttaa tietoturvan hoitamiselle suuria haasteita. [Cavalli et al., 2004, Grimson et al., 2000]

2.2.4. Hallinnollinen tietoturva terveydenhuollossa

Terveydenhuollon tietojärjestelmissä tiedon saatavuus ja eheys ovat erittäin merkittävässä roolissa. Myös arkaluontoisten tietojen käsittely on määritelty tarkoin useissa eri laissa. Tietoturva terveydenhuollossa ei ole pelkästään teknisten ratkaisujen kehitystä, vaan sitä tulee tukea myös johtamisen prosesseilla. Organisaatioiden pitää löytää tasapaino tietotekniikan uusien hyödyntämismahdollisuuksien, tietoturvan ja tiedon liikkumisen välillä. [Cavalli et al., 2004]

Hallinnollisella tietoturvalla tarkoitetaan tietoturvan johtamista, joka toimii pohjana koko tietoturvatoiminnalle [Reponen ja Ensio, 2005]. Tammisalo [2007] määrittää hallinnollisen tietoturvan hallinnollisina keinoina, kuten organisaatiojärjestelyt, tehtävien ja vastuiden määrittely sekä henkilökunnan ohjeistus, koulutus ja valvonta, joiden päämääränä on tietoturvallisuus. Suurin osa tietojärjestelmien väärinkäytöistä aiheutuukin joko työntekijöiden tai entisten työntekijöiden toimesta, tästä johtuen hallinnolliseen tietoturvaan tulee

suunnata erityishuomio. Tämä aiheuttaa organisaatioiden johdolle suuren vastuun, koska heidän tulee huolehtia koko organisaation kattavasta tietoturvan suunnittelemisesta ja sen vaikutuksista työntekijöihin. [Huston, 2001]

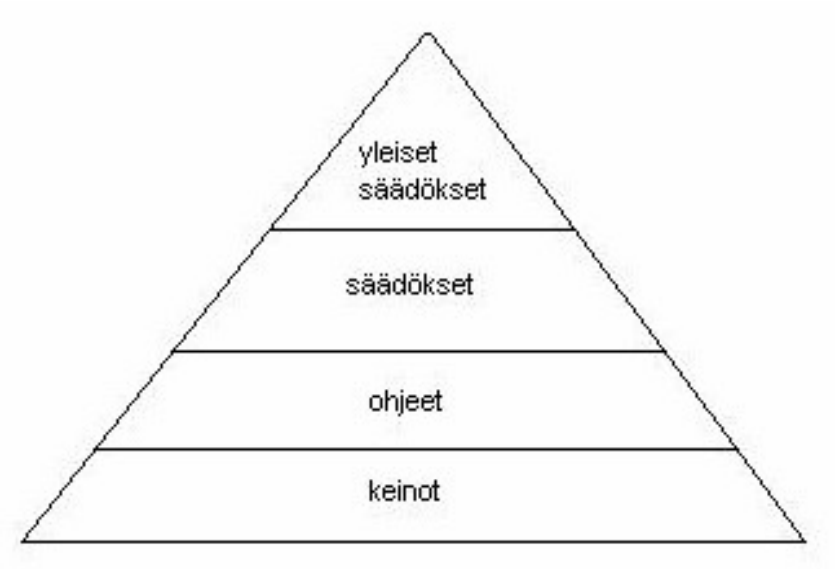
Terveydenhuollossa hallinnolliseen tietoturvaan vaikuttaa suuresti organisaatioiden rakenteet, jotka eroavat hyvin paljon muista aloista, koska hoitohenkilökunta on suuressa roolissa päätöksenteossa. Terveydenhuollossa myös eri sidosryhmillä on erilaisia näkemyksiä järjestelmien toiminnalle. Näitä sidosryhmiä ovat mm. hoitohenkilökunta, hallinnolliset henkilöt, valtiovalta. Terveydenhuoltoa ohjaa myös erilaiset sosiaaliset ja eettiset arvot. Lisäksi järjestelmissä käsiteltävän tiedon pitää olla saatavilla ja eheätä, mutta toisaalta potilaiden yksityisyys tulee turvata. Tässä kontekstissa terveydenhuollon tietojärjestelmien tietoturvan hallinnointi on erittäin haastava tehtävä. Eräs keino hallinnollisen tietoturvan toteuttamiseksi on asianmukaisen tietoturvapolitiikan kehittäminen. Tietoturvapolitiikan tehtävä on ohjata tietojärjestelmien käyttäjien ja ylläpitäjien toimia tietoturvallisemman järjestelmän saavuttamiseksi. [Gritzalis and Kokolakis, 2003]

Tietoturvapolitiikka määritellään korkean tason ohjeiksi, joiden tavoitteena on ohjata päätöksentekijöitä tietoturva-asioissa nyt ja tulevaisuudessa. Se on johdon kannanotto tietoturvallisuuden toteuttamiseksi. Tietoturvapolitiikka toimii perustana jokaiselle tietoturvaan liittyvälle toimelle [Katsikas and Kokolakis, 2004].

Tietoturvapolitiikassa määritellään vaatimukset ja edellytykset luotettavalle kommunikaatiolle ja arkaluontoisten tietojen luomiselle, varastoimiselle sekä käsittelylle. Se sisältää lailliset ja eettiset vaatimukset, organisatoriset ja toiminnalliset näkökulmat sekä myös erilaiset tekniset ratkaisut. Tietoturvapolitiikassa tulee huomioida organisaation tietojärjestelmien kaikki komponentit ja prosessit, ja se on saatettava kaikkien asianosaisten tietoon. [Nordberg, 2004; Tammisalo, 2005; Ruotsalainen, 2006]

Terveydenhuollon tietojärjestelmien tietoturvapolitiikka koostuu neljästä eri tasosta. Nämä tasot ovat yleiset säädökset, säädökset, ohjeet sekä keinot (kuva 4) [Gritzalis and Kokolakis, 2003; Katsikas and Kokolakis, 2004].

- *Yleiset säädökset* hallinnoivat ja ohjaavat terveydenhuollon tietojen turvallisuutta ja yksityisyyttä sekä niitä käyttäviä prosesseja. Yleiset säädökset ovat riippuvaisia yhteiskunnasta ja kulttuurista, kuten esimerkiksi erilaiset lait ja eettiset ohjeet.
- *Säädökset* johdetaan yleisistä säädöksistä, kun käsitellään jotain tiettyä hallinnoitavaa ympäristöä. Säädökset ovat siis riippuvaisia hallinnoitavasta alueesta.
- *Ohjeet* ovat spesifejä toiminnallisia askeleita, joita henkilöstön tulee noudattaa. Ohjeet johdetaan säädöksistä, kun käsitellään jotain tiettyä teknistä ympäristöä, ne ovat siis riippuvaisia käytetyistä teknisistä ratkaisuista.
- *Keinot* rakentuvat kun ohjeita käsitellään tietyssä asennusympäristössä. Ne ovat siis riippuvaisia asennusympäristöistä.



Kuva 4. Terveydenhuollon tietojärjestelmien tietoturvapolitiikan rakenne [Gritzalis and Kokolakis, 2003].

Tietoturvapolitiikka määrittää, miten tulisi toimia, jotta tietoturva hoidetaan mahdollisimman tehokkaasti. Sen tulee kertoa käyttäjien vastuut ja velvollisuudet, säännöt miten tietoa tulee käsitellä, jaella, varastoida sekä vaatimukset tiedon laadulle ja pääsyoikeuksille. Lisäksi johdon rooli tietoturvakysymyksissä on oltava selvillä, sekä minkälainen organisaation infrastruktuurin tulee olla tietoturvapolitiikan mahdollisimman tehokkaan hyväksikäytön saavuttamiseksi [Katsikas and Kokolakis, 2004; Tammisalo, 2005].

Tietoturvapolitiikkaa luotaessa pitää määritellä tehtävän politiikan sisältö, analysoida sosiaalinen, organisatorinen ja tekninen konteksti sekä valita käytettävä metodologia, jonka avulla saadaan luotua toimiva ja tehokas politiikka [Gritzalis and Kokolakis, 2003]. Valmiilla tietoturvapolitiikalla pitää olla määriteltynä omistaja ja vastuullinen taho, jonka tehtäviin kuuluu ylläpito, säännölliset katselmoinnit sekä tarpeen tullen muutoksien tekeminen. Muutoksien tapahtuessa ne täytyy dokumentoida huolellisesti ja ne on saatettava kaikkien asianomaisten tietoon [Tammisalo, 2005].

Cavalli et al. [2004] esittävät, että terveydenhuollon tietojärjestelmien turvallisuus ei ole pelkästään teknisten ratkaisujen varassa vaan sitä tulee tukea hallinnollisen tietoturvan keinoin. Heidän näkemyksensä mukaan tietoturvaa suunniteltaessa organisaatioiden tulisi ensin määritellä kaikki esiintyvät tietovarannot yksittäisistä tietokoneista isoihin tietovarastoihin saakka sekä luoda monialainen ryhmä vastaamaan prosessista. Tietovarannot tulisi tämän jälkeen arvioida luotettavuuden, eheyden ja saatavuuden suhteen, sekä määrittää näiden perusteella tiedoille tietoturvavaatimusluokat. Seuraavaksi organisaation tulisi tunnistaa kaikki tietovarantoja uhkaavat tekijät sekä määritellä näiden todennäköisyydet ja minkälaisia vaikutuksia toteutuvilla uhkilla on tiedoille ja toiminnalle. Viimeisenä toimena tulisi tehdä riskiarviointi, jossa riskejä arvioidaan suhteessa nykyisiin tietoturvakontrolleihin. Tammisalo [2007] esittää omassa näkemyksessään vielä viimeiseksi vaiheeksi sopivien kontrollien valinnan, joiden avulla varaudutaan riskeihin ja ongelmatilanteisiin. Näiden määrittelyjen ja valintojen perusteella

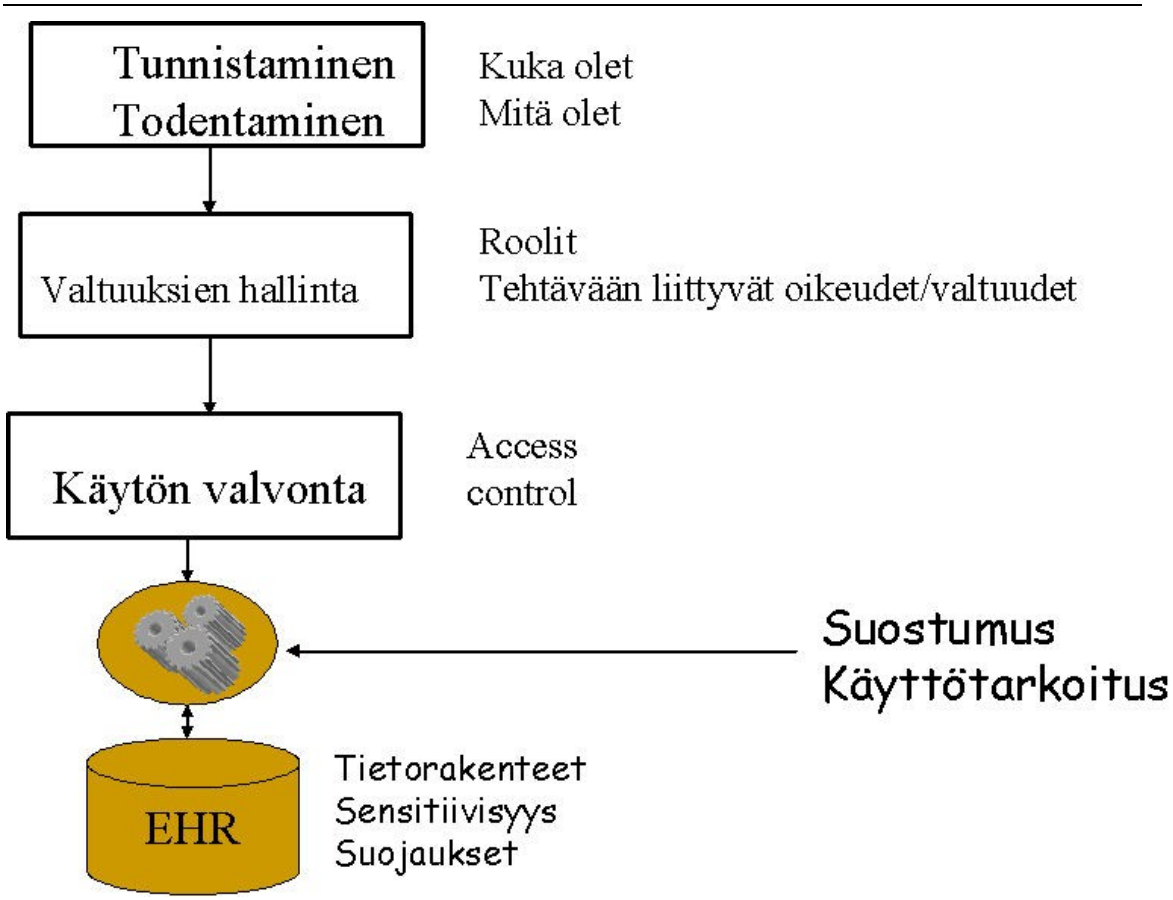
organisaatio voi lähteä suunnittelemaan ja kehittämään tietoturvatoimintaansa, sekä toteuttamaan mahdollisiin uhkatekijöihin valmistautumista.

2.2.5. Ohjelmistoturvallisuus

Ohjelmistoturvallisuuden tavoitteena on turvata tietojenkäsittelypalveluiden eheys, luottamuksellisuus sekä sovelluksissa käsiteltävien tietojen saatavuus. Ohjelmistoturvallisuuden yleisesti käytettyjä keinoja ovat pääsynhallinta, käyttäjänhallinta sekä käyttäjien todentaminen. Näiden keinojen avulla voidaan määritellä luotettavasti, kuka saa ja pääsee käyttämään tietoja sekä sovelluksia. yllä mainittujen keinojen avulla pystytään siis estämään tietojen luvaton käyttö, joten tarkoituksena on turvata tietojen luottamuksellisuus. [Blobel, 2002]. Näiden lisäksi organisaation tulisi aktiivisesti seurata tietojärjestelmiensä käyttöä, jotta voidaan reagoida mahdollisiin väärinkäytöksiin.

Lähtökohtana ohjelmistoturvallisuuden suunnittelussa on organisaation tietoturvapolitiikka, jossa määritellään miten pääsynhallinta, käyttäjänhallinta ja käyttäjien todentaminen tulisi hoitaa [Sullivan, 2004]. Hoitamalla ohjelmistoturvallisuus tehokkaasti, organisaatio voi estää niiden riskien syntyminen, jotka aiheutuvat valtuudettomasta tietoihin pääsystä. Nämä riskit eivät ainoastaan uhkaa tietojen luottamuksellisuutta, vaan myös vaarantavat tietojen olemassaolon sekä oikeellisuuden [Tammisalo, 2005].

Kuvassa 5 on kuvattuna terveydenhuollon käyttäjänhallinnan ja käyttöoikeuksien periaatemalli [Ruotsalainen, 2006b]. Kuvassa on yksinkertaistettu esitys pääsynhallinnan prosessista.



¨Kuva 5. Käyttäjän hallinta, käyttöoikeudet ja käytön valvonta [Ruotsalainen, 2006b, s 54].

Pääsynhallinnalla kontrolloidaan käyttäjien oikeuksia tiedonkäsittelyyn ja ohjelmistojen käyttöön sekä mahdollistetaan ylläpitäjille keinot seurata ja valvoa tietojärjestelmien käyttöä [Sullivan, 2004]. Terveydenhuollon organisaatioissa on useita eri sovelluksia ja käyttäjiä. Tämän vuoksi organisaation tulee määritellä tarkat politiikat, säännöt ja käytännöt millaisia pääsyoikeuksia tietoihin luodaan sekä millaisia oikeuksia (esimerkiksi luku-, kirjoitus-, muutos-, poisto-, suoritus- ja hallintaoikeus) voidaan valtuuttaa eri käyttäjille ja käyttäjäryhmille. Lisäksi organisaation on määriteltävä, millä menetelmillä käyttäjät tunnistetaan, millaisia yhteyksiä tietojärjestelmiin sallitaan ja miten tietojärjestelmien käyttöä seurataan. Käytettävien pääsynhallintamenetelmien on oltava riittävän vahvoja ja turvallisia, jotta voidaan varmistaa tietojärjestelmien turvatasojen täyttyminen. [Tammisalo, 2005]

Organisaatioiden on suunniteltava, kenellä on valtuudet myöntää käyttäjille oikeuksia tietojärjestelmiin ja miten oikeuksia hallinnoidaan. Käyttöoikeuksien myöntäminen on oltava ennalta tarkkaan määritelty prosessi, jossa on päätetty menetelmät, miten käyttäjälle myönnetään hänelle kuuluvat oikeudet. Verkkopalveluiden ja kriittisten järjestelmien käytöstä on oltava oma politiikka, jossa määritellään käyttäjille ja käyttäjäryhmille pääsy ainoastaan niihin resursseihin joihin on tarve. Organisaatioiden on huolehdittava, että myönnettyjä käyttövaltuuksia arvioidaan ja päivitetään säännöllisesti ennalta määritellyn prosessin mukaan. Tarvittaessa organisaation jokaiselle tietojärjestelmälle on määriteltävä oma pääsynhallintapolitiikka riippuen järjestelmän tietoturvatasosta. [Tammisalo, 2005]

Käyttäjänhallinta sisältää määritykset kuinka ja millä menetelmillä käyttäjät rekisteröidään sekä mitä valtuuksia heille kuuluu. Kaikki organisaation tietojärjestelmien käyttäjät tulee rekisteröidä henkilökohtaisesti, samalla kertoen heille tietojen käsittelyyn ja suojaamiseen liittyvät säännöt ja vastuut. Organisaation tulee suunnitella, kuinka käyttäjät saavat heille nimenomaisesti kuuluvat oikeudet ja tämä prosessi tulee dokumentoida huolellisesti. Oikeuksia käyttäjille myönnetään sen perusteella, mitä työtehtäviä käyttäjälle kuuluu sekä mitä tietoja hänen tulee käsitellä. Oikeudet on määriteltävä riittävän tarkasti ja turvallisesti, jotta voidaan varmistaa tietojärjestelmien turvatasojen noudattaminen. [Tammisalo, 2005]

Jokaisella tietojärjestelmän käyttäjällä tulee olla oma henkilökohtainen tunnus ja salasana. Kaikki tunnukset on rekisteröitävä, ja tähän rekisteriin tulee myös tallentaa tunnukseen liittyvät valtuudet. Tunnuksia käytetään hyväksi myös tietojärjestelmän käytön seurannassa. Mikäli tunnukselle on myönnetty poikkeuksellisen paljon valtuuksia, niin sen käyttöä on seurattava erittäin tarkkaan, jotta mahdollisiin väärinkäytöksiin voidaan reagoida riittävällä nopeudella. Ylläpitäjien on myös aktiivisesti seurattava tunnusten käyttöä ja poistaa tai asettaa käyttökieltoon ne, joita ei ole pitkään aikaan käytetty. [Tammisalo, 2005; Ferrara, 2000]

Terveydenhuollossa lait asettavat vaatimuksia käyttäjien rooleille ja velvollisuuksille. Näiden vaatimuksien takia, Blobel [2002] esittääkin, että organisaatioiden on syytä jakaa käyttäjille kaksi eri roolia, rakenteellinen ja toiminnallinen. Rakenteellinen rooli määrittää käyttäjän aseman suhteessa organisaation hierarkiaan. Se heijastuu käyttäjän ammatillisesta osaamisesta sekä vastuusta organisaation toiminnassa. Rakenteelliset roolit ovat hyvin staattisia ja ne muuttuvat suhteellisen harvoin. Rakenteellisia rooleja terveydenhuollossa ovat esimerkiksi:

- johtava lääkäri
- johtava ylihoitaja
- sairaanhoitaja
- osastonlääkäri
- lääkäri.

Toiminnalliset roolit perustuvat käyttäjän asemaan hoitoprosessissa, eli ne kertovat käyttäjän ja potilaan suhteesta. Toiminnalliset roolit kuvaavat erittäin dynaamista suhdetta. Hoitosuhteessa olevan potilaan tietoihin tulisikin päästä käsiksi toiminnallisen roolin mukaan. Esimerkkejä toiminnallisista rooleista terveydenhuollossa ovat mm:

- hoitava lääkäri
- diagnostiikkaryhmän jäsen
- konsultoiva lääkäri
- hoitoon ohjannut lääkäri
- oma lääkäri.

Molemmat roolit määrittelevät käyttäjän oikeuksia ja vastuita terveydenhuollon organisaatioissa. Koska käyttäjät toimivat molempien roolien mukaan, niin käyttäjänhallinta tulisikin rakentua molempien näkemysten perusteella [Blobel, 2002]. Terveydenhuollossa on tilanteita, milloin käyttäjä tarvitsee suuremmat käyttöoikeudet, kuin mitä hänelle roolinsa perusteella kuuluisi. Tämän takia käyttäjillä, jotka ovat tekemisissä hätätilanteiden kanssa,

tulisi olla mahdollisuus ylittää omat käyttöoikeutensa potilaan kohdalla, mikäli tilanne sitä vaatii. Käyttäjän ylittäessä käyttöoikeutensa tilanne tulisi jälkikäteen analysoida, jotta voidaan todeta oliko ylitykseen oikeutus [Bakker, 2003].

Käyttäjien todentamisen luotettavuus riippuu tunnistamisessa käytetystä todentamismenetelmästä. Käyttäjän tunnistaminen perustuu johonkin seuraavista vaihtoehdoista:

A) johonkin mitä käyttäjä tietää
B) jotakin mitä käyttäjällä on hallussaan
C) johonkin mitä käyttäjä on.

A-vaihtoehto tarkoittaa yleisesti salasanaa, jonka avulla käyttäjä tunnistautuu. B-vaihtoehdossa käyttäjällä on hallussaan esine, jonka avulla hän tunnistautuu. C-vaihtoehto tarkoittaa, että käyttäjä tunnistautuu omalla ominaisuudellaan, esim. sormenjälki tai silmän iiris. Mikäli käytetään ainoastaan yhtä näistä, niin tunnistaminen on kevyt. Vahvalla tunnistamisella tarkoitetaan kahteen tai useampaan todentamismenetelmään perustuvaa tunnistamista. [VAHTI, 2006]

Käyttäjien todentamisessa organisaation tulee määritellä menetelmät, miten käyttäjät todennetaan, jotta voidaan varmistaa tietojärjestelmien turvatasojen täyttyminen. Tietojärjestelmiin on aina kirjauduttava riittävän turvallisella menetelmällä. Tarvittaessa kaikille organisaation tietojärjestelmille on erikseen määriteltävä todentamismenetelmät, riippuen tietojärjestelmän turvatasosta. Joihinkin järjestelmiin voi riittää käyttäjän tunnuksella ja salasanalla kirjautuminen, mutta mikäli järjestelmä koetaan kriittiseksi ja se on turvatasoltaan korkea, niin käyttäjiltä voidaan vaatia vahvempaa tunnistautumista. Vahvoja todentamismenetelmiä ovat esimerkiksi vaihtuvat salasanalistat, USB-avaimet ja toimikortit varmenteineen, kertakäyttöiset tunnisteet ja toimikortit. Käytettäessä USB-avaimia tai toimikortteja niiden käyttö on oikeutettava PIN-koodilla tai biometrisellä tunnisteella. [Tammisalo, 2005]

Organisaation on huolehdittava, että käyttäjätunnuksia ja salasanoja pystytään valvomaan. Salasanojen tulee täyttää tietyt tietoturvavaatimukset, salasanan tulee esimerkiksi koostua numeroista ja kirjaimista, salasanalle määritellään vähimmäispituus ja lisäksi käyttäjän on pakko vaihtaa salasana automaattisesti tietyn ajan kuluttua. Lisäksi käyttäjille tulee järjestää koulutusta tunnuksien tietoturvallisesta käytöstä, jotta he saadaan ymmärtämään, että tunnukset ovat henkilökohtaisia ja salaisia, ja ettei niitä saa lainata työkavereille. Järjestelmissä on oltava käytössä myös automaattiset poiskirjautumiset, esimerkiksi käyttäjän verkkoyhteyden katketessa on järjestelmän uloskirjattava käyttäjä [Bakker, 2003; Tammisalo, 2005].

Käytettäessä tunnus-salasana menetelmää käyttäjän todentamiseen, kirjautumissovellus on suunniteltava siten, ettei käyttäjän tunnisteita liikutella missään vaiheessa selkokielisenä. Kaikki tunnusten käsittely on tapahduttava salattuna. Käyttäjien tunnuksia ja salasanoja ei saa tallentaa missään vaiheessa välimuistiin tai tiedostoon. Väärinkäytösten estämiseksi kirjautumisvaiheessa ei käyttäjälle tule kertoa, mikä kirjautumisessa meni väärin. Lisäksi kirjautumisyrityksien määrä on oltava rajattu ja mikäli tietystä verkko-osoitteesta tulee riittävä määrä kirjautumisyrityksiä, niin yhteydet kyseistä osoitteesta on pystyttävä estämään määräajaksi. [Tammisalo, 2005]

2.2.6. Tietoliikenneturvallisuus

Tietoliikenneturvallisuudella tarkoitetaan toimia, joiden tavoitteena on turvata organisaation tietoliikenne ja varmistaa välitettävien tietojen luottamuksellisuus, eheys ja käytettävyys. Tietoliikenneturvallisuuden keinoina voidaan käyttää tietojen luottamuksellisuuden turvaamiseksi erilaisia tietojen salausmenetelmiä. Tietojen eheys voidaan saavuttaa käyttämällä tiedonsiirrossa erilaisia tarkistussummia, tarkistuskoodeja ja digitaalista allekirjoitusta [Tammisalo, 2007]. Paavilainen [1998] listaa neljä päämäärää tietoliikenneturvallisuudelle. Tarkoituksena on varmistaa:

- sanomien alkuperäisyys, koskemattomuus ja luottamuksellisuus

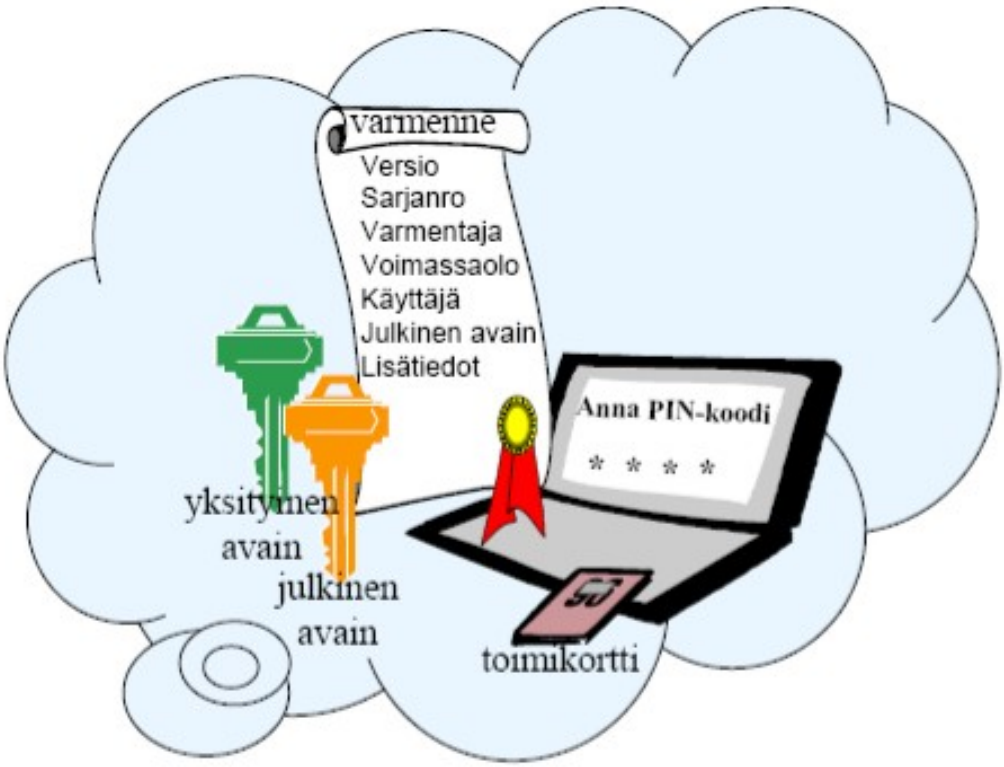
- lähettäjä ja vastaanottaja sekä todentaa heidät
- tietoliikennelaitteiden fyysinen turvallisuus
- väärinreitityksen estäminen.

Tietoliikenneturvallisuuteen kuuluvat kaikki asiat, jotka liittyvät tietoliikenteeseen, verkkojen rakentamiseen ja suunniteluun. Siihen vaikuttavat käytettävät protokollat, salausmenetelmät, verkkotopologiat sekä tietoturvatuotteet, kuten reitittimet ja palomuurit [Paavilainen, 1998]. Tietoliikenneturvallisuudessa tulee varmistaa, että tietoverkkojen hallinnan ja hoidon vastuut ovat selvillä, ja että turvahenkilöstöllä on riittävä asiantuntemus tehtävien hoitamiseksi. Organisaation tulee varmistaa, että hallintatehtävien hoitoon on varattu riittävästi resursseja ja tarvittavia apuvälineitä ja työkaluja [Tammisalo, 2005]. Tietoliikenneturvallisuuden keinoja ovat mm. laitteistojen ja siirtoyhteyksien suojaus, ylläpito ja hallinta, verkon- ja pääsynhallinta, tietoliikenteen käytön valvonta ja tarkkailu, ongelmatilanteiden kirjaaminen ja selvittäminen, sanomaliikenteen salaus sekä tietoliikenneohjelmien testaus [VAHTI, 2004b].

Tietoliikenneturvallisuuden merkitys terveydenhuollossa on kasvanut erilaisten aluetietojärjestelmien yleistymisen myötä. Aluetietojärjestelmissä vaaditaan tiedon välitystä eri organisaatioiden välillä [Georgoulas et al., 2003]. Aluetietojärjestelmissä tiedon siirtoon käytetään usein avointa tietoverkkoa, eli Internetiä. Internetin käyttö asettaa suuria paineita tietoturvallisuudelle, koska välitettävä tieto on useimmiten salassa pidettävää ja arkaluonteista [Porali, 2005]. Georgoulas et al. [2003] nostavat esiin kuusi erityistä turvallisuusuhkaa liittyen tietoliikenneturvallisuuteen terveydenhuollossa:

- luvaton pääsy verkkoresursseihin ja palveluihin
- luottamuksellisen ja salassa pidettävien terveydenhuollon asiakirjojen paljastuminen
- luvaton pääsy tietoliikenteeseen
- terveydenhuollon asiakirjojen luvaton muokkaaminen
- tietoihin liittyvien päivämäärien kiistäminen
- tietojen alkuperän salaaminen.

Riittävän tietoliikenteen salaamisen lisäksi, yksi parhaista keinoista turvata tiedon luottamuksellisuus ja eheys tiedonvälityksessä on PKI-järjestelmä. PKI-järjestelmällä tarkoitetaan julkisen avaimen menetelmää, joka yhdistää julkisen avaimen salauksen, varmenteet ja varmenneorganisaatiot yhdeksi kokonaiseksi arkkitehtuuriksi [Ruotsalainen, 2004]. Kuvassa 6. on esitetty PKI-järjestelmän vaatimat työkalut.



Kuva 6. PKI-arkkitehtuurin vaatimat työkalut [Hakala, 2002, s 10].

Julkisen avaimen salauksessa tarkoitetaan yksityiseen ja salaiseen avaimeen perustuvaa tietojen salausta. Avaimet muodostavat yhdessä avainparin, joiden avulla tietoa voidaan salata ja avata. Ne on liitetty toisiinsa matemaattisella kaavalla. Julkisella avaimella salattu tieto voidaan avata ainoastaan yksityisellä avaimella. Avaimia tulisi säilyttää ulkopuolisilta turvassa, ja yleinen säilytyspaikka onkin toimikortti [Hakala et al., 2002; Porali, 2005].

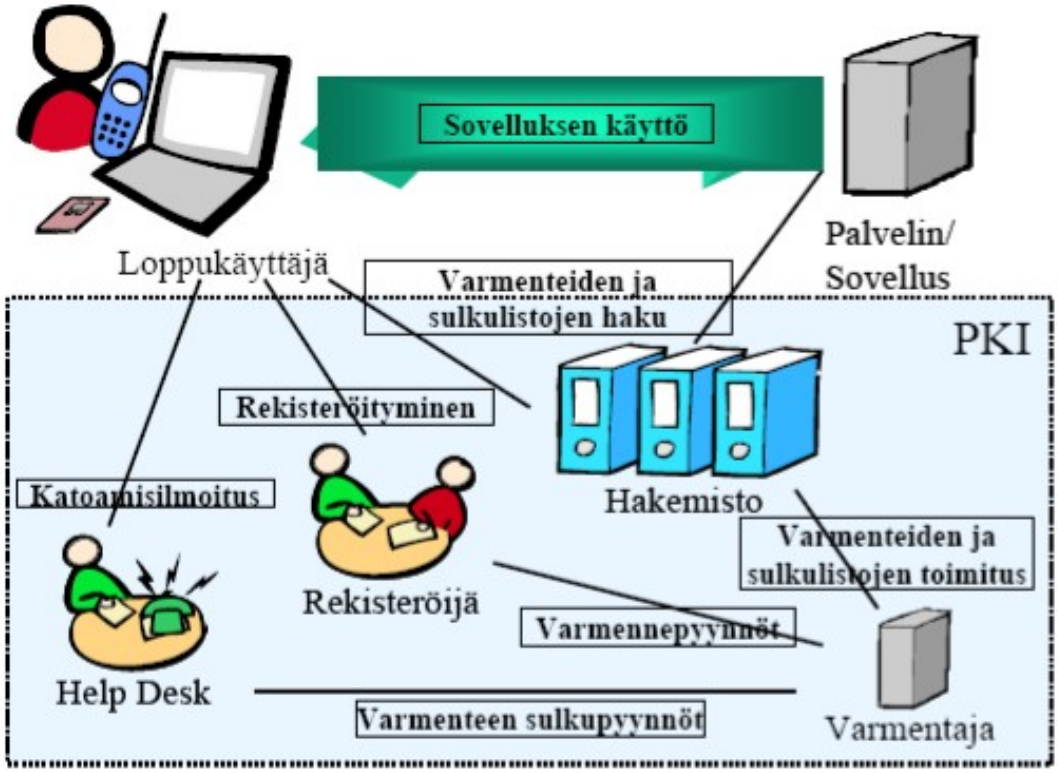
Varmenteella tarkoitetaan elektronista dokumenttia, jonka varmentajaorganisaatio myöntää, ja jonka avulla voidaan todistaa varmenteen sisällön kuuluminen asianomaiselle käyttäjälle. Käyttäjä voi olla tässä tapauksessa sekä henkilö että tietojärjestelmä. Organisaatioiden tulisi myös hankkia palvelinvarmenteet, jotta käyttäjät voivat varmistua palvelimen kuulumisesta ko. organisaatiolle. Lisäksi selaimen ja palvelimen välinen tietoliikenne voidaan salata. Julkinen avain varastoidaan varmenteeseen ja varmenteet tallennetaan erityiseen hakemistoon. Hakemistosta voivat eri sovellukset hakea tarvittavia varmenteita. [Ruotsalainen, 2004; Tammisalo, 2005]

Varmentajaorganisaation tehtävänä on luoda, jakaa ja varmentaa käyttäjille myönnettäviä varmenteita. Se on ns. luotettu organisaatio, johon eri osapuolet voivat luottaa varmennetietoihin liittyen. Varmentaja myös huolehtii avainparien ja varmenteiden turvallisesta toimittamisesta organisaatioille [Ruotsalainen, 2004, Porali, 2005]. Varmentajan luotettavuus perustuu sen käyttämään varmennepolitiikkaan. Käyttäjäorganisaation tulisikin ennen varmenteen hyväksymistä arvioida varmentajan varmennepolitiikka [Tammisalo, 2005].

Julkisen avaimen menetelmällä voidaan järjestää organisaation sisäinen ja ulkoinen tiedonvälitys tietoturvallisesti. PKI:n avulla voidaan saavuttaa tiedon luottamuksellisuus ja eheys, kun kukaan muu kuin vastaanottaja ei saa viestejä auki sekä voidaan osoittaa, ettei viestiä ole muutettu siirron aikana. PKI toteuttaa myös vahvan tunnistamisen, jolloin voidaan todentaa tiedon siirron osapuolet, kuten esimerkiksi henkilöt ja järjestelmät. Koska siirrettävät viestit ovat digitaalisesti allekirjoitettuja, niin tiedon kiistämättömyys toteutuu myös tiedon siirrossa. [Hakala et al., 2002; Ruotsalainen, 2004]

PKI koostuu teknologiasta, toimintapolitiikasta ja hallinnollisista menetelmistä. Ja siinä on käyttäjien asenteilla suuri merkitys. PKI muodostaa alustan, jonka päälle organisaatiot voivat toteuttaa omia järjestelmiään. Se tulee olla osa organisaation perusinfrastruktuuria, jolloin voidaan turvata arkaluontoisten

tietojen vaihto turvattomassa ympäristössä. Kuvassa 7. on kuvattu PKI-arkkitehtuuri ja sen toiminnallisuus. [Hakala et al., 2002; Ruotsalainen, 2004]



Kuva 7. PKI-arkkitehtuuri [Hakala et al., 2002, s 9].

Potilaslaissa [PotL, 1992] säädetään, että useissa potilasasiakirjoissa pitää olla asiakirjan laatijan omakätinen tai sähköinen (varmennettu) allekirjoitus. PKI-arkkitehtuurin avulla voidaan toteuttaa varmennettu sähköinen allekirjoitus. Sähköisen allekirjoituksen avulla voidaan turvata tiedon eheys ja kiistämättömyys. Sähköisellä allekirjoituksella sidotaan asiakirjaan allekirjoittajan henkilöllisyys ja voidaan estää tietojen myöhempi väärentäminen tai muuttuminen vahingossa. Allekirjoitus tehdään esimerkiksi toimikortin avulla, johon on tallennettu käyttäjän salainen avain. [Tammisalo, 2005]

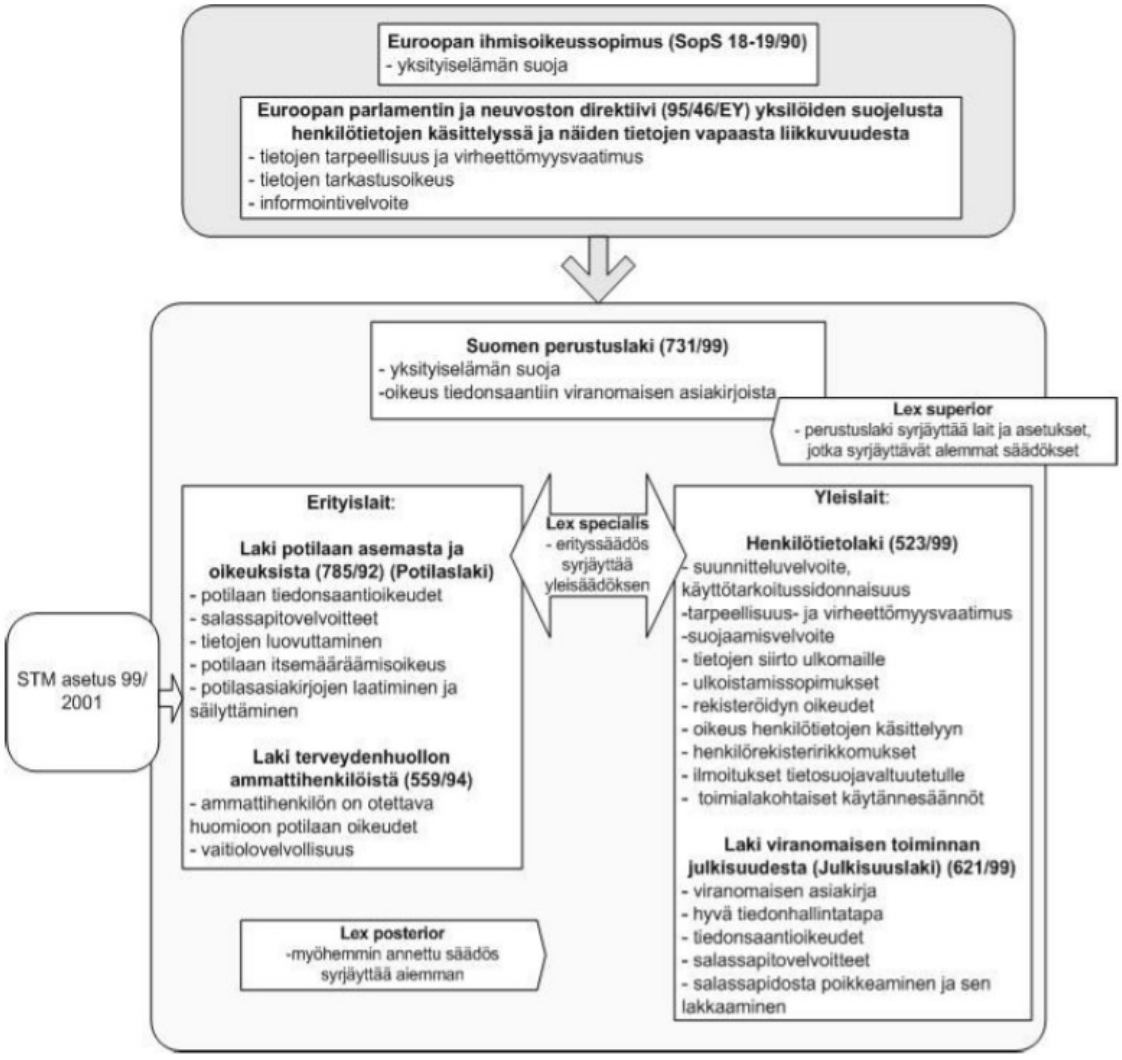
2.3. Lait ja asetukset

Tietosuojaa käsitteleviä lakeja on Suomessa useita. Eräänlaisena tietosuojan yleislakina voidaan pitää henkilötietolakia (1999/523). Tietosuojan ja terveydenhuollon osalta oleellisia lakeja ja asetuksia ovat ainakin seuraavat:

- Perustuslaki (731/1999)
- Euroopan ihmisoikeussopimus (SopS 18-19/90)
- Euroopan parlamentin ja neuvoston direktiivi (96/46/EY) yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta
- Laki viranomaistoiminnan julkisuudesta (621/1999)
- Laki sähköisestä asioinnista viranomaistoiminnassa (13/2003)
- Laki sähköisistä allekirjoituksista (14/2003)
- Sähköisen viestinnän tietosuojalaki (516/2004)
- Arkistolaki (831/1994)
- Erikoissairaanhoitolaki (1062/1989, muutos 652/2000)
- Laki yksityisestä terveydenhuollosta (152/1990)
- Laki potilaan asemasta ja oikeuksista (785/1992, muutos 653/2000)
- Laki terveydenhuollon ammattihenkilöistä (559/1994)
- Laki sosiaali- ja terveydenhuollon saumattoman palveluketjun kokeilusta (811/2000)
- Sosiaali- ja terveysministeriön asetus potilasasiakirjojen laatimisesta sekä niiden ja muun hoitoon liittyvän materiaalin säilyttämisestä (PotA99/2001)
- Laki sosiaali- ja terveydenhuollon saumattoman palveluketjun kokeilusta annetun lain muuttamisesta (1225/2003)
- Työterveyshuoltolaki (1383/2001)
- Hallintolaki (434/2003)

Tietosuojasta Suomen lainsäädännössä on säädetty useissa eri laeissa, mutta merkittävimmässä asemassa on henkilötietolaki (523/1999). Kuvaan 8 on koottu keskeisimpiä terveydenhuollon henkilötietojen käsittelyyn liittyviä

oikeusnormeja sekä näiden suhteita. Henkilötietolaki on yleislaki, jossa säädetään henkilötietojen käsittelystä. Sen tarkoitus on turvata yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia. Näiden perusoikeuksien suojattavuus pohjautuu jo Suomen perustuslakiin (731/1999). Henkilötietolaki sisältää yleiset määräykset ja säännöt henkilötietojen käsittelystä, keräämisestä, tallentamisesta, luovuttamisesta ja siirrosta. Henkilötietolaki väistyy silloin, kun henkilötietojen käsittelystä poikkeavalla tavalla on säädetty jossain toisessa laissa. [HetiL, 1999; Pahlman, 2005; Ylipartanen, 2004].



Kuva 8. Terveydenhuollon henkilötietojen käsittelyyn liittyviä oikeusnormeja [Reponen, 2006, s 14]

Toinen merkittävä yleislaki liittyen julkisen terveydenhuollon tietosuojaan on laki viranomaistoiminnan julkisuudesta (621/1999), eli julkisuuslaki. Julkisuuslain tavoitteena on turvata viranomaistoiminnan julkisuus. Siinä säädetään, että kaikki viranomaisen asiakirjat ovat julkisia, ellei julkisuuslaissa tai muussa lainsäädännössä ole toisin säädetty. Julkisuuslain 24§:n mukaan viranomaisen asiakirjat ovat salassa pidettäviä, kun ne sisältävät tietoja sosiaalihuollon asiakkaasta tai henkilön terveydentilasta. Tästä johtuen sosiaali- ja terveydenhuollon asiakas- ja potilasrekistereiden tiedot ovat salassa pidettäviä. [JulkL, 1999]

Laki potilaan asemasta ja oikeuksista (785/1992), eli potilaslaki sisältää säännöksiä potilaan hoitoon ja kohteluun liittyen terveydenhuollossa. Siinä säädetään pääasiallisesti potilassuhteen luottamuksellisuudesta ja potilaan hoidollisesta itsemääräämisoikeudesta. Myös potilaslaissa määritellään potilasasiakirjojen salassa pidettävyydestä. Potilaslaissa säädetään myös potilaan oikeudesta antaa tai olla antamatta suostumus tietojensa luovuttamiselle. Lisäksi potilaslaissa on säädetty terveydenhuollon toimintayksiköiden velvollisuudesta nimittää potilasasiamies, jonka tehtäviin kuuluu neuvoa ja auttaa potilasta potilaslakiin liittyvissä asioissa sekä edistää potilaiden oikeuksia. [PotL, 1992]

Laissa sosiaali- ja terveydenhuollon saumattoman palveluketjun kokeilusta (811/2000) säädetään alueellisten tietojärjestelmien toteutukseen liittyvistä säännöksistä. Laissa säädetään mm. tunnistamiseen, sähköiseen allekirjoitukseen ja viitetietokantaan liittyvistä asioista. Terveydenhuollon ammattilainen tulee lain mukaan todentaa riittävän tasoisella varmenteella, myös organisaatiot voidaan varmentaa sähköisessä asioinnissa. Lisäksi lähetettävät asiakirjat ja muut viestit voidaan sähköisesti allekirjoittaa tai salata. Lain tarkoituksena on edistää salassapitoa, yksityisyyden suojaa sekä asioinnin luotettavuutta. [Pahlman, 2005]

Henkilötietolain, julkisuuslain ja -asetuksen lisäksi tietoturvasta säädetään useassa muussakin laissa. Näissä laissa säädetään mm. tietojen arkistointiin liittyviä vaatimuksia ja periaatteita (arkistolaki 831/1994), sähköisistä allekirjoituksista (laki sähköisistä allekirjoituksista 14/2003), sähköisestä asioinnista (laki sähköisestä asioinnista viranomaistoiminnassa 13/2004) sekä sähköisen viestinnän tietosuojasta (sähköisen viestinnän tietosuojalaki 516/2004). Näiden lakien tarkoituksena on turvata viestinnän luottamuksellisuus ja yksityisyyden suoja sekä asioinnin luotettavuus, osapuolten tunnistaminen, tietojen virheettömyys ja suojaaminen.

2.4. Uusi laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä

Sosiaali- ja terveydenhuollossa pyritään parantamaan tieto- ja viestintäteknologialla palveluiden laatua, saatavuutta ja kustannustehokkuutta. Hallituksen tietoyhteiskuntaohjelmalla on ollut merkittävä rooli tässä kehitystyössä. Myös EU-tasolla on panostettu ns. eTerveyspalveluiden kehittämiseen. Suomessa perusjärjestelmien suhteen on edistytty hyvin, esimerkiksi sähköiset potilaskertomusjärjestelmät ovat jo laajalti käytössä. Lisäksi potilaiden tietojen jakamista toisten toimintayksiköiden kanssa on helpotettu kehittämällä erilaisia aluetietojärjestelmiä. Aluetietojärjestelmiä kehitettiin kansallisilla ja alueellisilla projekteilla, joiden myötä syntyi aluearkkitehtuurimalli, joka keskittyi pääasiallisesti tiedonvälitykseen, eikä siinä esimerkiksi huomioitu tietojen arkistointia tai tietoarkkitehtuuria [Iivari ja Ruotsalainen, 2006].

Alueellisten ratkaisujen kehittyessä nousi useiden työryhmien ja asiantuntijoiden keskusteluissa esiin tarve valtakunnalliselle yhteistoiminnallisuudelle. Asiantuntijoiden yhteistyön tuloksena määriteltiin toiminnan kannalta kriittisiä kehitysalueita. Teemoiksi nousivat valtakunnantasoinen yhteistoiminnallisuus, potilaskertomusten sähköinen arkistointi, tietosuoja- ja tietoturva sekä keskitetyt palvelut ja ohjaus. Lisäksi

mm. Kelalla ja vakuutusyhtiöillä on toimintoja, joita tukemaan pitäisi luoda valtakunnalliset palvelut. Kun palvelut rakennetaan keskistetysti, niin voidaan mahdollisesti saavuttaa kustannussäästöjä, helpottaa yhteistoiminnallisuuden toteuttamista, tukea kansalaisten omien tietojen tarkastelua sekä varautua yhä lisääntyvään potilaiden liikkuvuuteen. Yhteisillä ratkaisuilla mahdollistetaan valtakunnan tasoinen standardointi, tietojen pitkäaikaisarkistointi sekä tietojen jakelu tietoturvallisesti sekä varmistuen tietosuojan toteutumisesta. [Iivari ja Ruotsalainen, 2006]

Tällä hetkellä Suomen terveydenhuollon ja tietosuojaan liittyvä lainsäädäntö on hajaantunut useaan eri lakiin (mm. henkilötietolaki, julkisuuslaki, potilaslaki, yms.). Lait ovat myös osittain päällekkäisiä, mikä voi aiheuttaa sekaannuksia. Lisäksi lainsäädäntö kaipaa selkeämpiä pykäliä liittyen sähköiseen terveydenhuoltoon. Tästä syystä on haluttu tehdä uusi laki, joka pystyy vastaamaan kehittyvään terveydenhuoltoon ja muuttuvaan palveluntarjontaan.

2.4.1. Lain esittely

Heinäkuussa 2007 voimaan tulleen lain tarkoituksena on parantaa sosiaali- ja terveydenhuollon organisaatioiden mahdollisuuksia hyödyntää tietotekniikkaa palveluidensa tuottamisessa. Tietotekniikan avulla toimintayksiköiden on mahdollista saada tietoa oikea-aikaisesti edistäen potilasturvallisuutta ja samalla tehostaen palveluitaan. Lisäksi tarkoitus on parantaa asiakkaiden mahdollisuutta vaikuttaa omaan palveluunsa. [HE, 2007]

Laissa 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. Lain varsinainen sisältö voidaan jakaa neljään lukuun:

- asiakastietojen sähköisen käsittelyn yleiset vaatimukset
- potilastietojen sähköinen luovuttaminen
- terveydenhuollon valtakunnalliset tietojärjestelmäpalvelut
- asiakkaan tiedonsaantioikeudet.

Asiakastietojen sähköisen käsittelyn yleiset vaatimukset 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. Tosin vaatimuksia on määritelty aika vähän, ja monet kohdat odottavatkin sosiaali- ja terveysministeriön asetuksia. [HE, 2007]

Luvussa potilastietojen sähköinen luovuttaminen säädetään niistä edellytyksistä, jolloin potilastietoja voidaan luovuttaa sähköisesti toiselle terveydenhuollon toimijalle tai muulle luovutuksensaajalle. Siinä määritellään myös hakutietojen sisältö, jotka liitetään potilasasiakirjoihin, joiden perusteella muut organisaatiot voivat löytää tarvitsemansa asiakirjat. Potilastietojen luovutus tapahtuu ainoastaan potilaan suostumuksen tai laissa säädetyn perusteen nojalla. Potilaan kirjallinen suostumus voidaan antaa kertaluontoista palvelutapahtumaa tai palvelukokonaisuutta varten. Potilaalla on myös aina oikeus peruuttaa tai muokata suostumustaan. [HE, 2007]

Suostumuksen tulee olla allekirjoitettu omakätisesti tai kehittyneellä sähköisellä allekirjoituksella. Eräissä poikkeustilanteissa (potilaslaissa määritelty) suostumus voi olla myös suullinen, mutta silloinkin siitä pitää tehdä merkintä suostumusasiakirjaan. Potilaan suostumuksen yhteydessä hänelle tulee luovuttaa jäljennös tai sähköinen tiedonsaanti suostumuksesta. Suostumuksista muodostuu osa toimintayksikön sähköistä potilasrekisteriä, joten he ovat vastuussa tietojen lainmukaisesta kohtelusta. [HE, 2007]

Laissa säädetään myös terveydenhuollon valtakunnallisten tietojärjestelmäpalveluiden järjestämisestä. Näitä palveluita ovat arkistointipalvelut, hakemistopalvelut, suostumuksenhallintapalvelut, varmennepalvelut sekä sosiaali- ja terveydenhuollon koodistopalvelu. Tietojärjestelmäpalveluiden avulla voidaan järjestää tietoturvallisesti potilastietojen säilytys, käyttö ja luovuttaminen koko valtakunnan tasolla. Varmennepalvelun tarkoituksena on terveydenhuollon työntekijöiden ja tietoteknisten laitteiden tunnistaminen ja todentaminen. Lisäksi se sisältää sähköisessä allekirjoituksessa vaadittavat palvelut. [HE, 2007]

Asiakkaan tiedonsaantioikeudet luvussa säädetään asiakkaan oikeuksista saada tietoja sähköisistä asiakasrekistereistä, asiakastiedon käsittelyyn liittyvistä tietojärjestelmistä sekä häntä koskevista asiakastietojen käsittelyistä. Asiakkaan oikeus saada tietää häntä koskevien tietojen käsittelystä on oleellista potilaan oikeusturvan takaamiseksi. Luvun säädökset asiakkaan oikeuksista perustuvat pitkälti henkilötietolakiin. [HE, 2007]

2.4.2. Luovutusten ja suostumusten käsittely uudessa laissa

Uusi laki koskee ainoastaan terveydenhuollon toimintayksiköiden asiakirjojen luovuttamista. Potilastietojen sähköistä luovuttamista koskevat pykälät löytyvät luvun 3 alta. Lain 10§ mukaan potilastietojen luovutuksen perustana tulee olla potilaan suostumus tai lakiin perustuva vaatimus tietojen luovuttamisesta. Tämä pohjautuu jo muuhun voimassaolevaan lainsäädäntöön, mutta merkittävyytensä takia asiasta säädetään uudessakin laissa. 10§ toisessa momentissa säädetään potilastietojen sähköiseen luovutuspyyntöön perustuvien tietojen luovutuksen toteutustavoista, kun tietojen luovutus tapahtuu terveydenhuollon palvelun tuottajalta toiselle. [HE, 2007]

Sähköinen luovutuspyyntö koskee tilannetta, jossa terveydenhuollon palvelun tuottaja pyytää sähköisesti potilastietoja oma-aloitteisesti toisesta terveydenhuollon toimintayksiköstä. Ennen varsinaista tietojen luovutusta

tulee varmistaa tietoteknisesti potilastietojen luovutuksen perusteen olemassaolo, eli asiallinen yhteys. Potilastietojen sähköiseen luovutuspyyntöön perustuva luovutus toteutetaankin tästä syystä laissa säädettävien valtakunnallisten tietojärjestelmäpalveluiden avulla. Muut sähköisten potilastietojen luovutukset voidaan järjestää joko valtakunnallisten palveluiden avulla tai sitten palvelun antajien välisenä luovutuksena. Muilla sähköisillä potilastietojen luovutuksilla tarkoitetaan tilannetta, jossa terveydenhuollon palvelun antaja lähettää omasta aloitteestaan omien potilasrekisteriensä tietoja, esim. sähköiset lähete- ja hoitopalautteet. Kaikista tietojen luovutuksista kuitenkin tulee tehdä merkintä potilasasiakirjaan ja lain 5 pykälän perusteella tietojen käyttöä sekä luovutuksia tulee pystyä seuraamaan. [HE, 2007]

Lain 13 § koskee potilaan suostumusta. Laissa määritellään, että suostumus voidaan antaa yhtä palvelutapahtumaa tai palvelukokonaisuutta varten. Palvelukokonaisuus koostuu erilaisista palvelutapahtumista joko yhden tai useamman toimintayksikön välillä. Mikäli palvelutapahtumassa käsitellään ainoastaan yhden toimintayksikön sisäisiä tietoja, niin suostumusta ei tarvita. Palvelukokonaisuutta varten annettava suostumus helpottaa hoitohenkilökunnan työtä, kun suostumusta ei tarvitse pyytää erikseen jokaista yksittäistä tapahtumaa varten. Suostumuksen tulisi olla allekirjoitettu, joko potilaan omakätisesti tai kehittyneellä sähköisellä allekirjoituksella. Poikkeuksena allekirjoitetulle suostumukselle on suullinen suostumus. Suullista suostumusta voidaan käyttää potilaslain 13 §:n 3 momentin 2 kohdassa tarkoitettujen tietojen sekä potilaan hakutietojen luovuttamisessa. [HE, 2007]

Potilaan hakutiedoilla tarkoitetaan merkintöjä, joiden avulla voidaan jäljittää tietyn potilaan potilastiedot muiden terveydenhuollon palvelun antajien sähköisistä potilasrekistereistä. Hakutiedot ovat osa terveydenhuollon toimintayksikön potilasrekisteriä, joten ne ovat potilastietoina salassa pidettäviä. Potilaalla on myös oikeus kieltää hakutietojensa luovutus. Näin potilas voi päättää, löytävätkö muut terveydenhuollon toimijat valtakunnallisen tietojärjestelmän avulla tietoa, että potilas on ollut hoidossa

tietyssä toimintayksikössä. Kielto voidaan tehdä joko palvelutapahtumaa tai sitten kokonaista palvelukokonaisuutta koskevaksi. Potilaalla on myös oikeus peruuttaa hakutietojen luovutuskielto tai tehdä siihen muutoksia. Luovutuskielto on aina allekirjoitettava ja se tulee antaa sille terveydenhuollon palvelujen antajalla, jota kielto koskee. Kiellosta huolimatta tietoja voidaan luovuttaa potilaslaissa määriteltyjen erityisten tilanteiden mukaan.

2.5. Terveydenhuollon tietoteknologiastandardit

Standardi voidaan määritellä seuraavasti: se on tunnetun standardointijärjestön hyväksymä dokumentti, jossa on määritelty yleistä ja toistuvaa käyttöä varten sääntöjä, ohjeita tai piirteitä tuotteille, prosesseille tai palveluille [Mykkänen, et al., 2005]. Standardoinnilla tavoitellaan yhteentoimivampia tuotteita, kun eri osapuolet tietävät yhtenäisesti sovitut säännöt. Tietojärjestelmissä standardien avulla tavoitellaan yhteistoiminnallisuutta, kun käytettävät rajapinnat ja sanomat ovat standardien mukaisia, joten järjestelmien kehittäjien on helpompaa luoda uusia ominaisuuksia. [Ensio ja Ruotsalainen, 2004; Mykkänen et al., 2005]

Standardointijärjestöjä on maailmassa useita kymmeniä. Alle on kerätty merkittävimpiä standardointijärjestöjä:

- ISO (International Organizational for Standardization)
- IEC (International Electrotechnical Commission)
- ITU (International Telecommunication Union)
- CEN (Comite Europeen de Nominalisation)
- ANSI (American National Standards Institute)
- IEEE (the Institute of Electrical and Electronics Engineers, Inc)
- W3C (World Wide Web Consortium)
- OMG (Object management Group)
- OASIS (Organization for the Advanced of Structured Information Standards).

Suomessakin on useita standardointijärjestöjä. SFS on Suomen Standardoimisliitto, joka osallistuu ulkomaisten järjestöjen toimintaan Suomen edustajana (mm. ISO ja CEN). Julkisella sektorilla toimii JUHTA (julkisen hallinnon tietohallinnon neuvottelukunta), joka tuottaa julkisen hallinnon suosituksia (JHS). Myös STAKES ja Suomen kuntaliitto ovat aktiivisia toimijoita Suomalaisessa standardointityössä. Nämä Suomalaiset standardointijärjestöt osallistuvat myös terveydenhuollon standardoimistyöhön. Stakes on esimerkiksi tuottanut erilaisia raportteja ja suosituksia standardien käytöstä. [Ensio ja Ruotsalainen, 2004]

Yleisissä standardointijärjestöissä on myös terveydenhuoltoon keskittyviä osia. ISO TC 215:n tehtäviin kuuluu terveyteen, terveydenhuollon tietoon ja tietotekniikkaan tapahtuva standardointi. ISO TC 215:sta tavoitteisiin kuuluu yhteentoimivuuden ja yhteensopivuuden parantaminen erilaisten järjestelmien välillä. CEN TC 251 on Eurooppalainen terveydenhuollon tekninen toimikunta, joka pyrkii omalla toiminnallaan yhtenäistämään Eurooppalaisia terveydenhuollon sovelluksia. [Mykkänen el al., 2005; Ensio ja Ruotsalainen, 2004]

Maailmalla on myös täysin terveydenhuoltoon keskittyneitä standardointijärjestöjä. Yksi merkittävimmistä järjestöistä on Yhdysvalloissa alun perin perustettu HL7. HL7:n kehittämät standardit ovat terveydenhuollon alueella eniten käytettyjä. Alun perin HL7 alkoi kehittää tiedonsiirtostandardeja, joiden avulla eri tietojärjestelmät pystyisivät keskustelemaan toistensa kanssa. Tiedonsiirtoon liittyvät viestistandardit ovat vieläkin HL7:n standardeista tärkeässä roolissa. HL7 pyrkii määrittämään viestien tietosisältöjä, jotta tietojärjestelmien välisessä tiedonsiirrossa liikkuvat viestit olisivat samanlaisia kaikkialla. [Mykkänen et al., 2005]

HL7 sanomamäärityksien lisäksi, he kehittävät muitakin standardeja. Terveydenhuollon työpöytäintegraatiota varten HL7 on kehittänyt CCOW-standardin (Clinical Context Object Workgroup). HL7 on myös kehittänyt CDA-standardin (Clinical Document Achitecture), jossa on määritelty

potilaskertomusten sisältöjä sekä rakenteita. CDA-standardi on myös Suomessa laajalti käytössä mm. aluetietojärjestelmissä.. HL7 CDA soveltuu hyvin tiedonsiirtoon ja tiedon säilytykseen. HL7:lla on myös toimintaa Suomessa. Sen jäseninä on yrityksiä, sairaanhoitopiirejä ja tutkimuslaitoksia. [Mykkänen et al., 2005]

Toinen merkittävä tekijä terveydenhuollon standardointityössä on IHE (Integrating the Healthcare Enterprise). IHE ei ole varsinainen standardointiorganisaatio, vaan sen tarkoituksena on ohjeistaa erilaisten standardien käyttöä terveydenhuollon tietotekniikassa. IHE kehittää integrointimalleja, joiden perusteella terveydenhuollon järjestelmien yhteistoiminnallisuutta voidaan parantaa. [Mykkänen et al., 2005]

Pääasiallisesti terveydenhuollossa käytetään yleisiä tietoturvastandardeja. Tietoturvallisia järjestelmiä kehitettäessä voidaan standardeja käyttää ainakin tiedonsiirtoon, salaukseen, käyttäjien yksilöintiin, tunnistamiseen, varmenteisiin, sähköisiin allekirjoituksiin ja dokumenttien pitkäaikaiseen säilytykseen [Mykkänen et al., 2005]. Ensio ja Ruotsalainen [2004] ovat määrittäneet listan standardeista, joita terveydenhuollon organisaatioiden tulisi käyttää tietoturvaa toteuttaakseen:

- ISO 17799 (BS7799) Part 1 Code for practice for information security management
- ISO-7816 toimikorttistandardit
- ISO / IEC-7816-X toimikorttistandardi
- PKCS#15 toimikortin sisällölle
- RFC 2459 varmenteelle ja sulkulistastalle
- IETF-PKIX QC laatuvarmennestandardi
- IETF PKI X.509 2527
- ITU X.509 standardi (jonka myös IETF standardisointijärjestö on adaptoinut (IETF RFC 2459)).
- IETF PKI X.509 RFC 2527 (Certification policy & Certification Practice Statement Framework)

- ISO TS 17090 (kolmiosainen terveydenhuollon PKI-standardi, jossa on kuvattu sertifikaattipolitiikkaa, hyviä PKI:n toteutustapoja ja esitetty esimerkkejä sertifikaateista)

Standardien hyöty saavutetaan kunnolla vasta, kun terveydenhuollon organisaatiot ja järjestelmäkehittäjät on saatu noudattamaan samoja standardeja. Tämän vuoksi yhteisten pelisääntöjen sopiminen on ehdottoman tärkeää. Samojen standardien käytöllä voidaan mahdollisesti parantaa järjestelmien tietoturvaa ja yhteistoiminnallisuutta.

3. Tutkimusmenetelmät ja –tavoitteet

3.1. Tutkimuksen tavoitteet

Tämä tutkimus käsittelee Fiale-aluetietojärjestelmäympäristössä tietosuojan toteutumiseen liittyviä asioita. Erityisesti keskityn potilaan suostumuksen ja potilastietojen käsittelyyn sekä käyttäjänhallintaan liittyviin kysymyksiin. Potilastietojen käsittely on tarkoin määritelty erinäisissä laeissa, kuten luvussa kaksi on käsitelty. Lainmukaisuus aiheuttaa täten paineita organisaatioiden toiminnallisuudelle ja tietoturvaratkaisuille.

Terveydenhuollon yksiköiden toiminnassa tietosuojan ja tietoturvan merkitys kasvaa erilaisten tietojärjestelmien hyödyntämisen myötä, koska potilaiden tietojen siirto helpottuu ja mahdollisuudet väärinkäytöksiin kasvavat tiedon sähköisen olomuodon takia. Tiedon liikkuessa toimintayksiköiden välillä asettaa tämä paineita tietoturvan hallinnoinnille yli organisaatiorajojen. Organisaatioiden rajojen ylittävä tiedon käsittely luo haasteita, joita ei aikaisemmin ole varsinaisesti tarvinnut terveydenhuollon palvelutuotannossa huomioida.

Aluetietojärjestelmää tutkin sekä toiminnallisesta että tietojärjestelmätason näkökulmasta. Aluetietojärjestelmää analysoin tietosuojan ja tietoturvan suhteen, jolloin voidaan havaita mahdollisia ongelmakohtia. Aluetietojärjestelmästä tarkastelen erityisesti miten potilaiden suostumuksia käsitellään ja hallitaan sekä miten potilastietojen luovutus ja käsittely tapahtuu. Oleellista on myös arvioida käyttöoikeuksien- ja käyttäjienhallintaa sekä erilaisia valvontakeinoja, kuten seurantalokeja, joilla on suuri merkitys lainmukaisen toiminnan turvaamisessa.

Tutkimuksessa määrittelen aluetietojärjestelmäympäristön nykytilan ja sen pohjalta arvioin, minkälaisia muutoksia tarvitaan, jotta voidaan täyttää lainsäädännön vaatimukset. Tutkimuksen tuloksina analysoin, miten lainsäädännön vaatimukset on täytetty sekä toiminnallisesti että tietojärjestelmätasolla. Suomessa tuli heinäkuussa 2007 voimaan uusi laki potilastietojen sähköisestä käsittelystä. Lailla tulee olemaan vaikutuksia myös nykyisiin aluetietojärjestelmiin. Tulevaisuudessa siirrytään puhtaasti alueellisista järjestelmistä kohti valtakunnallisia tietojärjestelmäpalveluita. Osana tutkimusta pohdin, minkälaisia vaikutuksia lailla on aluetietojärjestelmiin.

3.2. Tutkimusmenetelmät

Tässä tutkimuksessa kuvaan millainen on nykytila aluetietojärjestelmäympäristössä sekä luon uutta teoriaa miten asioiden tulisi olla tietyn tapauksen perusteella. Tutkimus on reaalimaailmaa tarkasteleva, uutta teoriaa luova empiirinen tapaustutkimus. Tapaustutkimuksessa tiedonhankintatapoina ovat kyselyt, haastattelut, havainnointi ja arkistomateriaalin käyttö. [Järvinen & Järvinen, 2004]

Tutkimuksessa tarkastelen Fiale-aluetietojärjestelmää ja sen käyttötilanteita Pirkanmaan ja Satakunnan sairaanhoitopiireissä. Tässä vaiheessa määrittelen siis järjestelmän ja sen käytön nykytila. Nykytilan ja lainsäädännön vaatimusten sekä rajoitusten perusteella luodaan uutta teoriaa, eli miten aluetietojärjestelmäympäristössä asiakastietojen käsittely ja suostumusten hallinta tulisi hoitaa, jotta voidaan varmistua tietosuojan toteutumisesta.

Nykytilan selvittämisessä perustana voidaan pitää Pirkanmaan ja Satakunnan sairaanhoitopiirien, aluetietojärjestelmien ylläpitäjien ja kehittäjien tekemiä erilaisia ohjeita, oppaita sekä mallinnuksia. Järjestelmän suunnittelu-, toteutus- ja kehitystyössä tehtyjen mallinnusten ja määrittelyjen avulla on mahdollista

selvittää, miten aluetietojärjestelmä toimii ja minkälaisia mahdollisia riskejä ja ongelmia siinä esiintyy tietoturvan tai tietosuojan kannalta.

Tutkimuksen perustana toimivat sairaanhoitopiirien tietoturvapolitiikat, potilastietojen käsittelyohjeet, aluetietojärjestelmän erilaiset käyttö- ja muut ohjeet sekä organisaatioiden yleiset tietotekniset ohjeistukset. Lisäksi erilaiset tietoturvaoppaat ja ohjeistukset auttoivat tutkimuksen teossa. Kirjallisen tietoturvamateriaalin perusteella oli hyvä kartoittaa kokonaiskuvaa järjestelmän tietoturvallisuudesta ja mahdollisista ongelmakohdista.

Kirjallisen materiaalin luomaa kuvaa täydensin järjestelmän kehittäjien, ylläpitäjien ja pääkäyttäjien haastatteluilla. Siten sain käytännön kokemuksia ja ajatuksia järjestelmästä. Tietoturvavastaavien avulla pystyin määrittelemään miten tiedonsiirtoon, käyttäjänhallintaan, todentamiseen, rooleihin ja valvontaan liittyvät asiat on ratkaistu. Myös sairaanhoitopiirien tietohallintoon kuuluvia henkilöitä haastateltiin. Heidän tehtäviinsä kuuluu sairaanhoitopiirien tietoturvan suunnittelu ja hallinnointi sekä kokonaiskuvan suunnittelu. Tietohallinnon avulla sain kuvan, miten organisaatioiden toiminnassa tietoturva ja tietosuoja kysymykset on ratkaistu sekä miten käyttäjien ohjeistus ja koulutus on hoidettu. Pääasiassa organisaation toiminnallisen tason arviointi keskittyy Pirkanmaan sairaanhoitopiirin.

Järjestelmään tutustuin myös käytännössä koulutusympäristön avulla. Käytännön tutustumisen avulla pystyin havainnoimaan miten järjestelmä todellisuudessa toimii, ja minkälaisia mahdollisia ongelmia siinä on. Lisäksi sairaanhoitopiireissä järjestettiin pienimuotoisia demoesityksiä järjestelmän käytöstä.

3.3. Tietosuojan ja tietoturvan arviointikriteeristö

Aluetietojärjestelmän ja sen käytön nykytilan määrittämiseen käytän tutkimuksen yhteydessä kehitettyä kriteeristöä. Kriteeristö on eräänlainen tarkistuslista, johon on kerätty vaatimuksia, rajoituksia ja kysymyksiä mitä aluetietojärjestelmäympäristössä tulee huomioida sekä ratkaista liittyen tietosuojaan ja tietoturvaan. Kriteeristön vaatimukset ja rajoitukset on johdettu Suomen lainsäädännöstä, erityisesti luvussa 2 mainituista.

Kriteeristöön on kerätty vaatimuksia jotka kohdistuvat sekä tietojärjestelmiin että hoitohenkilökunnan toimintaan. Kriteeristön avulla määritellään miten tietosuoja ja tietoturva on ratkaistu. Tämän määrittelyn perusteella voidaan havaita, missä kohdin on parannettavaa, mitkä asiat hoidetaan jo hyvin ja mitkä ovat kriittisiä kohtia tietosuojan ja tietoturvan kannalta. Kriteeristöä käytettiin tutkimuksen yhteydessä olevien haastattelujen kysymysrunkona.

Kriteeristö koostuu seitsemästä ylätasosta. Ylätasoja ovat yleiset lainsäädännölliset vaatimukset, suostumusten hallinta, potilastietojen luovutus ja käsittely, yleinen tietoturva, ohjelmistoturvallisuus, tietoliikenneturvallisuus sekä lokit ja valvonta. Kuvassa 9. näkyy yleiskuva kriteeristöstä. Eri tasojen vaatimuksia otetaan huomioon, myös muiden tasojen tarkastelussa. Esimerkiksi yleiset lainsäädännölliset vaatimukset kohdistuvat käytännössä kaikkiin tasoihin, jolloin ne huomioidaan muiden tasojen analysoinnissa.

Vaatimukset	Tietojärjestelmä taso	Toiminnallinen taso	Arviointi nykytilasta
1. Yleiset lainsäädännölliset vaatimukset			
Etukäteissuunnittelun vaatimus			
Yhteysvaatimus			
…			
2. Suostumusten hallinta			
Suostumuksen kohde			
Suostumuksen rajaus			
…			
3. Potilastietojen luovutus ja käsittely			
Tiedon luovuttajan vastuut			
Vastaanottajan velvollisuudet			
…			
4. Yleinen tietoturva			
Tietojen eheys			
Tietojen käytettävyys			
…			
5. Ohjelmistoturvallisuus			
Käyttäjäroolit			
Käyttöoikeudet			
…			
6. Tietoliikenneturvallisuus			
Siirrettävän tiedon eheys ja luottamuksellisuus			
Tietoliikenteen salaus			
…			
7. Lokit ja valvonta			
Tapahtumatietoloki			
Käyttäjäloki			
…			

Kuva 9. Yleiskuva kriteeristöstä.

Kriteeristön ensimmäinen ylätaso on yleiset lainsäädännölliset vaatimukset. Tähän kohtaan on kerätty yleisiä lainsäädännön asettamia vaatimuksia terveydenhuollon tietojenkäsittelylle. Pääasiallisesti nämä vaatimukset johtuvat henkilötietolaista, mutta joukossa on myös mukana mm. vaatimuksia julkisuuslaista ja potilaslaista. Taulukkoon 1 on listattu tarkasteltavat vaatimukset.

1. Yleiset lainsäädännölliset vaatimukset		
Etukäteissuunnittelun vaatimus		
Yhteysvaatimus		
Huolellisuus- ja suojaamisvelvoite		
Virheettömyys, eheys ja luotettavuus		
Käyttötarkoitussidonnaisuus		
Tarpeellisuusvaatimus		
Rekisterinpitäjän velvollisuudet (ohjeistus + valvonta)		
Asiakkaan informointi henkilötietojen käsittelystä		
Asiakkaan tarkastusoikeus		
Luottamuksellisen viestin suoja		
Luottamuksellinen hoitosuhde		
Tiedon alkuperän tunnistettavuus		
Tietojen suojaamisvelvoite		
Hyvä tiedonhallintatapa		
Vaitiolovelvollisuus ja salassapito		
Tietojen saatavuus ja käytettävyys		
Tietosuoja riskianalyysi		
Alkuperäisen tiedon muuttumattomuus		

Taulukko 1. Yleiset lainsäädännölliset vaatimukset.

Suostumusten hallinta kohdassa on listattu vaatimuksia, mitä lainsäädäntö asettaa suostumuksille. Siinä käsitellään suostumuksen sisältöä, käsittelyä, hallintaa ja velvoitteita. Taulukossa 2 esitellään suostumukseen kohdistuvia vaatimuksia ja velvoitteita.

2. Suostumus ja sen hallinta		
Kohde		
Rajaus		
Saaja		
Syy		
Kesto		
Antaja		
Tyyppi		
Allekirjoitus		
Asiakkaan informointi		
Sähköinen allekirjoitus		
Asiakkaan suostumukset		
Suostumusten arkistointi		
Suostumusloki		

Taulukko 2. Suostumus ja sen hallinta.

Kolmantena tasona on varsinainen potilastietojen luovutus ja käsittely (taulukko 3.). Siinä tarkastellaan minkälaisia vaatimuksia lainsäädäntö asettaa potilastietojen luovutukselle ja käsittelylle. Tärkeimpiä kohtia ovat, mitä vaatimuksia ja velvoitteita pitää täyttää, ennen kuin luovutus on mahdollinen ja mitä luovutuksen saajan tulee täyttää. Lisäksi siinä tarkastellaan miten potilastietojen käsittelyn tulee aluetietojärjestelmäympäristössä tapahtua.

3. Potilastietojen luovutus ja käsittely		
Tiedon luovuttajan vastuut henkilötietolaissa		
Vastaanottajan velvollisuudet henkilötietolaissa		
Suostumuksen huomioimien luovutuksessa		
Luovutus ilman suostumusta		
Tiedon käsittelyyn oikeutetut henkilöt		
Luovutuksen edellytyksien tarkastus		
Tietojen luovutusprosessi (esim. merkinnät potilaskertomukseen)		
Luovutuspyynnön tietosisältö		
Potilastietojen käsittely: ohjeistus ja lainsäädännön huomioiminen		

Taulukko 3. Potilastietojen luovutus ja käsittely.

Yleinen tietoturvataso koostuu lainsäädännön asettamista vaatimuksista tietoturvalle. Vaatimukset johtuvat pääasiallisesti henkilötietolaista, julkisuuslaista ja julkisuusasetuksesta. Tässä kohdassa tarkastellaan että miten pystytään mm. turvaamaan tiedon kiistämättömyys, eheys ja jäljitettävyys sekä miten varmistutaan luovutuksen edellytyksien täyttämisestä. Lisäksi tarkastelun alaisena on tietoturvan hallinnointi, johon kuuluu organisaatioiden tietoturvatoiminta ja erilaiset tietoturvapolitiikat sekä -ohjeistukset.

4. Yleinen tietoturva		
Tietojen eheys		
Tietojen käytettävyys ja saatavuus		
Tietojen suojaus ja salaus		
Tietojen muuttumattomuus		
Tietojen kiistämättömyys		
Tietojen luottamuksellisuuden säilyttäminen		
Tietoturvan vastuuttaminen		
Turvaluokitukset		
Käyttäjien koulutus, vastuuttaminen ja velvoitteet		
Tietoturvan suunnittelu ja hallinta (mm. tietoturvapolitiikka)		
Järjestelmien ja prosessien dokumentointi		
Ohjeistus		
Dokumentointi (järjestelmät ja tietoturvaratkaisut)		

Taulukko 4. Yleinen tietoturva.

Viides pääkohta kriteeristössä on ohjelmistoturvallisuus (taulukko 5.). Tämä sisältää ohjelmistoturvallisuuden alueen vaatimuksia. Kohdan tärkeimpiä asioita ovat pääsynhallinta ja käyttäjänhallinta sekä niiden ratkaisut. Pääsynhallinta ja käyttäjänhallinta sisältävät mm. tunnistamiseen ja todentamiseen liittyviä asioita. Kohta ei kuitenkaan perustu pelkästään teknisten ratkaisujen tarkasteluun, vaan tärkeitä ovat myös organisaation prosessit liittyen esimerkiksi käyttöoikeuksien myöntämiseen ja valtuuksien määrittämiseen.

5. Ohjelmistoturvallisuus		
Käyttäjänhallinta		
Käyttäjien tunnistaminen ja todentaminen		
Käyttäjäroolit		
Oikeudet ja valtuudet		
Pääsynhallinta		
Vastuut		
Käyttöoikeuksien hakemisprosessi		
Dokumentointi		
Käyttäjäkoulutukset ja ohjeistukset		
Prosessin tietoturva (tunnuksien jakelu yms.)		
Valtuuksien yksityiskohtainen määrittely		
Tunnuksien sulkeminen ja korttien hävittäminen		
Käytön seuranta ja valvonta		
Kirjautumisprosessi		
Asiakkaan tunnistaminen		
Oikeudet hoitoprosessiin		
Korttien väärinkäytökset		

Taulukko 5. Ohjelmistoturvallisuus.

Tietoliikenneturvallisuuskohta sisältää järjestelmän tietoliikenteeseen kohdistuvia vaatimuksia. Kohdassa käsitellään esimerkiksi tiedonsiirtoon ja tietojen salaukseen liittyviä kysymyksiä. Tärkeitä asioita ovat mm. PKI, sähköinen allekirjoitus ja varmenteet. Kohdassa siis pyrin selvittämään miten voidaan turvata sanomien luottamuksellisuus, alkuperäisyys ja koskemattomuus sekä miten tiedonsiirron osapuolet voivat varmistua toisistaan.

6. Tietoliikenneturvallisuus		
Siirrettävän tiedon eheys ja luottamuksellisuus		
Tietoliikenteen salaus		
Tietojen muuttumattomuus ja kiistämättömyys		
Osapuolten aitous ja oikeus (tunnistus, todentaminen)		
Tietojen sähköinen allekirjoitus		
Tietojen turvaamisen menetelmät		
Järjestelmän tietoturvaratkaisujen suunnittelu ja dokumentointi		
Ulkopuolisten tahojen käytön esto		

Taulukko 6. Tietoliikenneturvallisuus.

Kriteeristön viimeinen kohta sisältää lokeihin ja valvontaa liittyviä vaatimuksia. Lainsäädäntö asettaa vaatimuksen, että terveydenhuollon tietojärjestelmiä pitää pystyä valvomaan ja käyttöä seuraamaan. Tässä kohdassa pyritään selvittämään miten aluetietojärjestelmässä valvonta ja käytön seuranta on järjestetty.

7. Lokit ja valvonta		
Tapahtumatietoloki		
Käyttäjäloki		
Asiakkaan tarkastusoikeus		
Suostumukset		
Luovutusloki		
Käytön seuranta ja valvonta		
Väärinkäytökset: prosessi sekä tiedottaminen		
Valvonnan vastuut		
Kurinpitotoimet		
Tietoturvaloukkausten seuranta		

Taulukko 7. Lokit ja valvonta.

Kriteeristön avulla suoritetun analyysin perusteella nähdään, minkälainen nykytila aluetietojärjestelmässä on suhteessa tietosuojaan ja tietoturvaan. Tämän nykytila-analyysin perusteella voidaan päätellä, mitä kehitettävää

Fiale-aluetietojärjestelmissä ja niiden käytössä on nykyisen lainsäädännön suhteen. Kriteeristön perusteella voidaan myös alustavasti analysoida, minkälaisia muutoksia aluetietojärjestelmiin kohdistuu uuden lain sosiaali- ja terveydenhuollon asiakastietojen sähköistä käsittelystä astuttua voimaan.

4. Aluetietojärjestelmä

4.1. Saumaton palveluketju

Terveydenhuolto Suomessa on perinteisesti ollut erittäin organisaatiokeskeistä ja tietojärjestelmät on suunniteltu yhden organisaation tarpeisiin. Potilaiden hoito on usein sarja rajat ylittäviä palveluita, jossa on monia toimijoita eri organisaatioista. Viime vuosina Suomessa on alettu terveydenhuollon kohdalla lähestyä potilaiden hoitoa asiakaslähtöisesti. Asiakaslähtöinen ajattelutapa vaatii kuitenkin organisaatioiden rajojen ylittävää saumatonta tiedonkulkua. Asiakaslähtöinen ajattelu on tuonut terveydenhuoltoon muilta aloilta tutun prosessikeskeisen toimintamallin. Kyseistä prosessiajattelua kuvataan yleensä palveluketju-käsitteellä. [STM, 1998; Tuuri, 2003; Ruuska ja Haukkapää-Haara, 2004]

Terveydenhuollossa jouduttiin 1990-luvun loppupuolella pohtimaan asiakaskeskeistä toimintatapaa, koska väestö ikääntyi kovaa vauhtia ja hyvinvointiyhteiskuntaa kohtasi uhkia mm. korkean työttömyyden muodossa. Lisäksi asiakaslähtöistä ajattelua tuki tieto- ja viestintäteknologioiden kehittyminen. Teknologian kehittyminen mahdollisti toiminnan kehittämisen ja uusien toimintamallien luomisen. Tavoitteena palveluketjumallissa oli yhdistää erilliset järjestelmät ja organisaatiot, jolloin tieto olisi käytettävissä kaikkialla. Asiakaslähtöisellä ajattelutavalla tavoitellaan potilaan hoidon tuottamista mahdollisimman tehokkaasti ja samalla pyritään verkottamaan sirpaloituneet palveluntarjoajat. Palveluketju toimintamallilla pyrittiin mahdollistamaan asiakkaan palvelu saumattomasti ja alueellisesti eri toimintayksiköiden kesken. [STM, 1998; Ruotsalainen, 2000]

Laki sosiaali- ja terveydenhuollon saumattoman palveluketjun ja sosiaaliturvakortin kokeilusta (811/2000) astui voimaan lokakuussa 2000. Tällä

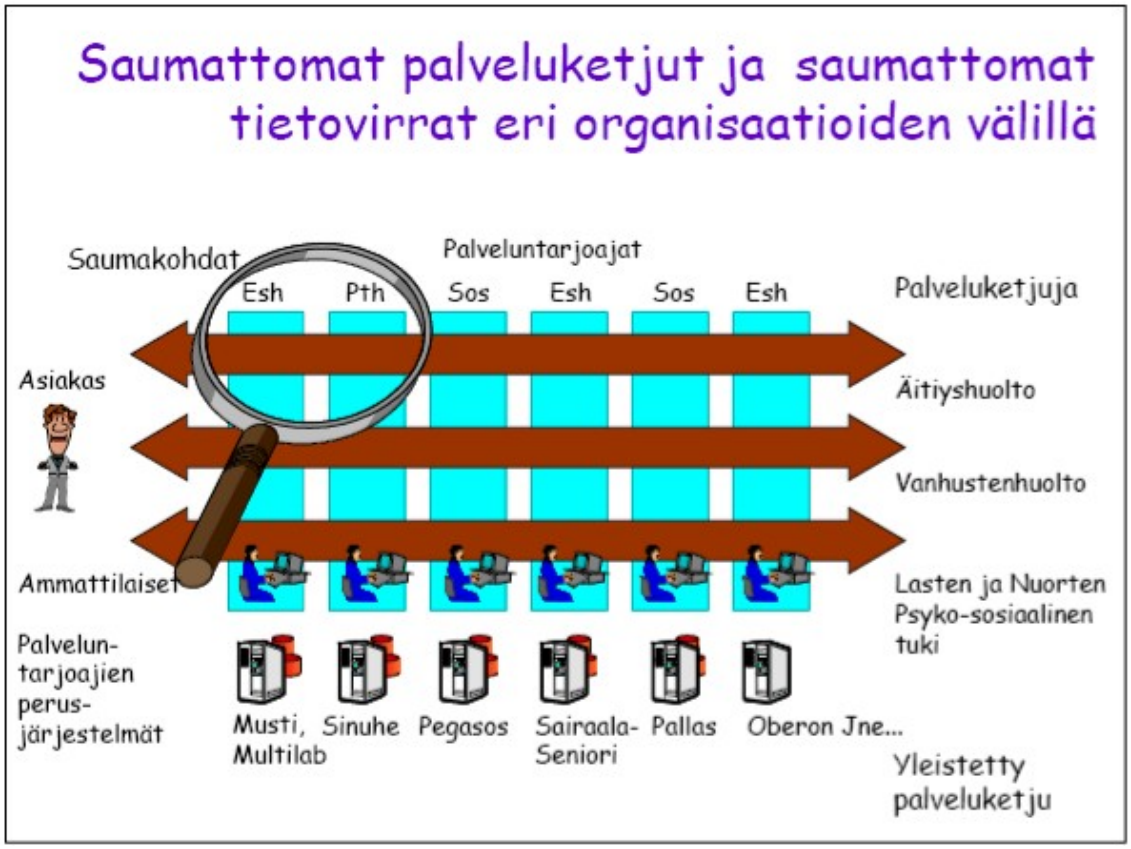
hetkellä lain voimassaoloaikaa on jatkettu vuoden 2011 loppuun asti. Samalla kun lain voimassaoloa jatkettiin, niin lain nimi muuttui laiksi sosiaali- ja terveydenhuollon saumattoman palveluketjun kokeilusta (1225/2003). Laissa säädetään mm. sosiaali- ja terveydenhuollon saumattoman palveluketjun kokeilusta. Palveluketjulla tarkoitetaan saman asiakkaan tiettyyn ongelmaan kohdistuvaa organisaatiorajojen ylittävää suunnitelmallisesti ja yksilöllisesti toteutettua kokonaisuutta [Sinervo, 2004]. Lain kolmannessa pykälässä saumaton palveluketju määritellään seuraavasti:

> *"saumattomalla palveluketjulla* tarkoitetaan toimintamallia, jossa asiakkaan sosiaali- ja terveydenhuollon ja muun sosiaaliturvan asiakokonaisuuteen liittyvät palvelutapahtumat yhdistyvät asiakaslähtöiseksi ja joustavaksi kokonaisuudeksi riippumatta siitä, mikä toiminnallinen yksikkö on palvelujen järjestäjä tai toteuttaja"

Saumattoman palveluketjun toteuttaminen vaatii terveydenhuollon organisaatioita yhtenäistämään toimintakäytäntöjään sekä sopimaan yhteisistä käsitteistä, termistöistä ja luokituksista. Yhtenäistämisprojekteja on tehty ihan valtakunnallisella tasolla mm. erilaisia sähköiseen potilaskertomukseen liittyviä hankkeita sekä Makropilotti hankkeessa. Palveluketjun muodostuessa kokonaisuudesta, jossa potilasta hoidetaan useammassa kuin yhdessä organisaatiossa, terveydenhuollon ammattilaisen pitää olla tietoinen muiden ketjuun osallistuvien toiminnoista ja toimintatavoista kokonaisuuden hahmottamiseksi. [Ruuska ja Haukkapää-Haara, 2004]

Makropilotti - hankkeessa saumattomia palveluketjuja kehitettiin asiakaskeskeisestä näkökulmasta. Tavoitteena oli palveluiden järjestäminen asiakaslähtöisesti, tiedonkulun esteetön liikkuminen yli organisaatiorajojen sekä palvelutuotannon verkostomaisuus. Edellytyksenä asiakkaan joustavalle palvelulle läpi palveluketjun on erilaisten palveluprosessien tunnistaminen ja määrittäminen, toimintojen organisointi organisaatiokeskeisistä kohti asiakaskeskeisyyttä sekä prosessien hallintaa organisaatio- ja ammattirajojen

ylittävällä yhteistyöllä. Kuvassa 10. esitetään, minkälaisessa ympäristössä asiakkaan palveluketjut ja tietovirrat liikkuvat. [STM, 1998; STM, 2002]



Kuva 10. Saumattomat palveluketjut ja tietovirrat eri organisaatioiden välillä [STM, 2002, s 22].

Saumattomien palveluketjujen tukemiseksi on terveydenhuollon toimintayksiköissä alettu pohtia ratkaisuja organisaatiorajojen ylittävään tietojenkäsittelyyn. Sosiaali- ja terveydenhuollossa käytössä olevat useat keskenään yhteentoimimattomat järjestelmät ovat muodostaneet merkittävän hidasteen toiminnan kehittämiselle ja verkostoitumiselle. Tämän takia palveluiden tuottajat ovat kehittäneet yhdessä organisaatioiden välisiä toimintaprosesseja ja näitä tukevia tietojärjestelmiä, jotta voidaan taata potilaille saumaton palveluketju. [Ekebom et al., 2003]

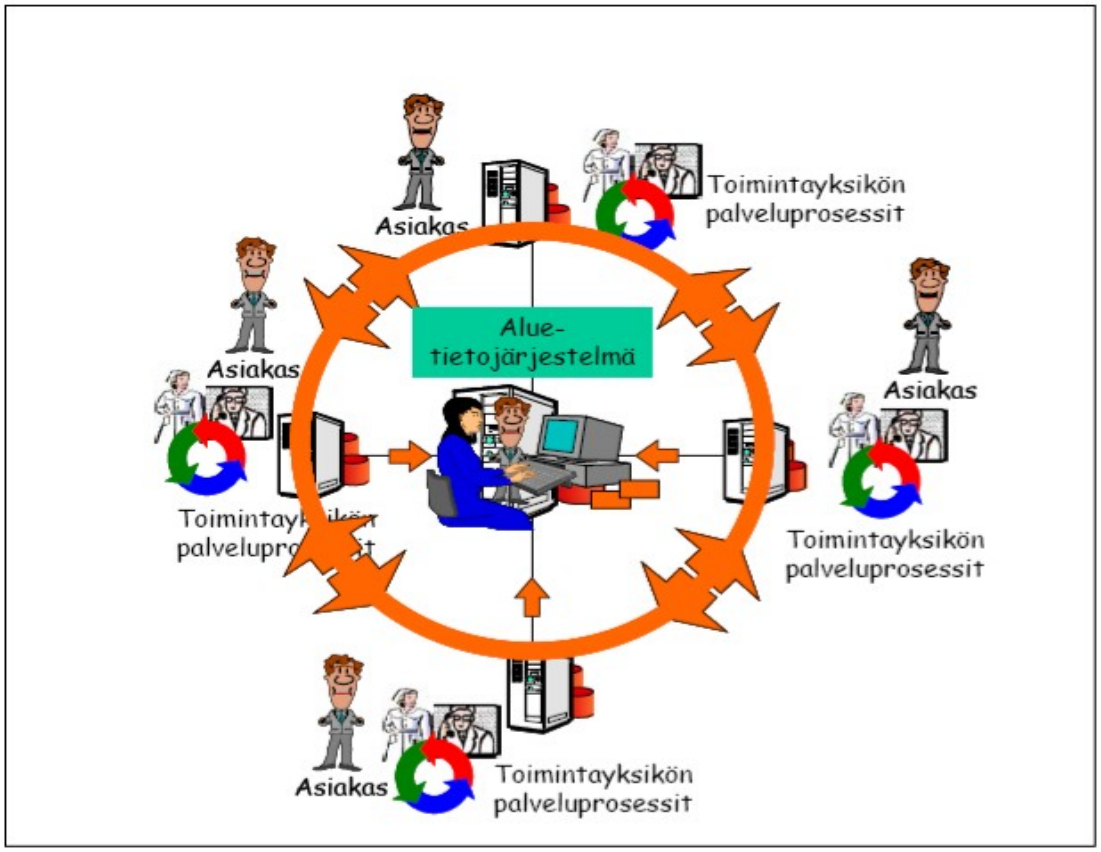
Saumattomien palveluketjujen luomiseksi terveydenhuollon organisaatioiden on saatava tietojärjestelmänsä yhteentoimiviksi. Järjestelmien yhteistoiminnallisuudella voidaan parantaa organisaatioiden välistä tiedonkulkua ja yhteistyötä. Tiedonkulun parantuessa hoitoon osallistuvien tehtävät helpottuvat ja nopeutuvat, kun tietoa on tarjolla kaikille toimijoille. Potilaan hoitotilanne on aina hallinnassa, riippumatta siitä mikä on hoitava toimintayksikkö, kun järjestelmät pystyvät keskustelemaan keskenään. Organisaatioiden yhteistyön kehittyessä ja organisatoristen kuilujen vähentyessä voidaan kenties saavuttaa kustannussäästöjä, kun tiedonpuutteesta johtuvat päällekkäiset hoidot ja tutkimukset sekä epäjohdonmukaisuudet voidaan karsia. Potilaan näkökulmasta katsottuna hoidon laatu paranee ja nopeutuu, kun hoito-ohjeet, lääketiedot ja muut tiedot seuraavat joustavasti mukana. [STM 1998; Tuuri, 2003; Saranummi, 2000; Ruuska ja Haukkapää-Haara, 2004]

Terveydenhuollon organisaatiot ovat pyrkineet vastaamaan tiedon liikkumisen tarpeisiin luomalla yhteisiä aluetietojärjestelmiä, joiden avulla voidaan vaihtaa tietoa helposti toimintayksiköiden välillä. Saumattomien palveluketjujen hyödyntäminen ei kuitenkaan perustu vain teknologiaan, vaan se vaatii organisaatioilta myös rakenteellisia sekä toimintatapojen ja –kulttuurien muutoksia. [STM 1998; Tuuri, 2003; Saranummi, 2000; Ruuska ja Haukkapää-Haara, 2004]

Laissa sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä esitellään korvaava käsite saumattomalle palveluketjulle. Laissa puhutaan palvelukokonaisuudesta, jolla tarkoitetaan yhden tai useamman terveydenhuollon palveluntarjoajan tuottamien palveluiden yksilöityä kokonaisuutta. Tässä tutkimuksessa kuitenkin käytetään näitä molempia termejä, johtuen siitä että saumaton palveluketju käsite liittyy olennaisesti aluetietojärjestelmiin.

4.2. Aluetietojärjestelmä

Sosiaali- ja terveydenhuollon aluetietojärjestelmällä tarkoitetaan usean organisaation käyttämää yhteistä asiakas- ja potilastietojärjestelmää sekä sen hallintaan käytettäviä komponentteja. Aluetietojärjestelmän tarkoituksena on mahdollistaa potilaiden tietojen vaihto eri toimintayksiköiden välillä alueellisessa sosiaali- ja terveydenhuollossa. Sen avulla voidaan katsella potilaiden tietoja toisten toimintayksiköiden rekistereistä (kuva 11.). [Sinervo, 2004; STM, 2002]



Kuva 11. Aluetietojärjestelmä mahdollistaa asiakkaan tietojen katselun eri toimintayksiköissä [STM, 2002, s 42].

Aluetietojärjestelmä tukee saumattomia palveluketjuja tarjoamalla tietoa eri organisaatioille potilaan hoitoon liittyen. Potilaan tietojen liikkumisen parantumisella voidaan saavuttaa sekä hoidon laadun paranemista että myös kustannussäästöjä, kun vältetään päällekkäisiä tutkimuksia ja hoitoja.

Alueellinen terveydenhuollon tietojenkäsittely voidaan toteuttaa usealla eri toteutustavalla, mutta tässä tutkimuksessa keskitytään viitejärjestelmään perustuviin tietojärjestelmiin, joita Suomessa yleisesti kutsutaan aluetietojärjestelmiksi. [Sinervo, 2004; STM, 2002; Mikola, 2003]

Aluetietojärjestelmiä on kehitetty helpottamaan terveydenhuollon ammattilaisen työtä, potilaan hoitoa. Sen avulla hoitohenkilöstön on helpompi muodostaa kokonaiskuva potilaan hoidosta ja historiasta. Ilman aluetietojärjestelmää potilaan tietojen katselu toisten toimintayksiköiden rekistereistä olisi käytännössä mahdotonta, ammattilaisella ei edes olisi tietoa mistä potilaan hoitotietoja löytyisi. Lisäksi yhden järjestelmän käytön oppiminen on huomattavasti helpompaa kuin usean eri potilasjärjestelmän. [Lausvaara et al., 2004]

Aluetietojärjestelmän avulla voidaan myös suunnitella potilaan hoitoa paremmin luomalla erilaisia palveluketjusuunnitelmia. Palveluketjuilla voidaan paremmin hallinnoida potilaan hoitoa eri toimintayksiköissä ja samalla tämä helpottaa potilaan tietojen liikkumista eri hoitoon osallistuvien toimijoiden välillä. Lisäksi aluetietojärjestelmän tulisi tuottaa toimintayksiköille tietoa toiminnan suunnittelua, ohjausta sekä seurantaa varten. [Lausvaara et al., 2004; Nykänen ja Karimaa, 2002]

Alueellista tietojenkäsittelyä kehitettäessä ja toimittaessa yli organisaatiorajojen kohdataan uudenlaisia haasteita. Nykänen ja Karimaa [2002] esittävät suuriksi haasteiksi toiminnallisen ja semanttisen yhteistoiminnallisuuden. Koska tarkoituksena on yhdistää eri sosiaali- ja terveydenhuollon toimintayksiköiden järjestelmiä toisiinsa, suureksi haasteeksi muodostuu erilaisten toimintakulttuurien, toimintatapojen, prosessien, palvelumuotojen ja tietojärjestelmien erilaisuus sekä käsitteiden, tietojen ja tietosisältöjen yksikäsitteinen ja riittävä määrittely.

Aluetietojärjestelmät nähdään muodostuvan palveluprosesseista, ihmistä sekä tietojärjestelmistä. Aluetietojärjestelmä tulee suunnitella asiakaslähtöisesti ja tämä vaatii asiakkaiden tarpeiden sekä vaatimusten määrittelyä. Onnistuminen edellyttää alueellisen yhteistyön organisoimista ja vastuuttamista sekä osaamista monelta eri ydinalueelta. Perustana yhteistyön sisällölle on kansallinen lainsäädäntö ja suositukset, koska järjestelmässä käsiteltävät tiedot ovat pääsääntöisesti arkaluonteisia ja salassa pidettäviä. [Nykänen ja Karimaa, 2002]

Aluetietojärjestelmän käyttäjäorganisaatioiden välillä pitää sopia yhteisistä tietoturvapolitiikoista ja tietosuojaohjeista, jotta voidaan varmistua järjestelmän ja sen käytön lainmukaisuudesta ja tietoturvallisuudesta. Mikola [2003] nostaa kuusi erityistä tietosuojavaatimusta aluetietojärjestelmille:

- käyttäjien tunnistaminen
- käyttöoikeuksien laatimisperiaatteet
- suostumusten hallinta
- käytön seuranta
- rekisterinpidon hallinta
- dokumentointi.

Aluetietojärjestelmässä potilaan tiedot säilytetään toimintayksiköiden omissa potilasrekistereissä, joten jokainen rekisterinpitäjä vastaa tietojen oikeellisuudesta sekä säilyttämisestä lakien ja säädösten mukaisesti. Aluetietojärjestelmällä luodaan tekninen katseluyhteys potilaan tietoihin. Eli tieto ei varsinaisesti siis liiku potilasrekistereistä toisiin, vaan aluetietojärjestelmän avulla terveydenhuollon ammattilainen voi ainoastaan katsella toisten toimintayksiköiden rekistereiden tietoja. Katseluyhteys kuitenkin tulkitaan tietojen luovuttamiseksi, joten pääsääntöisesti ammattilainen tarvitsee potilaan suostumuksen tietojen katseluun.

4.3. Pirkanmaan ja Satakunnan sairaanhoitopiirit

Pirkanmaan sairaanhoitopiiri (PSHP) on 28 kunnasta muodostunut kuntayhtymä, jonka vaikutusalueella asuu noin 470000 ihmistä. Varsinaisten jäsenkuntien lisäksi sairaanhoitopiirin yliopistollinen sairaala tuottaa erityistason palveluita Kanta-Hämeen, Etelä-Pohjanmaan ja Vaasan sairaanhoitopiireille, sekä Päijät-Hämeen sosiaali- ja terveysyhtymälle (Kuva 12.). Kaiken kaikkiaan palveluiden piirissä on siis yli miljoona ihmistä. [PSHP, 2007]

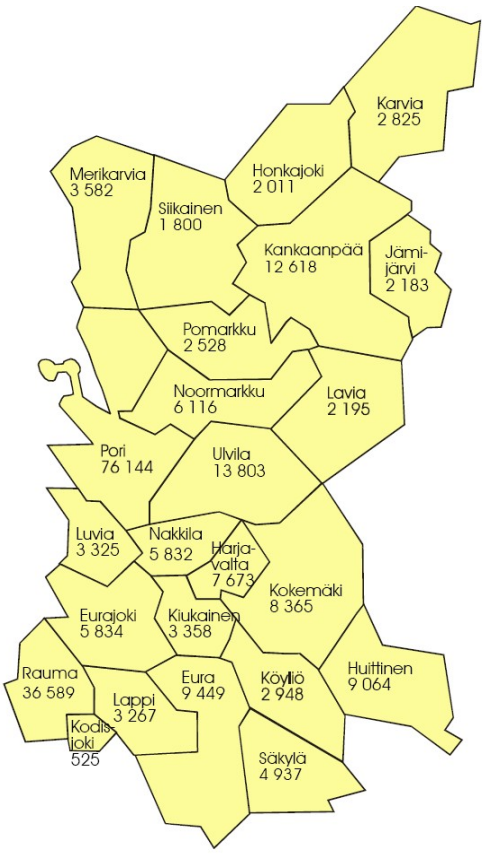
Kuva 12. Pirkanmaan sairaanhoitopiiri ja sen erityisvastuualueet [PSHP, 2007].

Pirkanmaan sairaanhoitopiiriin kuuluu Tampereen yliopistollinen sairaala (TAYS), Vammalan (VAS) ja Valkeakosken aluesairaalat (VALS) sekä Mäntän seudun terveydenhuoltoalue (MTSH). Yhteensä näissä oli vuonna 2004 vuodeosastopaikkoja noin 1550, suurimpana yksikkönä Tays. Henkilöstöä

sairaanhoitopiirissä on noin 5700. Potilaita hoidetaan vuodessa vuodeosastoilla noin 75000 ja poliklinikoilla noin 370000. [PSHP, 2007; PSHP, 2004]

Helmikuussa 2007 PSHP:n aluetietojärjestelmää käytettiin 36 julkisessa organisaatiossa ja kahdessa yksityisessä. Organisaatioissa järjestelmän käyttäjiä Pirkanmaalla oli yli 1400. Pirkanmaalaisista potilaista järjestelmässä oli yli 7,5 miljoonaa viitetietoa (30.11.2006). Aluetietojärjestelmällä pystyttiin tarkastelemaan Pirkanmaan sairaanhoitopiirin (TAYS, VALS, VAS ja MTSH), Virtain ja Kihniön terveyskeskusten potilasjärjestelmien tietoja. [YT Tieto, 2007]

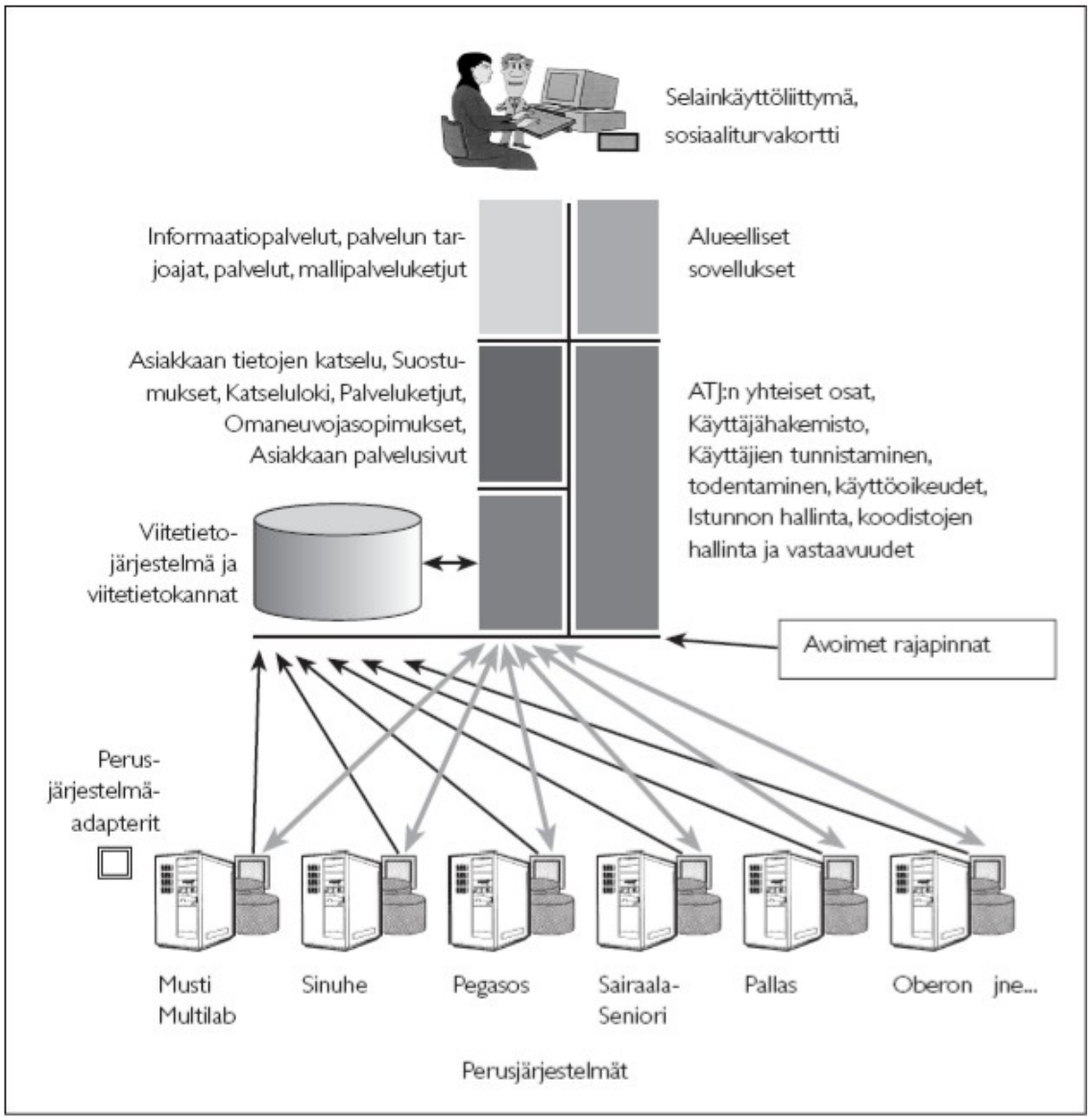
Satakunnan sairaanhoitopiiri tarjoaa erikoissairaanhoidon palveluita 23 jäsenkunnalleen. Asukkaita näissä kunnissa on noin 227000 (kuva 13.). Sairaaloita piirissä on Porissa, Raumalla ja Harjavalla. Henkilöstöä sairaanhoitopiirissä on noin 3500. Hoitopäiviä vuodessa on noin 205000. Satakunnassa Fialella pystytään katselemaan SatSHP:n tietojen lisäksi kymmenen muun organisaation potilastietoja (mm. kuntayhtymiä ja terveyskeskuksia). Lisäksi sillä pystytään tarkastelemaan Varsinais-Suomen sairaanhoitopiirin aluetietojärjestelmän piiriin kuuluvia tietoja. [SatSHP, 2007]



Kuva 13. Satakunnan sairaanhoitopiiri [SatSHP, 2007]

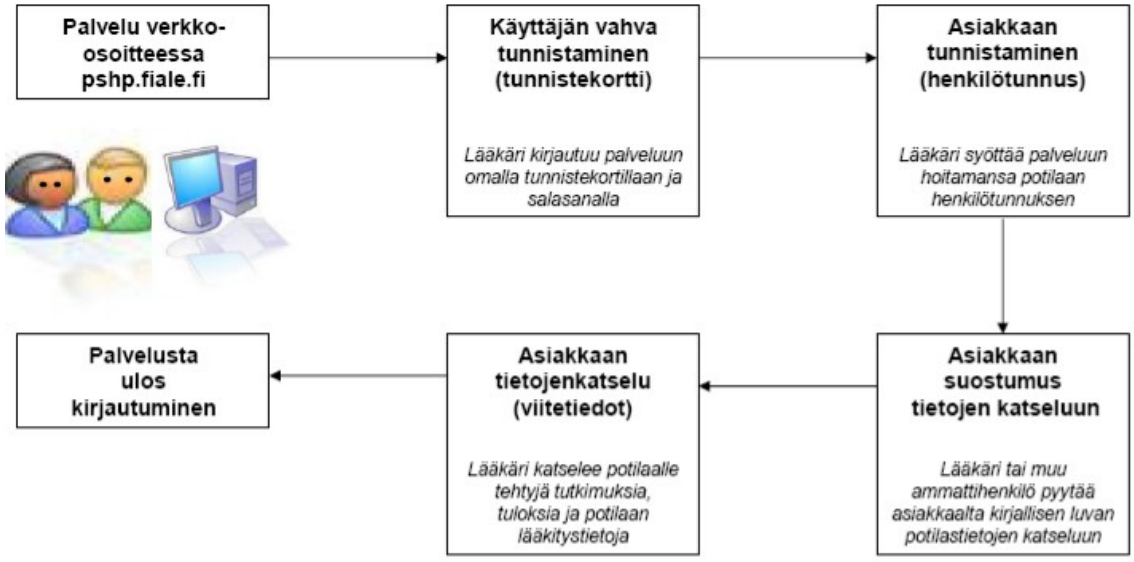
4.4. Fiale aluetietojärjestelmä

Aluetietojärjestelmä (ATJ) on alueellisesti eri sosiaali- ja terveydenhuollon organisaatioiden yhteisesti käyttämä tietojärjestelmä (kuva 14.). Aluetietojärjestelmän avulla voidaan turvata tiedon kulku nopeasti eri sosiaali- ja terveydenhuollon ammattilaisten kesken. Aluetietojärjestelmät on suunniteltu toteuttamaan saumattomia hyvinvointipalveluita. Aluetietojärjestelmällä voidaan myös suunnitella asiakkaan palveluketjuja. Pirkanmaan (PSHP) ja Satakunnan (SatSHP) sairaanhoitopiireissä on käytössä Fiale-aluetietojärjestelmä. Fiale on käytössä myös Varsinais-Suomen sairaanhoitopiirissä, joka on rajattu tämän tutkimuksen ulkopuolelle. [Lausvaara et al., 2004]



Kuva 14. Aluetietojärjestelmän toiminnallisuus. [Itälä, 2000].

Aluetietojärjestelmä toimii Internet-palveluna ja sen tulisi olla käytössä 24 tuntia päivässä ja seitsemänä päivänä viikossa. Koska ATJ toimii Internetin yli, niin tietoliikenteen pitää olla vahvasti salattua. Aluetietojärjestelmän käyttö tapahtuu selainpohjaisen käyttöliittymän avulla [YT Tieto, 2006a]. Kuvassa 15. näkyy, minkälainen prosessi asiakkaan tietojen katselu on.

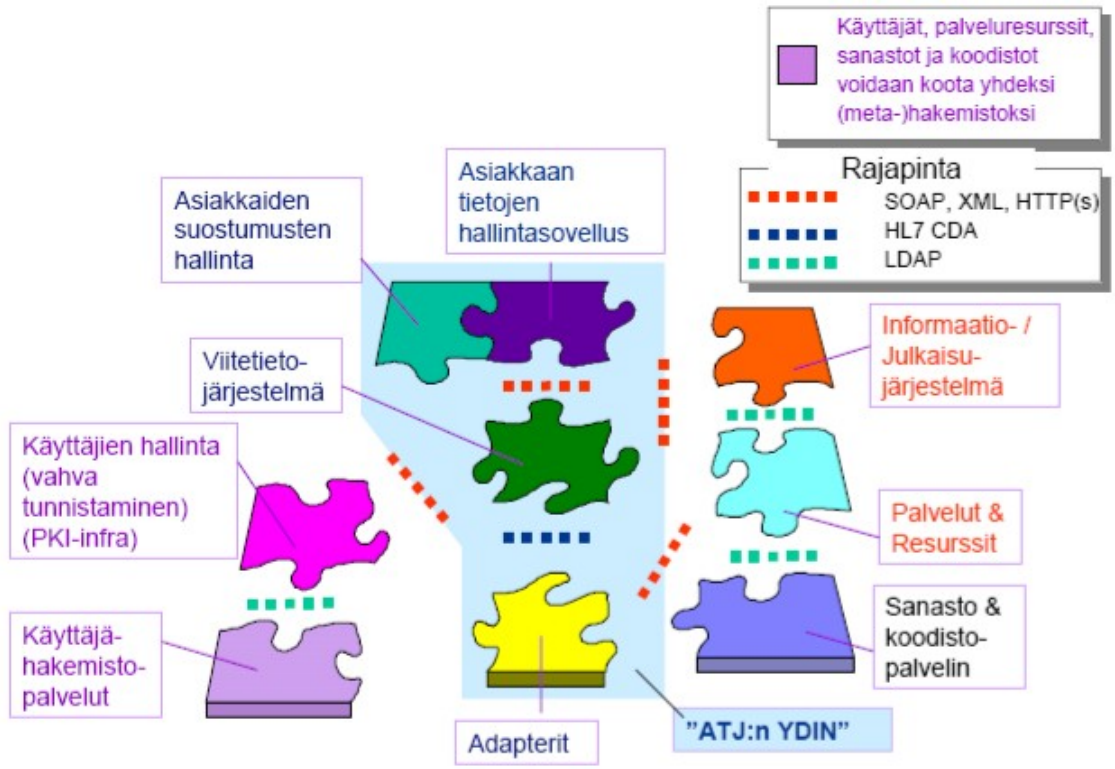


Kuva 15. Asiakastietojen katselu aluetietojärjestelmän avulla. [YT Tieto, 2006b]

Fiale-aluetietojärjestelmäpalvelu rakentuu viidestä osasta:

- viitetietojärjestelmä (viitetietokanta)
- asiakkaan tietojen hallintasovellus
- informaatiojärjestelmä
- ammattilaiskortti palveluineen ja järjestelmineen
- perusjärjestelmien adapterit, joiden avulla perusjärjestelmät kytketään aluetietojärjestelmään.[YT Tieto, 2006b]

Aluetietojärjestelmän arkkitehtuuri perustuu eri sovelluksiin ja komponentteihin, jotka yhdistetään toisiinsa avoimien rajapintojen avulla muodostaen saumattoman kokonaisuuden (kuva 16.) [Tuuri, 2003]. Fialen keskeisimmät osat ovat viitetietokanta ja viitetietojärjestelmä. Viitetietojärjestelmän avulla voidaan rakentaa alueellinen potilastietojen katselujärjestelmä. Siihen rakennetaan eri organisaatioiden potilastietojärjestelmistä liittymät, joiden avulla aluetietojärjestelmä ja potilastietojärjestelmät voivat keskustella keskenään. [YT Tieto, 2006a; YT Tieto, 2006b; Lausvaara et al., 2004]



Kuva 16. Aluetietojärjestelmän komponentit [Saranummi, 2003].

Viitteellä tarkoitetaan tietoa tiedosta, missä taustajärjestelmässä asiakkaaseen liittyvä tieto sijaitsee. Viitteet ovat teknisiä osoitteita, eli linkkejä, joiden avulla löydetään asiakkaan tiedot. Viite sisältää myös kuvauksen, mitä tietoa viite koskee [Itälä, 1999]. Kaikista perusjärjestelmien tapahtumista luodaan viite, jotta nämä tiedot ovat käytettävissä aluetietojärjestelmän kautta. Perusjärjestelmien luomat viitteet tallennetaan viitetietokantaan. Aluetietojärjestelmään ei siis tallenneta asiakkaiden tietoja, vaan se tarjoaa mahdollisuuden viitteiden avulla katsella perusjärjestelmien sisältäviä tietoja (kuva 17.).

Kuva 17. Aluetietojärjestelmä ja perusjärjestelmien suhde [Mikola, 2003, s 12].

Viitetietojärjestelmä on aluetietojärjestelmän toiminnallinen osa joka käyttää viitetietokantaa. Viitetietokanta sisältää viitteet asiakkaan tietoihin eri potilastietojärjestelmissä. Asiakkaan tietojen hallintasovellus hyödyntää viitetietojärjestelmää tietojen katselussa ja palveluketjujen suunnittelussa. Viitetietojärjestelmän avulla terveydenhuollon ammattilaiset voivat katsella asiakkaan tietoja eri potilasjärjestelmistä. Ammattilaisen valitessa viitteen, järjestelmä hakee perusjärjestelmästä kyseisen tiedoston katseltavaksi. [YT Tieto, 2006a; YT Tieto, 2006b; Lausvaara et al., 2004]

Viitetietona järjestelmään tallennetaan asiakkaan nimi, henkilötunnus, mahdolliset palveluketjutunnukset, tiedon sijaintipaikka, yleisluontoinen kuvaus viitetiedon osoittamasta tiedosta, viitetiedon tallentamisaika ja viitetietokannan toiminnan edellyttämät tekniset tiedot. Lisäksi sinne tallennetaan asiakkaan suostumukset. Aina kun Fialella katsellaan asiakkaan tietoja, kirjautuu siitä tieto seurantalokitietokantaan. Seurantalokitietokannan avulla voidaan valvoa väärinkäytöksiä, sekä turvata asiakkaan ja ammattilaisen oikeusturva. [YT Tieto, 2006a; YT Tieto, 2006b; Lausvaara et al., 2004]

Aluetietojärjestelmä ja asiakastiedon hallintasovellus ovat toisistaan erillään, omissa laiteympäristöissään. Järjestelmät keskustelevat keskenään XML-viestien välityksellä salatun yhteyden ylitse. Asiakkaan tiedon hallintasovellus saa kaiken tietonsa adapterin avulla perusjärjestelmistä ja sen avulla päästään yksittäisen potilaan tietoihin käsiksi. Asiakastiedon hallintasovellus käyttää viitetietokantaa ja sen sisältämiä viitetietoja perusjärjestelmien tietosisältöjen katseluun. Asiakastiedon hallintasovellus sisältää seuraavat tiedot:

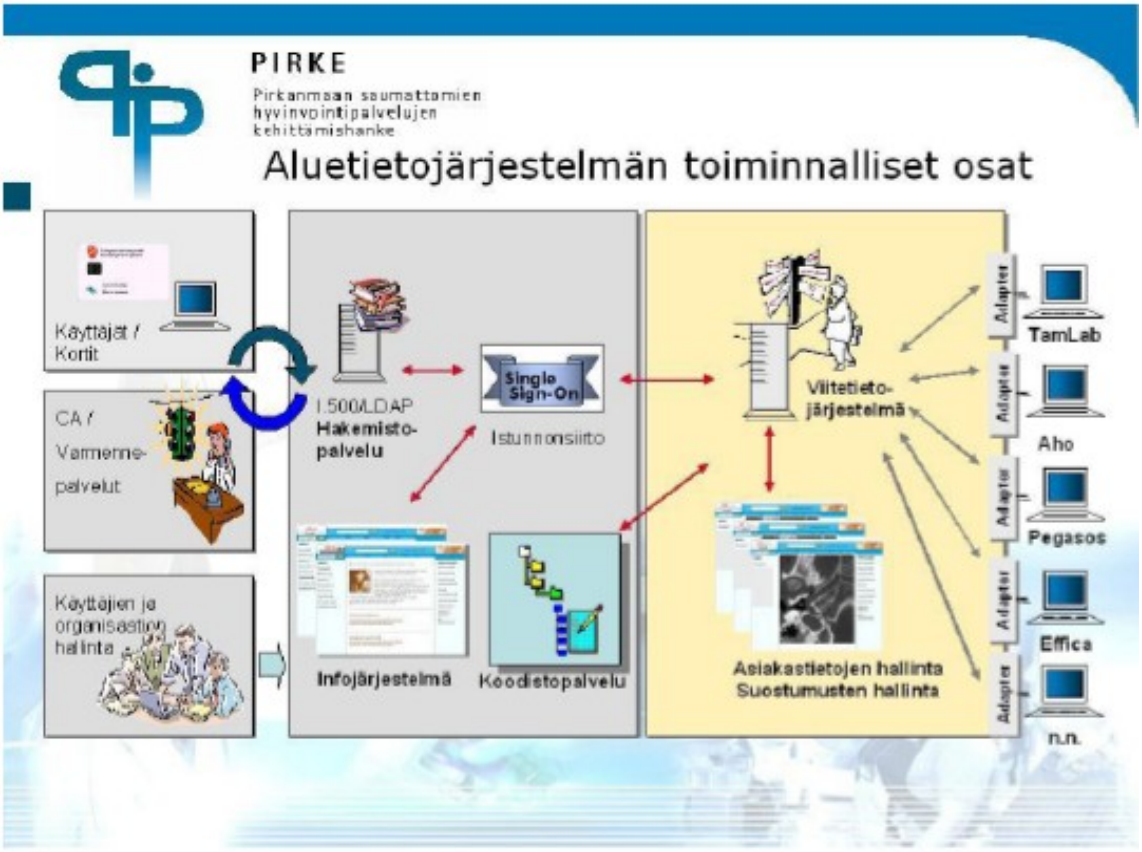
- asiakastiedot
- laillisen edustajan tiedot
- suostumukseen liittyvät tiedot (antaja, saaja, voimassaoloaika, tyyppi, yms.)
- palveluketjutiedot
- viitetiedot (yleisluontoiset kuvaukset tiedoista ja sijainnista)
- omaneuvojatiedot
- seurantalokitiedot (asiakas, käyttäjä, ajankohta, yms.) [YT Tieto, 2006a]

Asiakkaan tietojen hallintasovelluksella voidaan asiakkaalle tehdä palveluketjusuunnitelma, myös silloin kun hänen hoitonsa vaatii palveluita yli organisaatiorajojen. Palveluketjusuunnitelma helpottaa hoidon koordinointia sekä mahdollistaa hänen tietojensa katselun eri organisaatioissa yhdellä palveluketjusuostumuksella. Lisäksi asiakkaan tietojen hallintasovelluksessa ylläpidetään asiakkaiden suostumuksia sekä omaneuvojasopimuksia [Lausvaara et al., 2004; Tuuri, 2003].

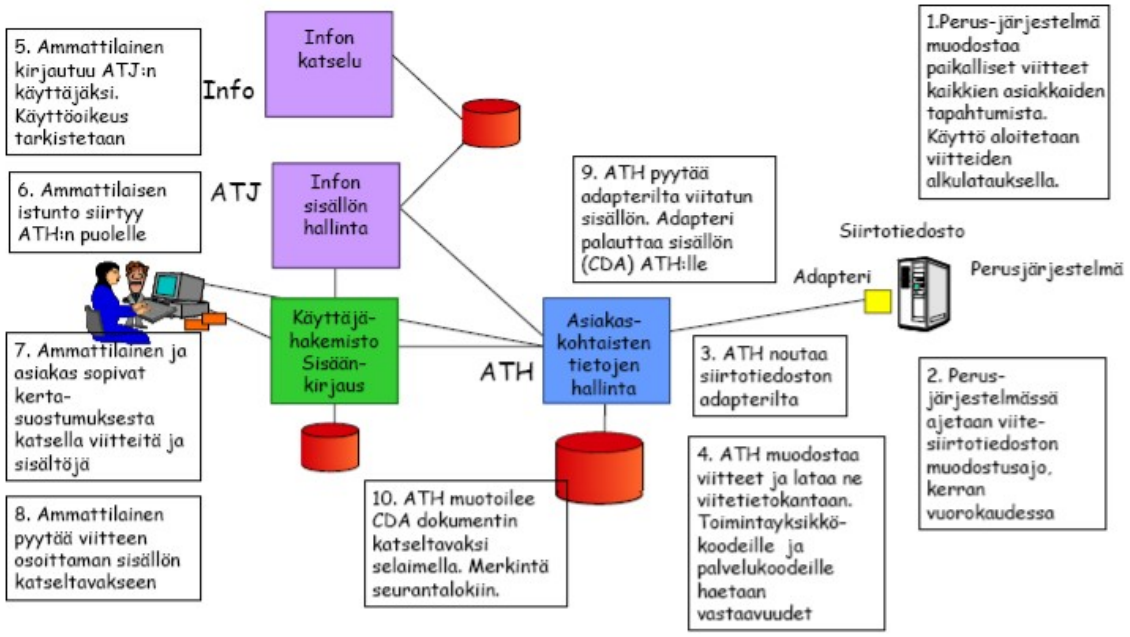
Olennainen osa aluetietojärjestelmää on myös informaatiopalvelu. Informaatiopalvelu jakaantuu kahteen osaan: ammattilaisportaaliin (extranet-ratkaisu) ja kansalaisportaaliin (avoin internetsivusto). Ammattilaisportaali on terveydenhuollon ammattilaisten tietopalvelu, jonka avulla voidaan jakaa tietoa helposti eri toimijoille. Järjestelmä vaatii tunnistautumisen. Kansalaisportaali toimii tiedotuskanavana alueen asukkaille eri palveluista ja toimijoista. [YT Tieto, 2006a]

Aluetietojärjestelmässä käyttäjien tunnistaminen hoidetaan erillisen toimikortin, eli ammattilaiskortin avulla. Ammattilaiskorttiin on tallennettu käyttäjän varmenne. Varmennepalvelun PSHP:lle ja SatSHP:lle tuottaa Varsinais-Suomen sairaanhoitopiiri. Ammattilaiskortin käyttö vaatii tietokoneeseen liitetyn kortinlukijan, joka lukee kortin. [YT Tieto, 2006a]

Perusjärjestelmät, eli aluetietojärjestelmään osallistuvien organisaatioiden potilastietojärjestelmät, liitetään aluetietojärjestelmään kansallisesti määriteltyjen liittymärajapintojen eli adapterien avulla. Adapterit noudattavat HL7 CDA R1 standardia [YT Tieto, 2006b]. Adapterien avulla voidaan siirtää viitetietoja perusjärjestelmistä viitetietokantaan, viitteen avulla voidaan myös hakea tietoa perusjärjestelmistä. Viitteessä näkyy missä tieto sijaitsee, mitä viitteen osoittama tieto sisältää, sekä milloin viitetieto on järjestelmään tallennettu [Tuuri, 2003]. Adapterien kautta liikkuva tieto on puhtaasti yksisuuntaista, mikä varmistaa, ettei perusjärjestelmien tietoja pysty muuttamaan aluetietojärjestelmästä. Aluetietojärjestelmän toiminnalliset osat ja niiden suhteet on kuvattu kuvassa 18. Näiden osien toimintaa käytännössä kuvataan kuvassa 19.



Kuva 18. Aluetietojärjestelmän toiminnalliset osat [YT Tieto, 2006a, s 21].



Kuva 19. Aluetietojärjestelmän käyttötapahtuma [STM, 2002, s 52].

4.5. Suostumukset Fialessa

Fialessa suostumukset on jaoteltu kolmeen erilaiseen suostumukseen. Nämä ovat suostumus, palveluketjusuostumus ja omaneuvojasuostumus. Asiakas antaa suostumuksella oikeuden katsella omia tietojaan määräajaksi. Suostumuksessa määritellään mihin kaikkiin tietoihin se oikeuttaa. Se voi koskea ennen suostumuksen antoa tehtyjä tietoja ja suostumuksen voimassaoloaikana luotavia tietoja. Suostumuksessa on oltava nimettynä ammattilainen, mutta sen piiriin voidaan liittää muita ammattilaisia palvelun, toimipisteen tai ammattiroolin perusteella. [YT Tieto, 2006c]

Palveluketjusuostumus on tarkoitettu tilanteisiin joissa asiakasta hoitaa useampi ammattilainen tai asiakas käyttää useaa eri palvelua. Palveluketjusuostumus annetaan aina koskemaan tiettyä rajattua palvelukokonaisuutta tiettynä ajankohtana. Suostumus annetaan koskemaan tietyn toimintayksikön ammattirooleja, kuten esim. lääkäri ja hoitaja. Kaikilla palveluketjuun osallistuvilla henkilöillä on oikeus katsoa suostumuksen antamia tietoja sen voimassaoloajan tai niin kauan kuin he osallistuvat asiakkaan palvelun tuottamiseen. [YT Tieto, 2006c; Lausvaara et al., 2004]

Palveluketjusuostumukseen voidaan myös liittää ennen palveluketjua tehtyjä viitteitä. Asiakas voi tehdä omaneuvojasopimuksen ja antaa omaneuvojasuostumuksen. Omaneuvojasuostumuksella asiakkaan omaneuvoja voi katsoa ennen suostumuksen antoa tehtyjä tietoja sekä suostumuksen aikana luotavia tietoja. Omaneuvojasuostumus on voimassa niin kauan kuin omaneuvojasopimuskin. [YT Tieto, 2006c; Lausvaara et al., 2004] Asiakkaan suostumukset tallennetaan viitetietojärjestelmään ja niitä ylläpidetään asiakkaan tietojen hallintasovelluksella. Suostumuksen pyytämisen vaiheet näkyvät kuvassa 20.

	Toiminto	Aluetietojärjestelmän palvelut	Asiakirjat
1	Asiakkaan yleinen informointi (HeTiL 24§, Kokeilulaki 811/2000) Kirjallinen informaatio	Tietopaketit	Tiedote viitteiden synnystä Tiedote henkilötietojen käsittelystä aluetietojärjestelmässä Henkilörekisteriseloste Seurantalokiseloste
2	Asiakaskohtainen informointi kirjallinen informaatio suullinen informaatio: suostumus ja sen merkitys	Tietopaketit	Tiedote henkilötietojen käsittelystä aluetietojärjestelmässä Henkilörekisteriseloste Seurantalokiseloste
3	Suostumuksen pyytäminen ja suostumuksen sisällön määrittely	Suostumusten hallinta Viitetietokanta Palveluketjutietokanta	
4	Suostumuksen tulostus ja asiakkaan allekirjoitus (vahvistus informaatiosta ja suostumus tietojen luovutukseen)		Suostumus
5	Suostumuksen arkistointi Kopio asiakkaalle	Suostumustietokanta Seurantaloki	Vahvistettu suostumus

Kuva 20. Suostumuksen pyytämisen prosessikuvaus [Lausvaara et al., 2004, s 27]

Suostumuksen tietosisältö aluetietojärjestelmässä on:

- suostumuksen antaja
- peruste, mikäli suostumuksen antaja on joku muu kuin asiakas itse
- suostumuksen saaja
- voimassaoloaika
- suostumuksen tyyppi
- mitä asiakirjoja tai tietoja suostumus koskee
- mahdollinen tietojen rajaus
- tietojen käyttötarkoitus
- asiakkaan allekirjoitus. [Lausvaara, 2004]

Seurantalokin avulla valvotaan järjestelmän ja asiakkaiden tietojen käyttöä ja luovutuksia. Fialessa asiakkaiden tietojen katsomisesta, luovuttamisesta ja käytöstä muodostuu seurantalokiin merkintä, josta selviää kenen tietoja on käsitelty, kuka tietoja on käsitellyt ja mikä hänen ammattiroolinsa on, käytön ajankohta, mitä viitetietoa on käsitelty sekä käytön peruste. Seurantalokiin on

käyttöoikeudet ainoastaan etukäteen määritellyille valvojille. Myös valvojien toimista muodostuu lokiin merkintä. Valvojan tehtävänä on valvoa järjestelmän käyttöä, sekä estää ja tutkia mahdollisia väärinkäytöksiä. Seurantalokin tavoitteena on turvata rekisteröityjä tietoja ja asiakkaan sekä ammattilaisen oikeusturvaa. Asiakkaalla on oikeus tarkistaa seurantalokista itseään koskevia tietoja. [YT Tieto, 2006c; Lausvaara et al., 2004]

5. Tulokset

5.1. Toiminnallinen taso

Tässä tutkimuksessa tarkastelen toimintaa pääsääntöisesti Pirkanmaan sairaanhoitopiirin näkökulmasta. Pyrin selvittämään, miten organisaatiossa tietosuoja ja tietoturva on hoidettu, sekä miten aluetietojärjestelmän käyttöä on ohjeistettu. Toiminnallisen tason vaatimukset kohdistuvat lähinnä ihmisten ja organisaation toimintaan ja tärkeitä ovat erityisesti toimintaan liittyvät ohjeistukset, määräykset sekä rajoitukset. Tietoturvan osalta toiminnalliselle tasolle kohdistuu eniten hallinnollinen tietoturva, jolla pyritään ohjaamaan ihmisten ja organisaation toimintaa.

5.1.1. Yleiset lainsäädännölliset vaatimukset

Fiale aluetietojärjestelmässä käsitellään potilaiden henkilötietoja, ja se rakentuu eri toimintayksiköiden potilastietojärjestelmistä, joista muodostuu sen loogisia osarekistereitä. Aluetietojärjestelmä ei varsinaisesti ole henkilörekisteri, vaan sen sisältämät asiakaskohtaiset tiedot ovat osa kunkin rekisterinpitäjän omaa henkilörekisteriä. Tästä johtuen aluetietojärjestelmää käyttävät organisaatiot vastaavat henkilötietolain vaatimuksista ja rajoituksista omien potilasrekisteriensä kohdalta.

Henkilötietolaissa [HetiL, 1999] velvoitetaan rekisterinpitäjää pitämään saatavilla vaadittavat selosteet. Pirkanmaan sairaanhoitopiirillä oli aluetietojärjestelmästä tehty asianmukaiset rekisteri- ja tietojärjestelmäselosteet sekä asiakastiedote. Nämä tiedotteet olivat nähtävillä sekä organisaation toimitiloissa että internet sivuilla. Niiden avulla varmistetaan, että rekisteröidyt ihmiset tietävät henkilötietojensa käsittelystä.

Rekisterinpitäjän tulee myös huolehtia asiakkaidensa oikeuksista. Näitä oikeuksia on pyritty täyttämään edellä mainituilla rekisteriselosteilla ja asiakastiedotteilla. Rekisteriselosteessa selvitetään selkeästi mihin tarkoitukseen ja mitä tietoja kerätään, kuka vastaa rekisteristä, yhteyshenkilö sekä muut vaadittavat asiat. Lisäksi asiakkaalla on mahdollisuus tehdä tarkastuspyyntö omien tietojensa kohdalta. Asiakkaiden oikeuksien turvaamista varten Pirkanmaan sairaanhoitopiirin potilaskertomusohjeissa on erityinen kappale asiakkaan oikeuksista, jotta terveydenhuollon ammattilaiset osaavat huolehtia näistä oikeuksista.

Rekisterinpitäjän tulee huolehtia tietojensa laadusta, virheettömyydestä sekä salassapidosta. Tähän vaatimukseen on pyritty vastaamaan toiminnallisella tasolla henkilökunnan koulutuksella ja tiedotuksella. Kaikkien aluetietojärjestelmän käyttäjien tulee käydä läpi koulutus, jonka osana on myös tietosuojakoulutus. Käyttöoikeuksia ei voi saada ennen kuin koulutus on suoritettu.

Pirkanmaan sairaanhoitopiirissä on tehty erillinen tietosuojaohje liittyen aluetietojärjestelmään, jossa käsitellään potilastietojen salassapitoa sekä erityisiä vaatimuksia tietojen käsittelylle. Lisäksi käyttäjien tulee allekirjoittaa tietosuojasitoumus. Sitoumuksessa käyttäjä sitoutuu noudattamaan salassapito- ja tietosuojaohjetta sekä vakuuttaa saaneensa asiankuuluvan koulutuksen ja selityksen tietosuojaohjeesta. Näiden keinojen avulla voidaan vaikuttaa ammattilaisten asenteisiin ja tapoihin toimia. Kuitenkin tietojen salassapidossa tärkeää on ihmisten toiminta.

Tietojen luottamuksellisuutta turvatessa ei sairaanhoitopiirissä luoteta pelkästään ihmisten moraaliin. Potilaiden tietojen katselua pystytään erilaisin teknisin välinein seuraamaan, jolloin mahdollisiin väärinkäytöstilanteisiin voidaan puuttua. Tästä valvonnasta on myös tiedotettu aluetietojärjestelmän käyttäjille, jolloin se mahdollisesti ennaltaehkäisee väärinkäytöksiä.

5.1.2. Suostumus ja potilastietojen käsittely

Henkilötietolaki [HetiL, 1999] asettaa useita vaatimuksia potilastietojen käsittelylle, joista seuraavaksi kerron, miten PSHP on näihin vaatimuksiin vastannut. Potilastietojen käsittely on oltava etukäteen suunniteltua. Etukäteissuunnittelun vaatimus on täytetty tekemällä rekisteri- ja tietojärjestelmäselosteet, joissa määritellään miten tietoja kerätään, käsitellään ja luovutetaan. Lisäksi niissä kerrotaan, mitä tietoja on tarkoitus kerätä. Tietojen käsittelyn menetelmät on määritelty useissa ohjeistuksissa, kuten esim. potilaskertomusohjeissa ja aluetietojärjestelmän käyttöohjeissa.

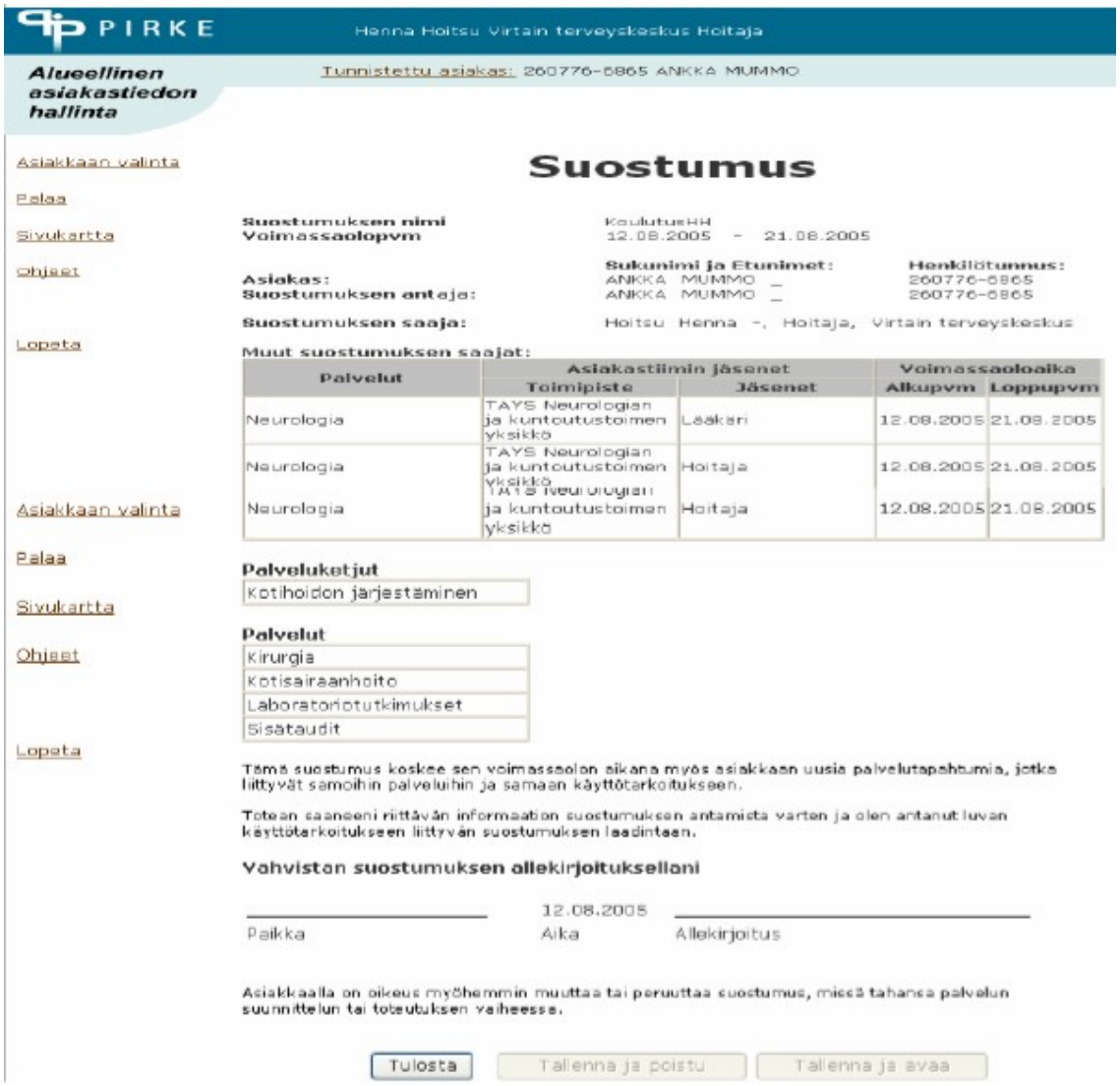
Potilastietoja käsiteltäessä tulee rekisterinpitäjän huolehtia huolellisuus- ja suojaamisvelvoitteesta. Potilastietoja suojataan erilaisin teknisin menetelmin, mutta rekisterinpitäjän on varmistuttava myös henkilökunnan toiminnan laillisuudesta. Tätä ongelmaa on ratkaistu koulutuksin ja sitoumuksilla sekä henkilökunnan käyttöoikeuksien määrittelyillä. Myös potilasasiakirja-asetuksessa [STM, 2001] erityisesti vaadittu kirjallinen ohjeistus potilasasiakirjojen käsittelystä on tehty sekä jaeltu henkilökunnalle. Pirkanmaan sairaanhoitopiirissä on aluetietojärjestelmästä tulostaminen estetty ja kielletty. Tämä on myös tiedotettu käyttäjille. Sillä pyritään estämään tietojen joutuminen vääriin käsiin tai niiden käyttö yhteyksissä jossa se ei ole sallittua.

Potilastietojen käsittelyssä tulee yhteysvelvoitteen täyttyä, eli käsittelijällä pitää olla asiallinen yhteys potilaaseen. Teknisesti tämän asiallisen yhteyden tarkistamista ei ole vielä käytännössä ratkaistu. Aluetietojärjestelmän käytössä potilas tunnistetaan henkilötunnuksella, jolloin käyttäjien on vaikeampi katsella muiden kuin omien potilaidensa tietoja. Eli aluetietojärjestelmästä ei saa minkäänlaista potilaslistaa, vaan käyttäjän on tiedettävä potilaan oikea henkilötunnus. Lisäksi yhteysvaatimusta pyritään täyttämään koulutuksella, tiedotuksella ja sitoumuksilla. Myös käytön valvonnalla on oma vaikutuksensa käyttäjien toimintaan. Näillä keinoilla pyritään myös turvaamaan tietojen käsittelyn tarpeellisuusvaatimus sekä tietojen käyttötarkoituksien

muuttumattomuus, ettei tietoja siis käytetä muihin tarkoituksiin kuin, mihin ne on alun perin kerätty.

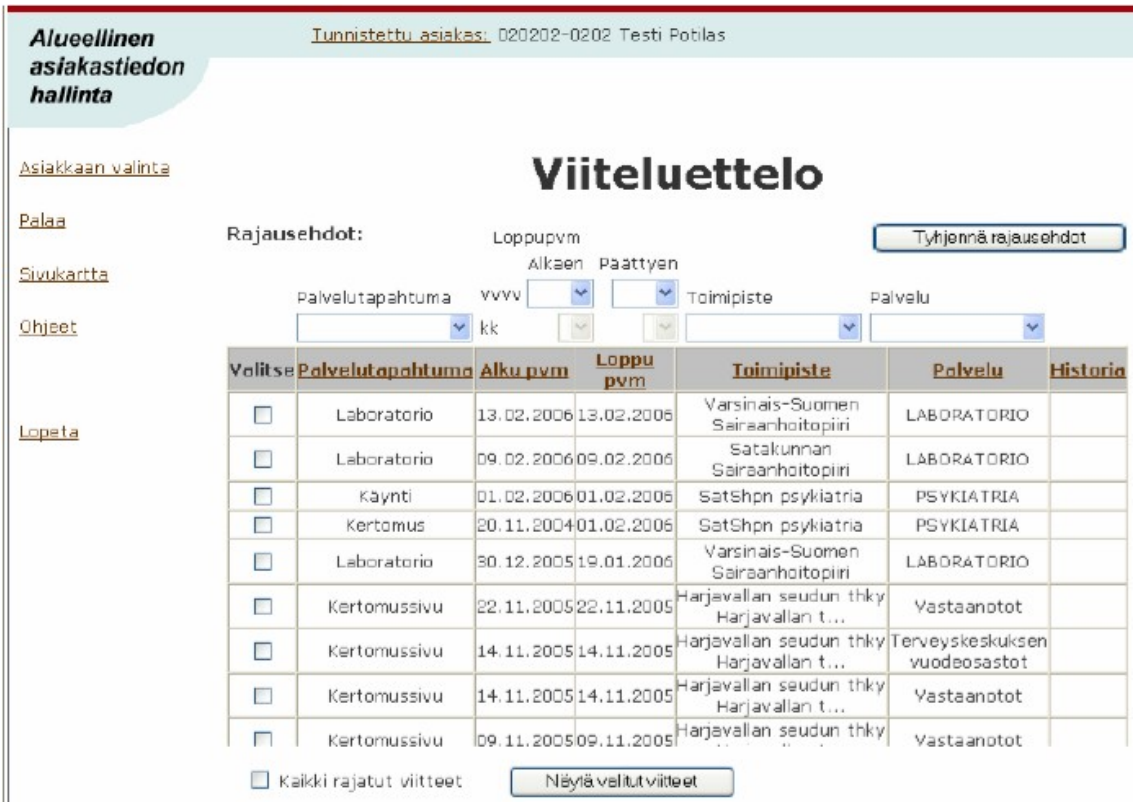
Potilaan tietoja luovutettaessa toiseen toimintayksikköön tarvitaan aina suostumus. Vaikka aluetietojärjestelmässä puhutaankin tietojen katselusta, niin siinä tapahtuu kuitenkin tietojen luovutus, joten suostumus on aina pyydettävä potilaalta. Aluetietojärjestelmässä tietojen katselu ei onnistu ilman asianmukaista suostumusta tai lakiin perustuvaa syytä. Järjestelmän käyttäjä tekee aina suostumuksen potilaan kanssa. Suostumus voi olla kirjallinen tai suullinen. Suostumuksesta kuitenkin pitää aina tehdä merkintä potilaan tietoihin. Kirjallinen suostumus tulostetaan ja potilas allekirjoittaa sen. Suostumuksesta tehdään merkintä perusjärjestelmiin. Suullisen suostumuksen vahvistaa hoitava lääkäri allekirjoituksellaan. Suostumukset ovat ainoita dokumentteja, joita aluetietojärjestelmästä arkistoidaan paperisesti.

Suostumuksen pitää olla vapaaehtoinen ja informoitu. Pirkanmaan sairaanhoitopiirissä terveydenhuollon ammattilaisia on ohjeistettu asiakkaan informoimisesta suostumusta pyydettäessä sekä kirjallisesti että suullisesti. Suostumuksessa (kuva 21.) pitää ilmetä seuraavat asiat: kenelle tiedot luovutetaan, mitä tietoa luovutetaan, miksi tietoa luovutetaan, minkälainen suostumus on kyseessä, kuinka pitkään se on voimassa ja kuka suostumuksen antaa. Asiakkaan ollessa mukana suostumusta täyttäessä voidaan suostumus helposti rajata koskemaan vain tarvittavia tietoja. Aluetietojärjestelmä pakottaa käyttäjän täyttämään kaikki vaaditut kohdat. Ilman kaikkien kohtien täyttämistä ei potilaan tietojen katselu onnistu.



Kuva 21. Aluetietojärjestelmällä luotu suostumus [YT Tieto, 2006c, s 23].

Suostumuksen luomisen jälkeen käyttäjä näkee potilaan viitelistan (kuva 22.), jonka perusteella voidaan valita mitä tietoja halutaan katsella. Viiteluettelosta käyttäjä valitsee viitteen, minkä jälkeen järjestelmä näyttää perusjärjestelmästä löytyvät tiedot. Viiteluettelossa näkyy ainoastaan ne viitteet, jotka suostumuksessa on valittu.



Kuva 22. Viiteluettelosta nähdään mitä tietoja asiakkaasta on perusjärjestelmissä [YT Tieto, 2006c, s 25].

Tietoja katsellessa jää tapahtumasta merkintä lokiin. Tällä pyritään täyttämään potilasasiakirja-asetuksen vaatimus siitä, että tietojen luovutuksesta pitää jäädä merkintä tiedon luovuttajan järjestelmään. Tietoja luovutettaessa luovuttajan tulee varmistua siitä, että tiedot ovat virheettömiä eivätkä ne joudu sivullisten käsiin. Luovutuksen saajan velvollisuus on varmistua tietojen alkuperästä ja muuttumattomuudesta. Nämä velvollisuudet on pyritty täyttämään, kun organisaatiot ovat liittyneet aluetietojärjestelmän käyttäjiksi. Liityttäessä varmistutaan sopimuksin ja katselmoinnein näiden ehtojen täyttymisistä. Myös sähköisen luovutuksen vaatimus riittävästä salauksesta on huomioitu järjestelmää rakennettaessa.

Erikoissairaanhoitolain perusteella tietoja on mahdollista luovuttaa ilman potilaan suostumusta, mikäli luovutusperuste perustuu lainsäädännössä esiintyvään pykälään. Jos esimerkiksi potilas on estynyt antamaan

suostumuksen, pystyy järjestelmän käyttäjä kuitenkin katsomaan potilaan tietoja. Tällöin järjestelmästä valitaan, ettei suostumusta voida saada ja kirjoitetaan peruste, miksi tietoja pitää katsoa ilman potilaan suostumusta. Näistä tapahtumista jää lokiin merkintä ja niitä tarkastellaan jälkikäteen, että onko tietojen katselu tapahtunut lain mukaisesti.

Potilasasiakirja-asetuksen mukaisesti Pirkanmaan sairaanhoitopiirissä on tehty asianmukaiset ohjeet tietojen luovutusta varten. Näissä ohjeissa kerrotaan millä edellytyksillä tietoja saadaan luovuttaa ja kenelle. Ohjeissa on myös määritelty mitä poikkeustilanteissa tulee huomioida ja milloin saadaan luovuttaa tietoja ilman suostumusta.

5.1.3. Yleinen tietoturva

Aluetietojärjestelmässä tieto liikkuu sähköisesti toimintayksiköstä toiseen internetin välityksellä. Tämä aiheuttaa suuria haasteita tietoturvalle. Tietoturvan pitää olla kunnossa sekä itse aluetietojärjestelmän osalta että myös aluetietojärjestelmään liittyvien organisaatioiden osalta. Tietoturvaa ei tässä yhteydessä voida ratkaista pelkästään teknisin keinoin vaan myös muut tietoturvallisuuden alueet tulee huomioida.

Henkilötietolaissa asetetaan vaatimuksia tietojen luovuttajalle ja luovutuksen saajalle. Vaatimuksissa määritellään, että luovuttajan tulee vastata tietojen virheettömyydestä ja salassa pidettävyydestä siirron aikana. Vastaanottajan tulee varmistua tietojen alkuperäisyydestä ja muuttumattomuudesta. Aluetietojärjestelmää käytettäessä luovutuksen edellytysten täyttyminen on pyritty turvaamaan sopimuksin ja katselmoinneilla. Sopimuksissa määritellään eri osapuolten vastuut liittyen aluetietojärjestelmään ja sen käyttöön sekä vaadittavat tietoturvatasot. Sopimuksessa osapuolet sitoutuvat täyttämään tietyt kriteerit ja velvoitteet, mm. liittyen tietosuojaan. Sopimus noudattaa sosiaali- ja terveysministeriön mallisopimusta tietojenkäsittelyn ulkoistamisesta.

Sopimukset tehdään kolmen osapuolen kesken. Osapuolia ovat palvelun toimittaja, sairaanhoitopiiri ja palveluun liittyvä toimintayksikkö. Sopimuksissa määritellään, mistä kukin osapuoli vastaa. Palvelun toimittaja vastaa aluetietojärjestelmällä siirrettävien tietojen muuttumattomuudesta sekä palvelussa olevien tietojen turvallisuudesta. Toimittaja vastaa varsinaisen aluetietojärjestelmän toimivuudesta ja tietojen teknisestä salassa pidosta. Toimittajan vastuulla on siis, järjestelmässä liikkuvien asiakastietojen säilyminen virheettöminä ja eheinä. Toimittajalle on myös toimeksiannettu aluetietojärjestelmään liittyvien sähköisten asiakirjojen asianmukainen arkistointi, säilytys ja hävittäminen. Jotta palveluun liittyvät toimintayksiköt voivat luottaa aluetietojärjestelmään ja palvelun tarjoajaan, on heillä ollut oikeus suorittaa tietoturvatarkastus.

Sairaanhoitopiirin tai rekisterinpitäjän vastuulla on tehdä perusjärjestelmäadapterit, joiden on tarkoitus mahdollistaa tiedon siirto perusjärjestelmistä aluetietojärjestelmään. Perusjärjestelmäadapterit testataan tietoturvan ja toimivuuden osalta huolellisesti ennen aluetietojärjestelmään liittämistä. Hyväksymistestien tavoitteena on varmistaa adapterin toimivuus, tietosisältöjen oikeellisuus ja tavoitteiden mukainen toiminta. Lisäksi varmistetaan, että aluetietojärjestelmän ja adapterin välinen rajapinta toimii asiallisesti ja standardinmukaisesti sekä sen soveltuvuus viitteiden osoittaman sisällön kyselyyn.

Hyväksymistesteissä testataan myös adapterin tietoturvallisuus. Siinä varmistetaan tietoliikenteen turvallisuus, tietojen muuttumattomuus, osapuolten tunnistus, käyttöoikeudet sekä potilasturvallisuus. Tavoitteena on, että järjestelmä estää asiattoman käytön ja kerää lokin yrityksistä. Lisäksi järjestelmän tulee seurata tehtyjä toimintoja ja mahdollistaa niiden valvomisen. Testauksessa varmistetaan myös, että virhetilanteet eivät hankaloita tai vaikuta järjestelmän käyttöön.

Hyväksymistestien jälkeen suoritetaan perusteellinen katselmointi, joka perustuu testien tuloksiin. Adapterien täytyy täyttää määrätyt kriteerit, jotta niiden tietoturvallisuuteen voidaan luottaa. Katselmoinnissa läpikäydään perusteellisesti tietoturvallisuuteen liittyvät näkökulmat. Katselmoinnissa tarkastellaan adapterin perusratkaisuja, jossa arvioidaan ylätason kuvausta adapterista sekä mitkä osat toimivat internetissä ja mitkä intranetissä. Katselmoinnissa arvioidaan myös palvelinratkaisuja, eli miten palvelinkokonaisuus on luotu ja miten tietoliikenneyhteydet on ratkaistu. Katselmoinnissa käsitellään myös, miten sanomaliikenne on ratkaistu ja onko siinä huomioitu usean rinnakkaisen ympäristön hallinta. Lisäksi katselmoinnissa varmistetaan, että perusjärjestelmään toteutettu rajapinta on riittävän tietoturvallinen ja että adapterista on tehty vaadittavat dokumentoinnit. Mikäli katselmoinnissa todetaan, että adapteri ei täytä vaadittavia kriteereitä, niin puutteista laaditaan korjauslista ja korjaukset varmistetaan ennen aluetietojärjestelmään liittämistä.

Perusjärjestelmää liitettäessä aluetietojärjestelmään, pitää liittyvän organisaation määritellä seuraavat vastuuhenkilöt: perusjärjestelmän yhteyshenkilö, hyväksymistestauksesta vastaava ja käyttöpalveluvastaava. Nämä henkilöt vastaavat, siitä että aluetietojärjestelmä on tietoturvallinen liittyjä organisaation osalta.

Aluetietojärjestelmän käyttäjäorganisaatiot vastaavat oman potilasrekisterinsä tietosuojasta ja tietoturvasta. Koska rekisterinpitäjyys säilyy käyttäjäorganisaatioissa, heidän tulee huolehtia henkilötietolain ja muun lainsäädännön asettamista vaatimuksista ja rajoituksista. Palvelua käyttävä toimintayksikkö vastaa siis, että tietoja pystyvät käyttämään vain niihin oikeutetut ja ettei tietojen käyttötarkoitukset muutu. Lisäksi he vastaavat, että aluetietojärjestelmälle tarjottavat tiedot ovat oikeita ja muuttumattomia adapteriin saakka. Toimintayksikkö vastaa myös käytön seurannasta ja valvonnasta. Aluetietojärjestelmän toimittajalla on oikeus tutustua toimintayksikön tietoturvaan liittyviin asioihin ja varmistua niiden toimivuudesta.

Pirkanmaan sairaanhoitopiirissä tietohallinnon johtoryhmä tekee tietoturvaan liittyen yleiset linjaukset. Johtoryhmä on määritellyt tietohallintostrategian vuoteen 2008 saakka. Strategiassa tietoturvalla on suuri merkitys. Kokonaisvaltainen tietoturva on nostettu yhdeksi tärkeimmistä päämääristä. Strategia on myös käsitelty sairaanhoitopiirin johtoryhmässä, joten sillä on johdon tuki, mikä on edellytys sen toteutumiselle. Strategian tarkoituksena on ohjata organisaatiota kohti turvallisempaa tulevaisuutta. Siinä on huomioitu terveydenhuollon palveluntarjonnan muutokset ja toiminnan sähköistyminen sekä tietojärjestelmien merkityksen kasvu.

Strategiassa painotetaan järjestelmien yhteistoiminnallisuutta ja alueellista yhteistyötä. Tietojärjestelmäliitokset tulisi tehdä valtakunnallisesti hyväksytyillä avoimilla rajapinnoilla. Strategiassa myös pidetään tärkeänä, että tietoturvallisuus ja tietosuoja on varmistettu koko prosessissa. Tavoitteeksi on listattu myös tietoturvapolitiikan luominen, jossa asetettaisiin tietoturvallisuuden ja tietosuojan periaatteet.

Pirkanmaan sairaanhoitopiirissä jokaisen tietojärjestelmien käyttäjän pitää tutustua organisaation tietoturvallisuusohjeisiin. Lisäksi käyttäjien on allekirjoitettava salassapito- ja käyttäjäsitoumus, jossa lupaudutaan noudattamaan tietoturvaohjeita. Tämä sitoumus allekirjoitetaan viimeistään, kun käyttäjälle luovutetaan käyttäjätunnukset. Ohjeissa käsitellään yleisiä tietoturvallisuutta parantavia keinoja, kuten käyttäjätunnuksen henkilökohtaisuutta ja työasemien suojaamista sivullisilta.

5.2. Tietojärjestelmätaso

Tietojärjestelmätasolla selvitän, miten aluetietojärjestelmä on teknisesti suunniteltu sekä miten tietoturvallisuus pyritään takaamaan. Tavoitteena on selvittää miten järjestelmässä on vastattu lainsäädännön asettamiin vaatimuksiin tietoturvasta. Tutkimuksessa ei siis varsinaisesti analysoida

teknisten keinojen tietoturvallisuutta, vaan lähinnä minkälaisilla keinoilla ja toimenpiteillä lainsäädännön vaatimuksiin ja rajoituksiin pyritään vastaamaan.

5.2.1. Ohjelmistoturvallisuus

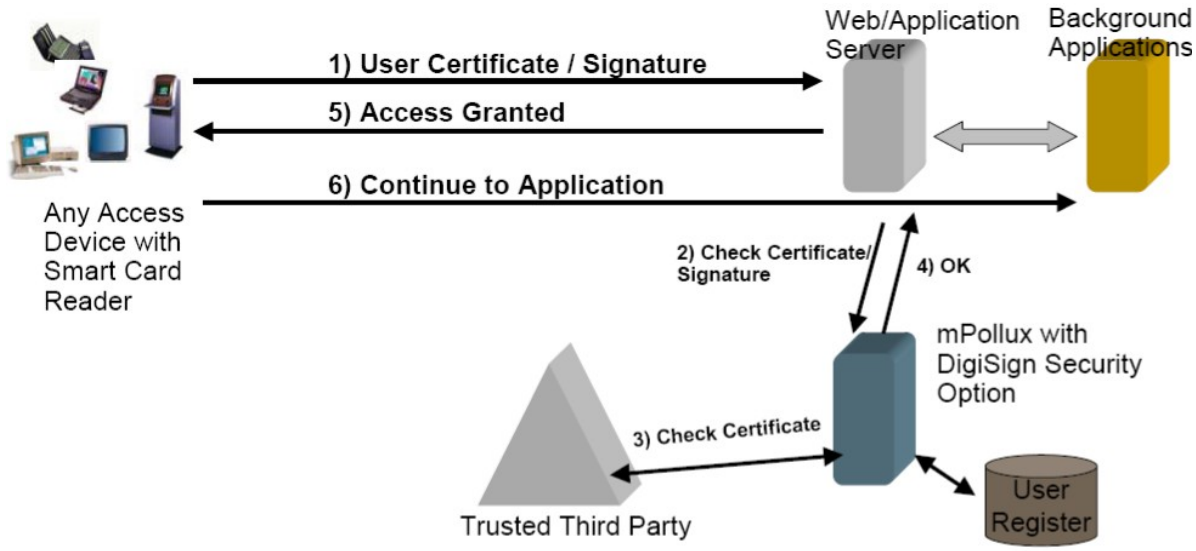
Aluetietojärjestelmässä on keskitetty käyttäjänhallinta, josta vastaa järjestelmän toimittaja. Aluetietojärjestelmän käyttöönottoa varten jokainen siihen liittyvä organisaatio on määritellyt aluetietojärjestelmässä käytettävän organisaatiohierarkian. Myös järjestelmässä käytettävät toimipisteet ja koodistot on määritelty. Hakemistoissa ja koodistoissa käytetään valtakunnallisten suositusten mukaisesti OID-koodeja, jotka on muodostettu Stakesin suositusten mukaisesti.

Koodistojen avulla turvataan järjestelmien välisten keskustelujen osalta, että molemmat osapuolet tarkoittavat samaa asiaa. Käytön aikana on kerätty kokemuksia hakemistojen ja koodistojen hallinnasta ja käytöstä, jotta niiden toimivuutta on voitu kehittää. Koodistoilla on määritelty organisaatiotiedot ja rakenteet, palvelut, käyttäjäroolit sekä muita adapterien tarvitsemia koodistoja.

Aluetietojärjestelmään kirjaudutaan ammattilaiskortilla ja PIN-koodilla. Järjestelmään ei siis pääse käyttäjätunnus – salasana yhdistelmällä. Tämä johtuu siitä, että laki saumattoman palveluketjun kokeilusta asettaa vaatimuksen vahvasta tunnistautumisesta ja ammattilaiskortilla sen toteutuminen voidaan turvata. Ammattilaiskortti on toteutettu samanlaisella tekniikalla kuin väestörekisterikeskuksen sähköinen henkilökortti (HST-kortti).

Ammattilaiskortille on tallennettu varmenteet, joiden avulla käyttäjän tunnistaminen tapahtuu luotettavasti ja turvallisesti. Sopimus varmennepalvelun tuottamisesta on tehty Varsinais-Suomen sairaanhoitopiirin kanssa. Varsinais-Suomen sairaanhoitopiiri toimii luotettavana kolmantena osapuolena, joka takaa aluetietojärjestelmässä ja korteissa olevat varmenteet. Autentikointi hoidetaan mPollux DigiSign – palvelulla (kuva 22.). Tämä

palvelu tarkistaa käyttäjän varmenteen oikeellisuuden luotetulta kolmannelta osapuolelta (Varsinais-Suomen sairaanhoitopiiri) ja myös varmistaa käyttäjän oikeudet käyttäjätunnushakemistosta, ennen kuin käyttäjä pääsee käyttämään varsinaista järjestelmää. Kun käyttäjä voidaan luotettavasti tunnistaa, on mahdollista myös luotettavasti todentaa käyttäjän oikeudet käyttää toimintaympäristössään olevia sovelluksia.



Kuva 22. mPollux DigiSignin toimintaperiaate [Fujitsu, 2005, s 7].

Ammattilaiskorttien luotettavuuden takaamiseksi niiden luovutusprosessi on määritelty ja dokumentoitu. Saadakseen ammattilaiskortin ja oikeudet aluetietojärjestelmään, käyttäjän pitää toimittaa kirjallinen, esimiehensä allekirjoittama käyttölupahakemus. Hakemuksen yhteydessä käyttäjän tulee allekirjoittaa kortinluovutussopimus. Siinä on määritelty käyttäjälle kortin tuomat velvoitteet ja rajoitteet, joiden avulla käyttäjät sitoutetaan pitämään kortti henkilökohtaisena ja noudattamaan tietoturvallisia menettelytapoja. Käyttäjiä opastetaan myös, miten pitää toimia, mikäli kortti katoaa tai hajoaa. Allekirjoittamalla sitoumuksen käyttäjä vastaa kaikesta, mitä kortin avulla aluetietojärjestelmässä tehdään.

Käyttöoikeuksien laajuus määräytyy käyttäjän työtehtävien mukaan. Lisäksi käyttäjän toimipaikka vaikuttaa oikeuksien laajuuteen. Oikeuksien määrittämisessä käytetään hyödyksi toimintayksikön tekemää aluetietojärjestelmään liittyvää organisaatiohierarkiaa. Käyttöoikeuksiin yhdistetään kortin geneerinen tunnus. Alueellinen tai organisaation pääkäyttäjä luo käyttäjälle käyttöoikeudet ja myös vastaa käyttöoikeuksien oikeellisuudesta. Pääkäyttäjille on käyttöoikeusprosessi selvitetty, jotta voidaan taata prosessin toimivuus ja turvallisuus. Kortin ja PIN-koodin jakeluprosessi tapahtuu tietoturvallisesti joko henkilökohtaisesti tai kortti ja koodi erikseen toimitettuina.

Pitkään käyttämättä olevia kortteja ei poisteta automaattisesti. Kortit asetetaan sulkulistalle vasta käyttäjän oikeuksien loppuessa. Oikeuksia myönnetään työsopimuksen pituuden mukaan tai maksimissaan viideksi vuodeksi. Organisaation pääkäyttäjä huolehtii korttien asettamisesta sulkulistalle. Lisäksi korttien hävittäminen hoidetaan asianmukaisella prosessilla.

Käyttäjän kirjautuessa aluetietojärjestelmään hänen täytyy tunnistautua toimikorttinsa ja PIN-koodinsa avulla. Kirjautumisikkuna on pyritty pitämään mahdollisimman pelkistettynä, jottei liikaa informaatiota päädy mahdollisille väärinkäyttäjille. Käyttäjien kirjautumisyritykset on rajoitettu kolmeen, minkä jälkeen kortti lukkiutuu. Lukkiutuneen kortin voi avata ainoastaan ATK-yhdyshenkilö ja sen avaamiseen tarvitaan PUK-koodi. Mikäli käyttäjän yhteys katkeaa kesken kirjautumisprosessin, niin järjestelmä katkaisee automaattisesti prosessin.

Kirjautuessaan aluetietojärjestelmään käyttäjä valitsee roolin itselleen, mikäli hän toimii useammassa eri roolissa. Käyttäjän kirjautuessa järjestelmään syntyy istunto, jonka avulla ylläpidetään yhteyttä käyttäjän ja järjestelmän välillä. Käyttäjän siirtyessä sovelluksesta toiseen aluetietojärjestelmän sisällä, niin istunnonsiirrolla varmistetaan, että käyttäjä kirjautuu järjestelmään sisään vain kerran. Istunnonsiirrossa välitetään välttämättömät käyttäjätiedot kuten

organisaatio, käyttäjärooli ja tunnuksen geneerinen-ID. Kirjautumistiedot siirtyvät aina salattuina.

Käyttäjän kirjautuessa aluetietojärjestelmään näytölle ilmestyy ikkuna, jossa kerrotaan edellisistä kirjautumisista. Siinä myös ilmoitetaan, mikäli käyttäjä on tehnyt epäonnistuneita kirjautumisia ja ohjeistetaan ottamaan epäselvissä tilanteissa yhteyttä käyttötukeen.

5.2.2. Tietoliikenneturvallisuus

Aluetietojärjestelmässä tietoliikenneturvallisuus on merkittävässä asemassa, koska järjestelmä toimii avoimen internetin yli. Tämä asettaa suuria vaatimuksia tietojen salaukselle, palomuureille ja tiedonsiirrolle. Tietojen siirto pitääkin olla suojattua adapterista aluetietojärjestelmään. Aluetietojärjestelmässä on turvallisuutta takaamaan luotu PKI-arkkitehtuuri. Käyttäjälle PKI-arkkitehtuuri näkyy oikeastaan vain toimikorttina, jolla kirjaudutaan sisälle palveluun.

Aluetietojärjestelmässä tiedonsiirtoon käytetään http-protokollaa. Kaikki liikenne on suojattu SSL-salauksella (Secure Socket Layer). HL7 Finland [2004] on listannut SSL-salaukselle kolme tehtävää

”1) Varmistaa, että yhteys on suojattu. Alustavassa kättelyssä muodostetaan salainen sessiokohtainen avain symmetrisellä salauksella (RC4, DES..)

2) Varmistaa yhteyden osapuolen identiteetti. Siihen voidaan käyttää asymmetrista- tai julkiseen avaimeen perustuvaa salausta (RSA, DSS)

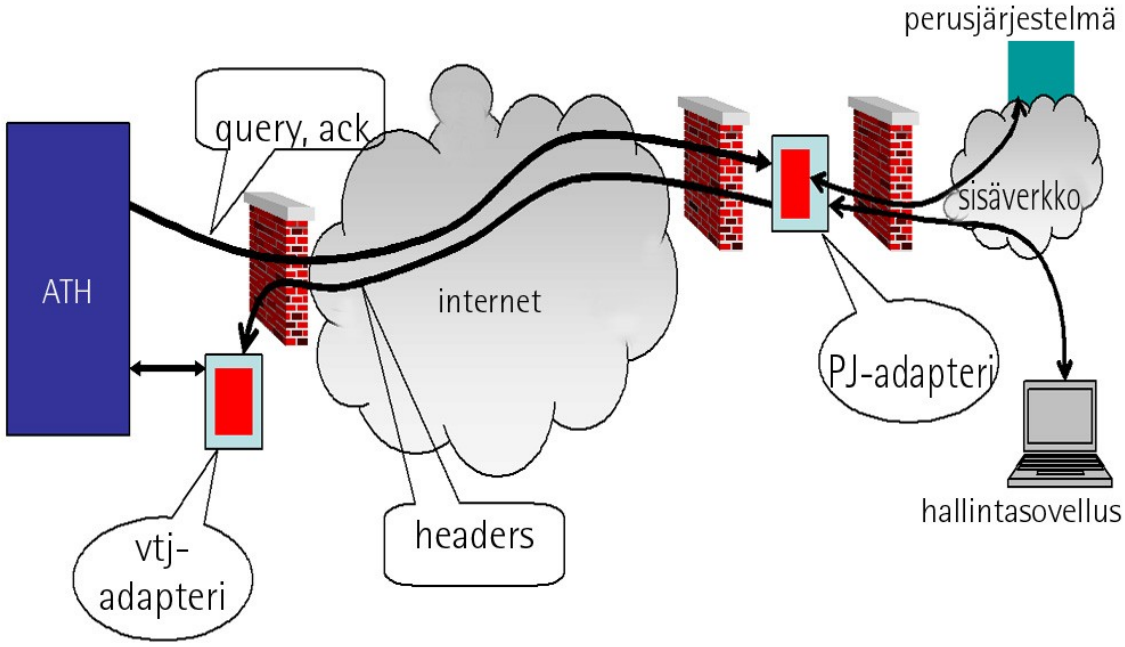
3) Yhteys on luotettava. Sanomaeheyden tarkistamiseen käytetään SHA ja MD5 algoritmeja MAC-tarkistuksen laskemiseen. ”

Järjestelmän eri osien välisessä keskustelussa osapuolien aitous ja oikeellisuus varmistetaan palvelinvarmenteilla ja varmennepolitiikoilla. Järjestelmässä liikkuvat tiedot allekirjoitetaan sähköisesti palvelinvarmenteilla. Palvelinvarmenteiden avulla voidaan luoda kaksisuuntainen SSL-yhteys, jonka

avulla turvataan adapterin ja aluetietojärjestelmän välinen tiedonsiirto. Varmenteiden avulla järjestelmän osat voivat vakuuttua palvelimien ja muiden osapuolien oikeellisuudesta. Kaikki järjestelmässä liikkuva tieto on siis salattua. Myös tietokannoista löytyvät tiedot on kryptattu, jolloin niitä ei voi katsella ilman asianmukaisia välineitä.

Asiakastietojen hallinta sovellus saa kaiken potilastiedon (CDA-dokumentit) perusjärjestelmiltä adapterin avulla. Tiedon tuottajien on siis noudatettava ennalta sovittua standardia (CDA1), jotta voidaan varmistua, että tiedot liikkuvat oikein ja kaikki osapuolet ymmärtävät ne samalla lailla. Aluetietojärjestelmä ja perusjärjestelmät (tai perusjärjestelmän adapteripalvelu) varmistuvat keskustelevansa laillisen osapuolen kanssa kaksivaiheisen ”SSL-kättelyn” avulla. Kaikki pyynnöt lähetetään SSL-salattuina niin, että SSL-yhteyden muodostamiseen vaaditaan molempien osapuolien varmenteet. Osapuolet pyytävät ja tunnistavat vastapuolen sertifikaatin.

Tietoturvallisuuden kannalta olennaisessa osassa on perusjärjestelmäadapterit. Ne sijaitsevat ns. DMZ-vyöhykkeellä (Demilitarized Zone). DMZ-vyöhykkeellä tarkoitetaan tilannetta, kun adapteripalvelimet on rajattu palomuurein, sekä aluetietojärjestelmästä että perusjärjestelmistä. Tällöin palvelin on suojattu palomuurein internetistä ja sisäverkosta katsottuna (kuva 23.). Palomuurien avulla varmistetaan, että internetistä on mahdollista käyttää ainoastaan suojattua http-yhteyttä. Lisäksi palomuurin tarkoitus on estää suora pääsy sisäverkon palvelimille. Palomuurien avulla voidaan myös rajoittaa mistä ip-osoitteista päästään käsiksi adaptereihin, jolloin adapteri voi varmistua, että yhteyttä yrittää todellakin aluetietojärjestelmä.



Kuva 23. Perusjärjestelmäadapterit sijaitsevat DMZ-vyöhykkeellä [HL7 Finland, 2004, s 4]

Potilastiedot ovat arkaluonteisia ja salassa pidettäviä, tästä johtuen aluetietojärjestelmässä on tietoturvaan kiinnitetty erityistä huomiota. Kaikki järjestelmän osat katselmoidaan ja kuvataan. Tarkan katselmoinnin avulla voidaan varmistaa, että kaikki järjestelmän osat ovat tietoturvallisia. Tietoturvallisuuden tarkka suunnittelu tulee esille laitteiden, palomuurien ja niiden sijoittelun, tietoliikenteen suojaamisessa, pääsynvalvonnassa, ohjelmien laittoman käytön estämisessä, tietojen kryptaamisessa sekä lokitiedoissa tietojen käytöstä.

5.2.3. Lokit ja valvonta

Laki saumattoman palveluketjun kokeilusta edellyttää, että aluetietojärjestelmässä seurataan kaikkia tietojen luovutuksia. Aluetietojärjestelmässä on käytössä seurantaloki, jonka avulla pystytään

valvomaan järjestelmän käyttöä. Seurantalokiin tallentuu käytännössä kaikki mitä järjestelmässä käyttäjien toimesta tapahtuu.

Asiakastietojen katselusta seurantalokiin tallentuu kuka tietoja on katsellut. Katselijasta tallennetaan nimi, henkilötunnus, ammattirooli ja toimipiste. Näiden tietojen avulla pystytään yksilöimään kuka on katsellut asiakkaan tietoja. Katselluista tiedoista samaan lokimerkintään tallennetaan myös asiakkaan yksilöivät tiedot, eli nimi ja henkilötunnus. Lisäksi seurantalokiin tallentuu asiakastiedon käytön ja katselun ajankohta, sisältö sekä millä perusteella tietoja on katseltu, eli käytännössä asiakkaan suostumus. Aluetietojärjestelmän osalta seurataan ja raportoidaan aktiivisesti myös käyttäjärekisteriä sekä ylläpito-oikeuksia.

Asiakkaalla on oikeus tarkistaa aluetietojärjestelmästä omien tietojensa käyttöä. Asiakas voi tehdä tarkastuspyynnön kirjallisesti, minkä jälkeen hänelle selvitetään kuka hänen tietojaan on käyttänyt, kenelle niitä on luovutettu sekä millä perusteella tietoja on käytetty tai luovutettu. Nämä tiedot saadaan seurantalokista. Seurantalokin avulla voidaan katsella sekä yksittäisen asiakkaan tietojen käyttöä että järjestelmän käyttäjän tekemiä toimia.

Jokaisen aluetietojärjestelmään kuuluvan organisaation tulee nimetä valvoja, jonka tehtäviin kuuluu valvoa järjestelmän käyttöä ja asiakkaiden tietojen katselua sekä seurata tietoturvan toteutumista. Valvoja ei varsinaisesti ole vastuussa seurantalokista, vaan siitä vastaa esimerkiksi Pirkanmaan sairaanhoitopiirissä johtava ylilääkäri. Valvojan tulee seurata järjestelmän käyttöä, mutta väärinkäytöstilanteessa hän ei itse saa katsella potilaan tietoja vaan tällöin hoitava lääkäri suorittaa viitetietojen tarkastamisen. Valvontatoimille tulee olla syy, ja näistä valvontatoimista jää myös lokeihin merkintä. Valvojan tehtäviin kuuluu myös tarvittavien jatkotoimenpiteiden käynnistäminen väärinkäytöstilanteissa.

Mikäli aluetietojärjestelmän käytössä ilmenee väärinkäytöksiä, niin siitä seuraa kyseisen organisaation tietosuoja- ja tietoturvaohjeissa mainittuja

kurinpitotoimia. Nämä kurinpitotoimet voivat johtaa jopa työsuhteen katkeamiseen ja rikoslain mukaisiin rangaistuksiin. Kurinpitotoimista on tiedotettu käyttäjille mm. erilaisissa sitoumuksissa mitä käyttäjät allekirjoittavat.

5.3. Tulosten analysointi

Henkilötietolaissa on esitetty rekisterinpitäjälle useita vaatimuksia, kuten aiemmin tutkimuksessa on esitelty. Pirkanmaan sairaanhoitopiirissä nämä vaatimukset rekisterinpitäjän velvollisuuksista on huomioitu varsin hyvin. Asiakkaille on tiedotettu henkilötietojen käsittelystä sekä vaadittavat selosteet liittyen aluetietojärjestelmään on tehty ja asetettu potilaiden nähtäviksi. Lisäksi henkilökunta on ohjeistettu merkitsemään potilaan tietoihin tapahtuneesta informoinnista. Selosteista on selvinnyt riittävän selkeästi mitä ja miksi tietoja käsitellään, mihin tietoja voidaan luovuttaa ja millä ehdoilla sekä miten rekisterin suojauksesta huolehditaan. Lisäksi organisaatiossa on huolehdittu rekisteröityjen tarkastusoikeudesta sekä henkilökunnan koulutuksella että tarkastuspyyntölomakkeiden avulla. Lainsäädännön asettamiin rekisterinpitäjän velvollisuuksiin potilaiden informoinnista on Pirkanmaan sairaanhoitopiirissä vastattu onnistuneesti, kuten erilaisista selosteista ja ohjeista voidaan huomata.

Henkilötietolain periaatteista esiin nousseet vaatimukset terveydenhuollon tietojenkäsittelylle olivat:

- etukäteissuunnittelun vaatimus
- huolellisuus- ja suojaamisvelvoite
- virheettömyys-, eheys- ja luotettavuusvaatimus
- käyttötarkoitussidonnaisuus
- tarpeellisuusvaatimus
- yhteysvaatimus.

Pirkanmaalla aluetietojärjestelmässä potilastietojen käsittely on ennalta suunniteltu, mikä näkyy selosteiden muodossa. Potilastietojen käsittely on

ohjeistettu käyttäjille, joten toiminnallisestikin tietojen käsittely on etukäteen suunniteltua. Osana etukäteissuunnittelua organisaation tulee analysoida toimintaan liittyvät tietosuojariskit. Aluetietojärjestelmän osalta ei ole tehty tietosuojariskianalyysiä, jossa tarkkaan analysoitaisiin toiminnan riskit ja uhat. Lisäksi kohdeorganisaatiossa ei ole kunnollista tietoturvapolitiikkaa, joten etukäteissuunnittelun vaatimuksen huomioimisessa olisi parannettavaa. Potilastietojen käsittelyohjeilla on pyritty vastaamaan tietojen huolellisuus- ja suojaamisvelvoitteeseen, virheettömyys-, eheys- ja luotettavuusvaatimuksiin, käyttötarkoitussidonnaisuuteen sekä tarpeellisuusvaatimukseen. Ohjeet ovat varsin kattavat, ja niissä on opastettu käyttäjiä oikeanlaiseen tietojen käsittelyyn.

Edellä esitetyistä vaatimuksista ongelmallisin toiminnallisesta näkökulmasta on yhteysvaatimus. Aluetietojärjestelmässä ei ole vielä teknisesti pystytty ratkaisemaan yhteysvaatimuksen täyttymisen tarkastamista, joten se asettaa vaatimuksia henkilökunnan toiminnalle. Asiallisen yhteyden varmistamiseksi henkilökunnan kouluttamisella on suuri merkitys. Hyvää on myös, että potilas pitää yksilöidä henkilötunnuksella, joten järjestelmän käyttäjät eivät voi selata potilaslistoja. Tämä voi parantaa yhteysvaatimuksen toteutumista.

Käyttäjien koulutuksella, joka on pakollinen aluetietojärjestelmän käyttäjille, pystytään hyvin lisäämään todennäköisyyttä, että lainsäädännön vaatimukset täytetään organisaation toiminnassa. PSHP:ssä koulutuksissa on hyvin huomioitu tietosuojan ja potilaiden oikeuksien merkitys, joten henkilökunnan tietoisuus oikeista toimintatavoista ja lainsäädännön säädöksistä pitäisi olla riittävä. Henkilökunnan toiminnan laillisuuden takaamiseksi organisaatiossa on varsin hyvin huomioitu oleellisia asioita. Erilaisilla sitoumuksilla ja koulutuksella on huolehdittu, että aluetietojärjestelmän käyttäjät ymmärtävät ja tietävät vastuunsa järjestelmää käytettäessä.

Organisaation toiminnalla on suuri merkitys potilaiden ja henkilökunnan oikeusturvan takaamiseksi. PSHP:ssä on tietosuoja-asiat huomioitu tarkkaan, mikä näkyy henkilökunnan koulutuksessa, ohjeistuksissa sekä sitoumuksissa.

Lisäksi organisaatiossa on tehty potilasasiakirja asetuksen mukaisesti ohjeet potilastietojen käsittelylle, jossa asiat käydään perusteellisesti läpi sekä käsittelyn että luovutuksen osalta. Myös potilaille vaaditut dokumentit ja tietojärjestelmäkuvaukset on tehty. Tärkeää lainmukaisuuden toiminnan takaamiseksi on myös valvonta, josta on tiedotettu käyttäjille, joten se voi vaikuttaa ennalta ehkäisevästi henkilökunnan toimiin. Muuten aluetietojärjestelmän ja sen käytön osalta on lainsäädännön vaatimuksista huolehdittu, mutta kunnollisen tietosuojariskianalyysin puuttuminen on huomioitavaa. Lisäksi asiallisen yhteyden tarkistaminen tulisi jotenkin järjestelmän osalta ratkaista.

Aluetietojärjestelmässä tietoja katseltaessa pitää käyttäjällä olla voimassa oleva suostumus tietojen katseluun, jonka järjestelmä tarkastaa, joten tietoja ei voi katsella luvattomasti. Mikäli käyttäjä katselee tietoja ilman suostumusta, niin hänen pitää antaa selitys miksi suostumusta ei tarvita. Tästä katselusta jää jälki lokeihin, jolloin jälkikäteen voidaan arvioida katselun oikeutus. Aluetietojärjestelmän suostumus vastaa lain pykäliä, koska siinä pitää riittävän tarkasti yksilöidä suostumus. PSHP:ssä suostumus pitää aina tulostaa ja antaa asiakkaalle allekirjoitettavaksi. Lisäksi potilaan pitää vahvistaa, että on saanut riittävän informoinnin suostumuksen osalta. Potilaan informoinnista ja suostumuksesta tehdään merkintä omiin potilastietojärjestelmiin. Suostumuksen merkitystä on korostettu käyttäjille koulutuksessa ja potilastietojen käsittelyohjeissa on erillinen kohta tietojen luovutukselle sekä katselulle, joten terveydenhuollon ammattilaisten pitäisi tietää lainsäädännön vaatimukset. Järjestelmä ei pysty valvomaan potilaiden suostumusten oikeellisuutta, joten suuri vastuu asiassa on henkilökunnan ammattietiikalla. Ratkaisuna tähän voisi olla, että potilailla olisi välineet sähköiseen allekirjoitukseen, jolloin järjestelmäkin varmistuisi suostumuksen olemassa olosta.

Aluetietojärjestelmässä on pyritty sopimuksin ja katselmoinneilla takaamaan, että tietojen luovutus sujuu lainmukaisesti. Näillä toimilla on pyritty turvaamaan, että tiedot ovat virheettömiä, salassa pidettyjä, muuttumattomia

sekä riittävästi salattu. Pirkanmaan sairaanhoitopiirissä vastuut tietoturvan ja aluetietojärjestelmän osalta oli hyvin määritelty. Aluetietojärjestelmän eri osapuolien vastuut on määritelty sopimuksissa erittäin tarkkaan. Vastuista on määritelty mistä osista ja tehtävistä kukakin osapuoli on vastuussa, kuten esimerkiksi kuka vastaa käytön seurannasta ja adapterien tietoturvasta. Mikäli osapuolet noudattavat sopimuksia ja katselmoinnit on tehty riittävällä huolellisuudella, niin järjestelmän osalta voidaan varmistua, että se noudattaa lain vaatimuksia tietojen luovuttamisen osalta. Potilaiden tietojen luovutuksesta jää merkintä lokiin, jolla pyritään vastaamaan potilasasiakirja-asetuksen vaatimukseen luovutuksesta tehtävään merkintään. Laissa kuitenkin vaaditaan, että merkintä luovutuksesta pitää tehdä potilasasiakirjaan, joten lokimerkintä ei ole riittävä täyttämään lain vaatimuksia.

Pirkanmaan sairaanhoitopiirissä tietoturvaa on suunniteltu ja sen merkittävyys on ymmärretty. Käyttöoikeuksiin ja käyttäjien tietoturvatietämykseen on panostettu minkä osoittaa esimerkiksi se, että käyttäjille on tehty ohjeita ja määräyksiä liittyen tietosuojaan, tietoturvaan ja potilastietojen käsittelyyn. Tietosuojasitoumusten lisäksi käyttäjien tulee allekirjoittaa sitoumuksia liittyen ammattilaiskorttiin ja tietoturvallisuuteen yleisestikin. Näiden avulla voidaan henkilökunnan tietämystä ja vastuullisuutta kasvattaa.

PSHP:ssä tietoturvatoimenpiteet ovat ennalta suunniteltuja. Suunnittelussa on otettu huomioon käyttöoikeudet, tietojen salaukset, kommunikaation turvallisuus, kryptaukset, palomuurit, varmenteet, yms. tekniset suojakeinot. Tietoturvatoiminnan suunnitelmallisuudella on pyritty vastaamaan julkisuuslain (621/1999) ja asetuksen viranomaistoiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (1030/1999) vaatimuksiin. Pääasiallisesti näihin vaatimuksiin on vastattu hyvin, mikä näkyy mm. käyttöoikeuksissa ja koulutuksissa. Pirkanmaan sairaanhoitopiirin osalta voitaisiin vielä paremmin vastata lainsäädännön vaatimuksiin tekemällä kunnollinen tietoturvapolitiikka. Tietoturvapolitiikassa määritellään koko organisaation tietoturvatoiminnan pääperiaatteet ja linjaukset, joten sen puuttumiseen tulisi organisaatiossa reagoida. Tietoturvapolitiikan rakentaminen tosin oli

tietohallintostrategiassa mainittuna, mutta se ei vielä riitä vaan politiikka tulee myös tehdä ja toteuttaa.

Käyttäjien ja heidän oikeuksiensa määrittelyt ja prosessit on hyvin toteutettu, niissä on määritelty riittävän perusteellisesti käyttäjien toimintayksiköt ja roolit. Myös Stakesin määrittelemien OID-koodien käyttö hakemistoissa ja koodistoissa on hyvä. Käyttäjien tunnistamiseen ja todentamiseen käytetään lain vaatimusten mukaista vahvaa tunnistautumista. Ammattilaiskortin käyttö on suunniteltu tietoturvallisesti ja se on myös ohjeistettu riittävästi käyttäjille. Käyttöoikeudet, pääsynhallinta ja käyttäjien todentaminen on aluetietojärjestelmässä hoidettu hyvin ja niihin liittyvät prosessit on riittävällä tarkkuudella suunniteltu ja dokumentoitu.

Aluetietojärjestelmäympäristössä on tietoturvallisuuden takaamiseksi luotu PKI-arkkitehtuuri, joka on yleisesti suositeltu ratkaisu, esimerkiksi Ruotsalainen [2004]. Arkkitehtuurin luotettavaksi kolmanneksi osapuoleksi on valittu Varsinais-Suomen sairaanhoitopiiri, joka on yleisesti tunnettu toimija ja jonka luotettavuuteen on takuut. Aluetietojärjestelmässä kaikki yhteydet on suojattu molempiin suuntiin, joten tiedonsiirto on turvallista ja voidaan taata tietojen salassa pitäminen. Tiedon siirrossa voidaan myös varmistua eri osapuolien aitoudesta ja oikeellisuudesta palvelinvarmenteiden avulla, joten lainsäädännön asettamat vaatimukset osapuolten oikeellisuudesta pystytään takaamaan. Siirrettävien tietojen virheettömyys, luotettavuus, kiistämättömyys ja eheys on turvattu palvelinvarmenteiden avulla tehdyillä sähköisillä allekirjoituksilla. Aluetietojärjestelmän ja adapterien tietorakenteet on standardoitu, mikä osaltaan parantaa tietojen eheyttä.

Aluetietojärjestelmässä on käytön valvonta järjestetty lakien mukaisesti. Valvontatyökalulla saadaan riittävän hyvin selville, mitä järjestelmässä on tehty. Valvontatyökalun käyttö edellyttää manuaalisia toimia, joten valvonta on organisaatioiden vastuulla. Lainmukaisen toiminnan parantamiseksi olisi hyvä kehittää automaattisia valvontakeinoja, jotka tarkistaisivat esim. käyttäjän ja potilaan asiallisen yhteyden sekä katseluperusteiden oikeellisuutta.

Pääasiallisesti aluetietojärjestelmä noudattaa lainsäädännön vaatimuksia, ja kaikessa toiminnassa on huomioitu tietosuoja. Potilaan ja henkilökunnan oikeusturva pystytään takaamaan järjestelmää käytettäessä, ja tiedot myös pysyvät salassa niiltä joille ne eivät kuulu. Tietoturva on teknisin keinoin varsin hyvin ratkaistu, mutta hallinnollisessa tietoturvassa on vielä parantamisen varaa, esimerkiksi tietoturvapolitiikan puuttuminen. Tietosuojan ja tietoturvan toteutuminen on kuitenkin paljon kiinni henkilökunnan toiminnasta, ja sitä ei yleensä teknisin keinoin ratkaista. Aluetietojärjestelmäympäristössä onkin pyritty varsin vahvasti vaikuttamaan henkilökunnan toimintatapoihin ja asenteisiin koulutuksin, ohjeistuksin, sitoumuksin sekä kurinpitotoimin.

6. Yhteenveto

Tutkimuksen tarkoituksena oli tutkia Fiale aluetietojärjestelmällä tapahtuvan tietojen käsittelyn lainmukaisuuden toteutumista. Tutkimuksessa keskityin terveydenhuollon alueeseen. Tutkimuksen alkupuoli keskittyi lainsäädännön asettamien vaatimusten kokoamiseen sekä terveydenhuollon tietoturvan erityiskysymyksiin. Näiden avulla pystyttiin kokoamaan arviointikriteeristö, joka toimi haastattelujen ja työn tulosten keräämisen perustana. Kriteeristöön koottiin vaatimuksia ja kysymyksiä, joiden avulla pyrittiin hallitsemaan suurta kokonaisuutta. Aluetietojärjestelmää tutkittiin sekä toiminnalliselta että tietojärjestelmätasolta.

Tutkimuksen loppupuoli keskittyi aluetietojärjestelmään ja sen arviointiin. Siinä tutkittiin, minkälainen aluetietojärjestelmä on rakenteeltaan, ja miten lainsäädännön vaatimuksia on pyritty täyttämään. Tietojärjestelmätasolla oli pyritty vastaamaan varsin hyvin lainsäädännön asettamiin vaatimuksiin, joitakin ongelmia lukuun ottamatta (taulukko 8.), kuten asiallisen yhteyden tarkistaminen. Tutkimuksessa ei arvioitu varsinaisten teknisten ratkaisujen luotettavuutta, vaan lähinnä keskityttiin miten ongelmia oli ratkaistu. Samalla myös arvioitiin organisaation toiminnallista tasoa, eli miten Pirkanmaan sairaanhoitopiirissä on aluetietojärjestelmän käyttäjien toimintaa pyritty ohjaamaan.

Havaittuja ongelmia:	
Vaatimukset	Ongelma
Etukäteissuunnittelun vaatimus	Tietosuojariskianalyysi ja tietoturvapolitiikat puuttuvat
Yhteysvaatimus	Järjestelmä ei tarkista asiallista yhteyttä tietojen katselijan ja potilaan välillä
Suostumus	Suostumuksen oikeellisuutta ei järjestelmä pysty varmistamaan
Merkintä luovutuksesta potilasasiakirjaan	Luovutuksesta jää merkintä lokeihin, mutta varsinaiseen potilasasiakirjaan ei siitä jää merkintää
Hyvä tiedonhallintatapa	Tietoturvapolitiikka puuttuu
Käytön seuranta	Lain mukaisesti kaikesta järjestelmän käytöstä jää merkintä lokiin, mutta käytön valvonta ei ole automaattista

Taulukko 8. Tutkimuksessa havaittuja ongelmia.

Tutkimuksessa havaittiin, että aluetietojärjestelmää suunniteltaessa ja rakennettaessa on potilaan tietosuoja pyritty huomioimaan koko prosessin ajan. Samalla havaittiin myös, kuinka suuri merkitys aluetietojärjestelmän käyttäjillä on lainmukaisuuden toteutumiseen ja miten käyttäjien toiminta voi vaarantaa muuten toimivan järjestelmän. Käyttäjien toiminnan lainmukaisuuden takaamiseksi Pirkanmaalla oli tehty paljon hyviä asioita, mutta myös puutteita havaittiin, kuten kunnollisen tietoturvapolitiikan puuttuminen. Lisäksi organisaatiossa oli varsin vähän pohdittu järjestelmään kohdistuvia tietosuojariskejä.

Tulevaisuudessa olisi mielenkiintoista tutkia terveydenhuollon ammattihenkilöiden toimintaa tarkemmin. Miten jokapäiväisessä työssä tietosuoja ja tietoturva todellisuudessa huomioidaan sekä minkälaisia vaikutuksia organisaation johdon tekemillä linjauksilla ja ohjeistuksilla on ihmisten toimintaan. Samalla voisi myös arvioida, minkälaisilla keinoilla henkilökunnan toimintaa tältä osin voitaisiin kehittää.

Aluetietojärjestelmien tulevaisuuden kannalta merkittävä muutos oli, kun heinäkuussa 2007 astui voimaan laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007). Aluetietojärjestelmälle lain aiheuttamista muutoksista suurin on määrittelyt kansallisista tietojärjestelmäpalveluista. Kansallisten tietojärjestelmäpalveluiden avulla tullaan tulevaisuudessa toteuttamaan monia aluetietojärjestelmän tarjoamia palveluita. Laissa säädetään asioista, joihin aluetietojärjestelmässä on jo varsin hyvin varauduttu vanhan lainsäädännön pohjalta. Esimerkiksi suostumuksessa ei sinänsä tapahdu merkittäviä muutoksia aluetietojärjestelmän kannalta.

Aluetietojärjestelmiä käyttävien organisaatioiden on varauduttava tulevaisuudessa liittymään kansallisen arkkitehtuuriin. Kansallisessa arkkitehtuurissa on yksi iso potilastietoarkisto, johon tallennetaan potilaiden tiedot. Aluetietojärjestelmän taustalla toimivia perusjärjestelmiä ei kuitenkaan lopeteta, vaan vieläkin potilastiedot säilytetään jokaisen organisaation omassa järjestelmässä. Kansallisen arkkitehtuurin avulla voidaan toteuttaa potilastietojen jakelu eri toimintayksiköiden välillä.

Kansallinen arkkitehtuuri voi herättää kysymyksiä aluetietojärjestelmien tulevaisuudesta ja merkityksestä, koska potilastietojen luovutus tulee tapahtua kansallisten tietojärjestelmäpalveluiden avulla. Koska perusjärjestelmistä pitää rakentaa kuitenkin liittymät kansalliseen arkkitehtuuriin, niin tässä kenties voitaisiin käyttää hyödyksi aluetietojärjestelmän tarjoamia liittymiä. Aluetietojärjestelmän avulla voidaan vähentää uusien liittymien määrää, kun tiedot voidaan siirtää alueelta keskitetysti kansalliseen arkkitehtuuriin. Tulevaisuudessa pitäisikin tutkia aluetietojärjestelmiä ja niiden liittymistä kansalliseen arkkitehtuuriin. Mitä muutoksia aluetietojärjestelmään tarvitaan, miten tietojen välitys tulisi hoitaa sekä mitä tietoja kansalliseen arkkitehtuuriin tulisi välittää ja mitä vaikutuksia kansallisella arkkitehtuurilla on organisaatioiden tietosuoja- ja tietoturvaratkaisuihin.

Kansallisessa arkkitehtuurissa tiedot säilytetään siten, että jokainen organisaatio pysyy omien rekistereidensä rekisterinpitäjänä. Mielenkiintoista

onkin nähdä, miten ratkaistaan tiedonsiirto aluetietojärjestelmien avulla kansalliseen arkistoon. Suomessa tiedonsiirtoon käytetään internetiä, joten se aiheuttaa suuria vaatimuksia tietoturvan toteutukselle. Liittymät arkistoon pitää huolellisesti katselmoida ja testata, jotta voidaan varmistua niiden tietoturvallisuudesta. Myös tietoliikenteen tulee olla vahvasti salattua.

Aluetietojärjestelmiä rakennettaessa on pohdittu nytkin ajankohtaisia asioita. Tietosuoja ja tietoturva ovat merkittävässä asemassa uusia kansallisiakin palveluita luotaessa. Kansallisessa arkkitehtuurissa pohditaan samoja tietosuoja- ja tietoturvakysymyksiä kuin aikanaan aluetietojärjestelmiä rakennettaessa, joten aluetietojärjestelmien kehitys- ja ratkaisumallien arviointeja tulisikin ottaa huomioon tietosuoja- ja tietoturvaratkaisuja suunniteltaessa. Aluetietojärjestelmien avulla saatuja kokemuksia ja oppeja ei tulisi unohtaa kansallisia palveluita suunniteltaessa. Aluetietojärjestelmien avulla on saatu arvokasta kokemusta eri toimintayksiköiden välisestä potilastietojen vaihdosta jo useamman vuoden ajan.

Viiteluettelo

[Bakker, 2003] Albert R. Bakker, The evolution of health information systems, security in practice and open issues. In: B. Blobel and P. Pharow (eds.) *Advanced Health Telematics and Telemedicine*. IOS Press, 2003, 15-20.

[Blobel, 2002] Bernd Blobel, *Analysis, Design and Implementation of Secure and Interoperable Distributed Health Information Systems.* IOS Press, 2002.

[Blobel and Pharow, 2000] Bernd Blobel and Peter Pharow, Security infrastructure for a regional electronic medical record. In: G.O. Klein (ed.) *Case Studies of Security Problems and their Solutions.* IOS Press, 2000, 65-74.

[Cavalli et al., 2004] Enrico Cavalli, Andrea Mattasoglioa, Francesco Pinciroli and Piergiorgio Spaggiari, Information security concepts and practices: the case of a provincial multi-specialty hospital. *International Journal of Medical Informatics* 73, 2004 297— 303.

[Ekebom et al., 2003] Ralf Ekebom, Tuire Mikkola ja Annakaisa Iivari, Saumattoman palveluketjun ja sitä tukevien tietohallintoratkaisujen ohjausryhmä. Suosituksia. *Sosiaali- ja terveysministeriön työryhmämuistioita* 18, 2003.

[Ensio ja Ruotsalainen, 2004] Antero Ensio ja Pekka Ruotsalainen, Tietoturvallinen kommunikaatioalusta: Suositus kansallisesti noudatettaviksi standardeiksi. *Osaavien keskusten verkoston julkaisuja* 7 2004.

[Ferrara, 2000] Fabrizio Ferrara, Security aspects in relation to the HISA standard middleware architecture. In: G.O. Klein (ed.) *Case Studies of Security Problems and their Solutions.* IOS Press, 2000, 95-110.

[Fujitsu, 2005] Fujitsu, Fujitsu mPollux: DigiSign Security Option. *Fujitsu Services Oy, Fujitsu mPollux Version 1.9* October 2005.

[Grimson et al., 2000] Jane Grimson, William Grimson and Wilhelm Hasselbring, The SI challenge in health care. Communication of the ACM 43: 6, June 2000, 49-55.

[Georgoulas et al., 2003] Aggelos Georgoulas, Athena Bourka, Alexandros Kaliontzoglou and Dimitris Koutsouris, RESHEN, a best practice approach for secure healthcare networks in Europe. In: B. Blobel and P. Pharow (eds.) *Advanced Health Telematics and Telemedicine*, IOS Press, 2003, 98-104.

[Gritzalis and Kokolakis, 2003] Dimitris Gritzalis and Spyros Kokolakis, Security policy development for healthcare information systems. In: B. Blobel and P. Pharow (eds.) *Advanced Health Telematics and Telemedicine*, IOS Press, 2003, 105-110.

[Hakala et al., 2002] Ari Hakala, Sirkku Helasterä ja Kristiina Luokomaa, Raportissa: Pekka Ruotsalainen (toim), Ehdotus Sosiaali- ja terveydenhuollon sähköisen asioinnin arkkitehtuuriksi - terveydenhuollon PKI-arkkitehtuuri. *Osaavien keskusten verkoston julkaisuja,* 4, 2002.

[HE, 2007] Hallituksen esitys Eduskunnalle sosiaali- ja terveydenhuollon asiakastietojen sähköistä käsittelyä koskevaksi lainsäädännöksi.

[HetiL, 1999] Henkilötietolaki 1999/523. Saatavana verkossa: http://www.finlex.fi/fi/laki/ajantasa/1999/19990523.

[HL7 Finland, 2004] OpenCDA HelpDesk –projekti, Perusjärjestelmäadapterin tietosuoja. *HL7 Finland ry* 2004.

[Huston, 2001] Terry Huston, Security issues for implementation of E-medical records. Communications of the ACM 44: 9 Sep. 2001, 89–94.

[Hyppönen el., 2005] Hannele Hyppönen, Päivi Hämäläinen, Marja Pajukoski ja Emmi Tenhunen, Selvitys sosiaali- ja terveydenhuollon saumattoman palveluketjun kokeilulain (22.9.2000/811) toimeenpanosta kokeilualueilla. *STAKES, raportteja* 6, 2005.

[Häyrinen et al., 2004] Kristiina Häyrinen, Jari Porrasmaa, Jorma Komulainen ja Kauko Hartikainen, Sähköisen potilaskertomuksen yhdenmukaiset rakenteiset ydintiedot. *Osaavien keskusten verkoston julkaisuja* 5, 2004.

[Iivari ja Ruotsalainen, 2006] Annakaisa Iivari ja Pekka Ruotsalainen (toim.), Terveydenhuollon valtakunnallisen tietojärjestelmäarkkitehtuurin

periaatteet, Alueellisista ratkaisuista kansalliseen kokonaisuuteen. *Sosiaali- ja terveysministeriön selvityksiä* 8, 2006.

[Itälä, 1999] Timo Itälä, Makropilotin aluearkkitehtuuri. *Satakunnan Makropilotti –Sosiaali- ja terveysministeriön kehittämishanke* 1999.

[Itälä, 2000] Timo Itälä, Perusjärjestelmäintegraatio ja aluetietojärjestelmä. Toiminnallinen kuvaus ja vaatimukset toteutukselle. Versio 0.3. 3.11.2000. *Satakunnan Makropilotti –Sosiaali- ja terveysministeriön kehittämishanke* 2000.

[Itälä ja Ruotsalainen, 2004] Timo Itälä ja Pekka Ruotsalainen, Tietoturvallinen kommunikaatioalusta luovutusten ja luovutuslokin hallinnan suositukset. *Osaavien keskusten verkoston julkaisuja* 6, 2004.

[Jokinen, 1999] Yrjö Jokinen, Tietoturvallisuus. Kirjassa: Kaija Saranto ja Mikko Korpela (toim.) *Tietotekniikka ja tiedonhallinta sosiaali- ja terveydenhuollossa.* WSOY, 1999, 175-187.

[JulkA, 1999] Asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta 1999/1030. Saatavana verkossa: http://www.finlex.fi/fi/laki/ajantasa/1999/19991030.

[JulkL, 1999] Laki viranomaisten toiminnan julkisuudesta 1999/621. Saatavana verkossa: http://www.finlex.fi/fi/laki/ajantasa/1999/19990621.

[Järvinen ja Järvinen, 2004] Pertti Järvinen ja Annikki Järvinen, *Tutkimustyön metodeista*. Opinpaja, 2004.

[Katsikas and Kokolakis, 2004] Sokratis Katsikas and Spyros Kokolakis, High level security policies for health care establishments. In: L. Bos et al. (eds.) *Medical and Care Compunetics*. IOS Press, 2004, 407- 415.

[Korhonen, 2003] Rauno Korhonen, *Perusrekisterit ja tietosuoja*. Edita publishing Oy, 2003.

[Lausvaara et al., 2004] Anni Lausvaara, Pia Soidinmäki ja Tiia Tuuri, Saumattomat palveluketjut Pirke-hankkeessa. *Pirkanmaan sairaanhoitopiiri, tietohallinto*, 2004.

[Lehto, 2000] Juhani Lehto, Saumaton palveluketju mosaiikkimaisessa järjestelmässä. Kirjassa: Susanna Nouko-Juvonen, Pekka Ruotsalainen ja Irma Kiikkala (toim.) *Hyvinvointivaltion palveluketjut*. Tammi, 2000, 33-48.

[Mikola, 2003] Tuire Mikola, Tietojen käyttö yli rajojen: Terveydenhuollon aluetietojärjestelmät. *Tietoyhteiskunta-ajan yhteistyö perusrekisteriseminaari*, 24.10.2003.

[Mykkänen, 2005] Juha Mykkänen, Maritta Korhonen, Jari Porrasmaa, Tuula Tuomainen ja Antero Ensio, Tietojärjestelmien standardointityön organisointi ja kehittäminen terveydenhuollossa: nykytila ja toimenpide-ehdotukset. *Osaavien keskusten verkoston julkaisuja* 3, 2005

[Määttä, 2000] Jarmo Määttä, Makropilotti välineenä sosiaali- ja terveydenhuollon uudistamistyössä. *Sairaalaviesti* 2, 2000, 5-6.

[Nordberg, 2004] Ragnar Nordberg, Policy management and access control in practice. In: L. Bos et al. (eds.) *Medical and Care Compunetics*. IOS Press, 2004, 428-433.

[Nykänen ja Karimaa, 2002] Pirkko Nykänen ja Erkki Karimaa, Satakunnan makropilotin ratkaisujen mallit ja tietotekniset suunnitelmat. Kirjassa: Jukka Ohtonen (toim.) *Satakunnan makropilotti: tulosten arviointi*. FinOHTAn raportti 21, 2002, 52-72.

[Ohtonen, 2002] Jukka Ohtonen (toim.), *Satakunnan makropilotti: tulosten arviointi.* FinOHTA raportti 21, 2002.

[Paavilainen, 1998] Juhani Paavilainen, *Tietoturva*. Suomen ATK-kustannus 1998.

[Pahlman, 2005] Irma Pahlman, *Asiakirjajulkisuus ja tietosuoja sosiaali- ja terveydenhuollossa*. Edita Publishing, 2005.

[Pajukoski, 2004] Marja Pajukoski, *Sähköinen asiointi sosiaali- ja terveydenhuollossa*. Stakes, 2004.

[Porali, 2005] Minna Porali, Julkisen avaimen järjestelmä osana terveydenhuollon tietoturvaa. Kuopion yliopisto, tietojenkäsittelytiede, Pro gradu –tutkielma (2005).

[PotL, 1992] Laki potilaan asemasta ja oikeuksista 786/1992. Saatavana verkossa: http://www.finlex.fi/fi/laki/ajantasa/1992/19920785

[PSHP, 2004] Pirkanmaan sairaanhoitopiiri, *Tilastoja - 2004*.

[PSHP, 2007] Pirkanmaan sairaanhoitopiiri, http://www.pshp.fi (viitattu 3.6.2007).

[Reponen, 2006] Kirsi Reponen, Terveydenhuollon organisaation tietoturvallisuus henkilöstön arvioimana. Kuopion yliopisto, terveyshallintotiede, Pro gradu –tutkielma, 2006.

[Reponen ja Ensio, 2005] Kirsi Reponen ja Anneli Ensio, Sähköisten työvälineiden juurruttaminen käytännön hoitoprosesseihin sekä näihin liittyvä tietoturva. Kuopion yliopisto, terveyshallinnon ja –talouden laitos, Shiftec-tutkimusyksikkö, loppuraportti 27.1.2005.

[Ruotsalainen, 2000] Pekka Ruotsalainen, Asiakaslähtöinen palveluketju ja tietoteknologia. Kirjassa: Susanna Nouko-Juvonen, Pekka Ruotsalainen ja Irma Kiikkala (toim.) *Hyvinvointivaltion palveluketjut*. Tammi, 2000, 7-32.

[Ruotsalainen, 2004] Pekka Ruotsalainen, Turvallinen kommunikaatioalusta: Ohjeita PKI-infrastruktuurin toteuttamiselle. Raportissa: Pekka Ruotsalainen (toim.) Turvallinen kommunikaatioalusta: Ohjeita PKI-infrastruktuurin toteuttamiselle, *Osaavien keskusten verkoston julkaisuja* 2, 2004.

[Ruotsalainen, 2005] Pekka Ruotsalainen, tietoturvallinen kommunikaatio sosiaali- ja terveydenhuollossa. Pirke yhteistyöseminaari 15.2.2005.

[Ruotsalainen, 2006] Pekka Ruotsalainen, Suositukset terveydenhuollon asiakastietojen tietoturvalliselle sähköiselle arkistoinnille. *STAKES*, raportteja 4, 2006.

[Ruotsalainen, 2006b] Pekka Ruotsalainen, Usean toimintayksikön yhteinen käyttäjän ja käyttöoikeuksien hallinta – periaatteet ja suositukset. *STAKES*, raportteja 4, 2006.

[Ruuska ja Haukkapää-Haara] Anitta Ruuska ja Pirjo Haukkapää-Haara, Saumattomien palveluketjujen edellytyksiä – teknologia, muuttuvat toimintamallit ja alueellinen yhteistyö. Kirjassa: Leini Sinervo (toim.), *Saumattomien toimintojen juurruttaminen – Juuria-hankkeen loppuraportti.* STAKES, aiheita 26, 2004.

[Saranummi, 2000] Niilo Saranummi, Järjestelmäintegraatio-opas, *VTT Tietotekniikka* 2000. Saatavana verkossa: http://http://www.vtt.fi/tte/tutkimus/tte5/tte53/SI_opas/Raportin_osiot/Raportin_osiot/SI_opas_paateksti.htm

[Saranummi, 2003] Niilo Saranummi, Pirkanmaan aluearkkitehtuuri: Sosiaali- ja terveydenhuollon saumattoman palveluketjun sekä niitä tukevan tietoteknologian käyttöönotto Pirkanmaalla - Loppuraportti. *VTT Tietotekniikka* 2003.

[SatSHP] Satakunnan sairaanhoitopiiri, www.satshp.fi (viitattu 4.7.2007).

[SatSHP, 2007] Satakunnan sairaanhoitopiiri, Aluetietojärjestelmän käyttöohjeet: versio 2.4.0.. *Satakunnan sairaanhoitopiiri,* 2007.

[Sinervo, 2004] Leini Sinervo, *Saumattomien toimintojen juurruttaminen – Juuria-hankkeen loppuraportti.* STAKES, aiheita 26, 2004.

[Sorvari, 2004] Hannu Sorvari, *Oikeudellisia näkökohtia potilastiedosta ja potilaan suostumuksesta tietokoneistuvassa terveydenhuollossa.* STAKES, *raportteja* 285, 2004.

[STM, 1998] Sosiaali- ja terveysministeriö, Sosiaali ja terveydenhuollon tietoteknologian hyödyntäminen osa 1 – saumaton hoito- ja palveluketju asiakaskortti. *Sosiaali- ja terveysministeriön työryhmämuistioita* 8, 1998.

[STM, 2001] Sosiaali- ja terveysministeriön asetus potilasasiakirjojen laatimisesta sekä niiden ja muun hoitoon liittyvän materiaalin säilyttämisestä 99/2001. Saatavana verkossa: http://www.finlex.fi/fi/laki/alkup/2001/20010099.

[STM, 2002] Sosiaali- ja terveysministeriö, Makropilotti - sosiaali- ja terveydenhuolto 2000 –luvulle. *Sosiaali- ja terveysministeriön julkaisuja* 22, 2002.

[STM, 2003] Sosiaali- ja terveysministeriö, Sähköisten potilasasiakirjajärjestelmien valtakunnallinen määrittely ja toimeenpano. *Sosiaali- ja terveysministeriön työryhmämuistioita* 38, 2003.

[STM, 2007] Sosiaali- ja terveysministeriö, KANTA kokonaisarkkitehtuuri – vaatimusmäärittely. *Terveydenhuollon kansallisen tietojärjestelmäarkkitehtuurin määrittelyprojekti,* 2007.

[Sullivan, 2004] Dan Sullivan, *The Definitive Guide to Security Management*. Realtimepublishers 2004.

[Tammisalo, 2005] Tero Tammisalo, Sosiaali- ja terveydenhuollon tietojärjestelmien tietoturvan ja tietosuojan hallinnan periaatteet ja hyvät käytännöt. *STAKES, raportteja* 5, 2005.

[Tammisalo, 2007] Tero Tammisalo, Sosiaali- ja terveydenhuollon organisaatioiden tietoturvan hallinnointi. *STAKES*, raportteja 5, 2007.

[Tuuri, 2003] Tiia Tuuri, Aluetietojärjestelmän avulla toteutettu järjestelmäintegraatio sosiaali- ja terveydenhuollossa. Tampereen teknillinen yliopisto, sähkötekniikan laitos, Diplomityö, 2003

[VAHTI, 2004a] Valtionhallinnon tietoturvallisuuden johtoryhmä, Tietoturvallisuus ja tulosohjaus. *Valtiovarainministeriö* 2, 2004.

[VAHTI, 2004b] Valtionhallinnon tietoturvallisuuden johtoryhmä, Valionhallinnon keskeisten tietojärjestelmien turvaaminen. *Valtiovarainministeriö* 5, 2004.

[VAHTI, 2006] Valtionhallinnon tietoturvallisuuden johtoryhmä, Tunnistaminen julkishallinnon verkkopalveluissa. *Valtionvarainministeriö* 12, 2006.

[Ylipartanen, 2004] Arto Ylipartanen, *Tietosuoja terveydenhuollossa: potilaan asema ja oikeudet henkilötietojen käsittelyssä*. Tietosanoma, 2004.

[YT Tieto, 2006a] Teemu Sainio, Pia Soidinmäki ja Sari Taivalsalmi, Kohti saumatonta palvelua – Pirke-hanke 2001-2005. *YT Tieto* 2006.

[YT Tieto, 2006b] YT Tieto, Pirke II – Pirkanmaan saumattomien hyvinvointipalvelujen kehittämishanke. *YT Tieto* 2006.

[YT Tieto, 2006c] YT Tieto, ATJ-käyttäjän opas. *YT Tieto* 2006.

[YT Tieto, 2007] YT Tieto, Pirkanmaan sosiaali- ja terveydenhuollon aluetietojärjestelmäpalvelu. *YT Tieto* 2007.

[Winblad et al., 2006] Ilkka Winblad, Jarmo Reponen, Päivi Hämäläinen ja Maarit Kangas, Informaatio- ja kommunikaatioteknologian käyttö Suomen terveydenhuollossa vuonna 2006 – Tilanne ja kehityksen suunta. *STAKES*, raportteja 7, 2006.

Liite 1. Arviointikriteeristö

Vaatimukset	**Tietojärjestelmä taso**	**Toiminnallinen taso**
1. Yleiset lainsäädännölliset vaatimukset		
Etukäteissuunnittelun vaatimus		Henkilörekisteriseloste, tietojärjestelmäseloste, asiakastiedote, tietosuojaohje.
Yhteysvaatimus	Potilaan tunnistaminen henkilötunnuksella	Koulutus ja ohjeistus, sitoumukset
Huolellisuus- ja suojaamisvelvoite	Henkilötiedot kryptattu.	Koulutus ja ohjeistus, tulostuskielto, sitoumukset
Virheettömyys, eheys ja luotettavuus	Adapterien katselmointi, tietojen salaus, siirrettävä potilastieto standardoitu, käyttöoikeudet	Valvonta, koulutus ja ohjeistus, sitoumukset
Käyttötarkoitussidonnaisuus	Käyttäjänhallinta	Ohjeistus, koulutus ja sitoumukset
Tarpeellisuusvaatimus		Ohjeistus, koulutus ja sitoumukset
Rekisterinpitäjän velvollisuudet (ohjeistus + valvonta)		Tietosuojaohje ATJtä koskien. Keskitetysti laadittu lainsäädännön mukainen ohjeistus jokaisen organisaation käytettävissä. Käyttöoikeudet antanut organisaatio huolehtii antamiensa ohjeiden ja määräysten oikeellisuudesta
Asiakkaan informointi henkilötietojen käsittelystä		Asiakastiedote, ohjeistus. Henkilötietojen käsittelyn informointi asiakkaille, tästä laitetaan merkintä potilastietojärjestelmään. Tietojärjestelmäselosteet ovat esillä
Asiakkaan tarkastusoikeus		Tarjolla tarkastuspyyntölomake
Luottamuksellisen viestin suoja	Adapterien tietoturvallinen liittäminen katselmoidaan. Henkilötiedot kryptattu. Tiedonsiirron salaus.	
Luottamuksellinen hoitosuhde		Koulutus, ohjeistus ja ammattietiikka
Tiedon alkuperän tunnistettavuus	Osapuolten todennus, varmenteet	
Tietojen suojaamisvelvoite	Ennen järjestelmään liittymistä toimintayksikössä pidetään perusteelliset testit liittyen tietoturvaan.	
Hyvä tiedonhallintatapa		Tietojärjestelmäselosteet, tietojen suojauksesta huolehdittu, potilasasiakirjaohjeet tietojen käsittelylle.
Vaitiolovelvollisuus ja salassapito		Koulutus, ohjeistus, sitoumukset ja

		ammattietiikka
Tietojen saatavuus ja käytettävyys	Sopimuksin määritelty järjestelmältä vaadittava käytettävyyden aste.	
Alkuperäisen tiedon muuttumattomuus	Tiedonsiirron salaus. Ennen järjestelmään liittymistä toimintayksikössä pidetään perusteelliset testit liittyen tiedonsiirron tietoturvallisuuteen.	
2. Suostumus ja sen hallinta		
Kohde	Asiakas tunnistetaan HETU:n perusteella. Järjestelmästä ei saa potilaslistoja esille. Järjestelmä pakottaa käyttäjän täyttämään vaadittavat tiedot.	Käyttäjä rajaa halutut palvelut. Käyttäjiä kehotettu tarkastamaan tunnistetun kohteen oikeellisuus.
Rajaus	Järjestelmä pakottaa käyttäjän täyttämään vaadittavat tiedot.	Viitteistä: voi rajata palveluittain tai organisaatioittain. Ohjeistettu, että yhdessä potilaan kanssa.
Saaja	Järjestelmä pakottaa käyttäjän täyttämään vaadittavat tiedot.	Voidaan laittaa joko henkilö-, rooli- tai organisaatiotasolla
Syy	Järjestelmä pakottaa käyttäjän täyttämään vaadittavat tiedot.	Suostumusohjeissa on selvitetty millä perusteilla voidaan tietoja katsella.
Kesto	Järjestelmä pakottaa käyttäjän täyttämään vaadittavat tiedot.	
Antaja	Järjestelmä pakottaa käyttäjän täyttämään vaadittavat tiedot.	
Tyyppi	Järjestelmä pakottaa käyttäjän täyttämään vaadittavat tiedot.	
Allekirjoitus		Suostumus tulostetaan, jonka kohdehenkilö allekirjoittaa.
Asiakkaan informointi		Koulutus, ohjeistus. Asiakastiedote pitää käydä suostumuksen yhteydessä läpi. Annetaan myös ohjeet tarkastuspyynnön tekemisestä.
Sähköinen allekirjoitus	Ei käytössä.	
Asiakkaan suostumukset		Tallennetaan katselijan arkistoihin. Merkintä suostumuksesta kirjataan käsin perusjärjestelmään.
Suostumusten arkistointi		Ammattilainen joka on tekemisissä potilaan kanssa pyytää suostumuksen ja tekee siitä merkinnän rekisterinpitäjän potilasrekisteriin. Allekirjoitettu suostumus arkistoidaan paperisena ko. toimintayksikön arkistoon.
Suostumus loki	Lokiin merkintä.	
3. Potilastietojen luovutus ja käsittely		
Tiedon luovuttajan vastuut henkilötietolaissa	Adapterien tietoturvallinen liittäminen katselmoidaan. Tietoturvasta on huolehdittu.	Potilasasiakirjojen luovutuksesta on tehty vaaditut ohjeet.

	Lokiin jää luovutuksesta merkintä.	
Vastaanottajan velvollisuudet henkilötietolaissa	Adapterien tietoturvallinen liittäminen katselmoidaan. Tietoturvasta on huolehdittu, Järjestelmä tarkastaa joka kerta oikeuden tietojen katseluun.	Ohjeistukset, sitoumukset. Potilasasiakirjojen luovutuksesta on tehty vaaditut ohjeet.
Luovutus ilman suostumusta	Potilaan tietoja ei pysty pääasiallisesti katselemaan ilman voimassa olevaa suostumusta. Käyttäjä voi katsella tietoja potilaan tietoja ilman suostumusta, mutta tällöin hänen pitää antaa syy, että mihin katselu perustuu.	
Tiedon käsittelyyn oikeutetut henkilöt	Käyttäjänhallinta ja ammattilaisten vahva tunnistautuminen.	
Luovutuksen edellytyksien tarkastus	Järjestelmä tarkastaa joka kerta katseluun vaadittavan oikeutuksen.	
Luovutuspyynnön tietosisältö	Määritelty suostumuksen yhteydessä.	
Potilastietojen käsittely: ohjeistus ja lainsäädännön huomioiminen		Potilasasiakirjojen käsittelyohjeet.
4. Yleinen tietoturva		
Tietojen eheys	Tiedon tuottajat noudattavat tiettyjä standardeja – CDA1.	
Tietojen käytettävyys ja saatavuus	Ennen järjestelmään liittymistä toimintayksikössä pidetään perusteelliset testit. Sopimuksissa määritelty järjestelmien käyttöasteet.	
Tietojen suojaus ja salaus	Adapterien tietoturvallinen liittäminen katselmoidaan. ATH saa kaiken potilastiedon (CDA-dokumentit) perusjärjestelmiltä adapterin avulla. ATJ ja perusjärjestelmä (tai perusjärjestelmän adapteripalvelu) varmistuvat keskustelevansa laillisen osapuolen kanssa kaksivaiheisen ”SSL-kättelyn” avulla.	
Tietojen muuttumattomuus	Adapterit / liittymät katselmoidaan.Tieto on salattua.	
Tietojen kiistämättömyys	Palvelinvarmenteet	
Tietojen luottamuksellisuuden säilyttäminen	Tiedon siirron salaus (2-way SSL 128bittinen salaus)	Tulostuskielto
Tietoturvan vastuuttaminen	Vastuu raja adapterin ja Fialen välissä. Rekisterinpitäjä vastaa rekisteristään, adapteristaan ja tuotettavasta tiedosta. Palvelusopimus tuottajien kanssa.	Organisaatio on tehnyt erityisen sopimuksen jossa määritellään tietoturvataso, toimittajan ja tilaajan vastuut. Organisaatioilla on oikeus tehdä katselmointeja toimittajan järjestelmiin. Liittyessä palveluun on tehty puitesopimus palveluntarjoajan kanssa, jossa liittyvä org. Vakuuttaa täyttävänsä

		tietosuojavelvoitteet. Noudattaa STM:n mallisopimusta tietojenkäsittelyn ulkoistamisesta.
Turvaluokitukset	Tiedot ovat salassa pidettäviä.	
Käyttäjien koulutus, vastuuttaminen ja velvoitteet		Käyttäjien koulutuksesta ja ohjeistuksesta sekä vastuiden ja velvoitteiden selittämisestä on huolehdittu järjestelmän koulutuksissa ja ohjeistuksilla. Jokainen käyttäjä tutustuu organisaation tietoturvallisuusohjeisiin ja allekirjoittaa sitoumuksen sen noudattamiseksi.
Tietoturvan suunnittelu ja hallinta (mm. tietoturvapolitiikka)		Erityinen tietohallintostrategia, jossa tärkeässä osassa myös tietoturva. Tietohallinnon johtoryhmä tekee linjaukset organisaatiossa. Käyttäjille tehty erityinen tietoturvaohje. Varsinaista tietoturvapolitiikkaa ei ole.
Järjestelmien ja prosessien dokumentointi		Suoritetaan tietoturvakatselmointi, määritellään ja kuvataan organisaation tietoturva.
Ohjeistus		Tietoturvaohjeet, sitoumukset ja koulutukset.
Dokumentointi (järjestelmät ja tietoturvaratkaisut)		Organisaation tietoturva ja siihen liittyvät prosessit (käyttäjänhallinta) on kuvattu ja määritelty.
5. Ohjelmistoturvallisuus		
Käyttäjänhallinta	Kun käyttäjä kirjautuu järjestelmään, syntyy istunto. Kun käyttäjä siirtyy sovelluksesta toiseen (ATJ-puoli, ATH-puoli jossa viitetietokanta on), istunnonsiirrolla varmistetaan että käyttäjä kirjautuu vain kerran järjestelmään. Välttämättömät käyttäjätiedot, organisaatio, käyttäjärooli ja tunnuksen yhdistetty geneerinen-ID välitetään istunnonsiirrossa.	Ammattilainen ei saa käyttöoikeuksia ennen koulutusta ja tietosuojasitoumusta.
Käyttäjien tunnistaminen ja todentaminen	Varmenteen sisältävä ammattilaiskortti, joka mahdollistaa vahvan tunnistautumisen.	Henkilökohtaiset käyttäjätunnukset, ei yleis- tai yhteiskäyttötunnuksia
Käyttäjäroolit	Roolit määritelty jokaisen käyttäjän työtehtävien mukaisesti. Käyttäjä kirjautuu aina tiettyyn käyttäjärooliin ja toimipaikkaan.	Aluetietojärjestelmän käyttöönottoa varten on määritelty jokaisen liittyjäorganisaation osalta aluetietojärjestelmässä käytettävä

		organisaatiohierarkia ja määritelty järjestelmässä käytettävät toimipisteet sekä tarvittavat koodistot. Hakemistoissa ja koodistoissa käytetään valtakunnallisten suositusten mukaisesti OID-tunnuksia, jotka on muodostettu STAKESin ohjeistuksen mukaisesti. Käytön aikana on kerätty kokemuksia hakemistojen ja koodistojen hallinnan ja käytön kehittämiseksi aluetietojärjestelmässä.
Oikeudet ja valtuudet	Tunnistekortti ja PIN-koodi – vahva tunnistaminen ja todentaminen varmenteiden avulla. Käyttäjän tunnistamiseksi on olemassa PKI-tasoinen korttipohjainen ympäristö. Käyttöoikeudet eri sovelluksiin ja toimintoihin sidotaan käyttäjärooliin. Lisäksi käyttäjien oikeuksia rajaa toimipaikka.	Oikeudet on määritelty roolien mukaisesti. Oikeuksien myöntämisprosessi on ennalta määritelty ja dokumentoitu.
Pääsynhallinta		
Vastuut		Käyttäjille on selvitetty koulutuksissa ja sitoumuksissa omista vastuistaan ja tunnuksien henkilökohtaisuudesta. Käyttöoikeuksista vastaa alueellinen pääkäyttäjä tai organisaatioiden pääkäyttäjät.
Käyttöoikeuksien hakemisprosessi		Kirjallinen esimiehen allekirjoittama käyttöoikeushakemus. Alueellinen pääkäyttäjä tai organisaation pääkäyttäjä tekee käyttöoikeudet. Käyttöoikeusprosessi on kokonaisuudessaan dokumentoitu.
Dokumentointi		Käyttöoikeuksien hakemisen prosessi on dokumentoitu.
Käyttäjäkoulutukset ja ohjeistukset		PSHP tietosuojasitoumus, kuittaus tietosuojakoulutuksen yhteydessä sitoumukseen. Ammattilaiskortti ja sen käyttö ohjeistetaan ja allekirjoitetaan säännöt ymmärretyiksi. Samoin PIN-koodin vaihto. Käyttäjille on monissa kohdin ohjeistettu että kortti ja koodi ovat henkilökohtaisia.
Prosessin tietoturva (tunnuksien jakelu yms.)		PKI-kortti haetaan esimiehen allekirjoittamalla

		hakemuksella. PKI-kortin käyttöönottoon liittyy allekirjoituksella vahvistettava sitoutuminen tietoturvallisiin menettelytapoihin. Korttien ja PIN-koodien jakelu tapahtuu erikseen. RA-pisteen prosessit tietoturvallisten menettelytapojen ja prosessien mukaan.
Valtuuksien yksityiskohtainen määrittely		Määritellään työtehtävien mukaisesti henkilökohtaisesti.
Tunnuksien sulkeminen ja korttien hävittäminen		Oikeudet myönnetään työsopimuksen mukaisesti. Sopimuksen loputtua kortti palautetaan ja hävitetään asianmukaisesti. Käyttäjän poistuessa organisaatiosta pääkäyttäjät pyytävät kortin asettamista sulkulistalle.
Käytön seuranta ja valvonta	Kaikesta järjestelmän käytöstä jää lokeihin merkintä. Valvojat seuraavat väärinkäytöksiä.	
Kirjautumisprosessi	Kirjautumisikkuna ja ammattilaisen etusivu: ohjeet. Asiakastiedon hallinnassa tietomäärä minimissä. Kirjautumistiedot 2-way SSL. Käyttäjälle tulee kirjautuessa informaatiota edellisistä kirjautumisista ja yrityksistä sekä häntä opastetaan ilmoittamaan mahdollisista epäselvyyksistä.	
Asiakkaan tunnistaminen	Henkilötunnuksella, ei mahdollista katsella potilaslistoja.	
Oikeudet hoitoprosessiin	Mahdollisuus luoda palveluketjuja järjestelmässä: organisaatiot, roolit ja palvelut jotka osallistuvat potilaan hoitoon.	
Korttien väärinkäytökset	Kirjautumisyritysten määrä rajattu kolmeen. Väärä PIN-koodi lukitsee kortin, avaaminen vain ATK-yhdyshenkilön pyynnöllä RA-pisteessä, jossa PUK-koodeja hallitaan.	
6. Tietoliikenneturvallisuus		
Siirrettävän tiedon eheys ja luottamuksellisuus	Kaikki pyynnöt lähetetään SSL-salattuina niin, että SSL-yhteyden muodostamiseen vaaditaan molempien osapuolien varmenteet. Osapuolet pyytävät/tunnistavat vastapuolen sertifikaatin.	
Tietoliikenteen salaus	Kaksisuuntainen SSL-yhteys.	
Tietojen muuttumattomuus ja kiistämättömyys	SSL ja palvelinvarmenteet. Alueellinen koodistojen hallinta ja	

	hakemistot. Adapterit katselmoidaan tarkasti.	
Osapuolten aitous ja oikeus (tunnistus, todentaminen)	Tiedonsiirrossa palvelinvarmenteet ja käyttäjät todennetaan lain mukaisesti ammattilaiskortilla. Sopimus varmennepalvelun tuottamisesta on tehty V-SSHP:n kanssa. Autentikointi hoidetaan mPollux DigiSign –palvelulla.	
Tietojen sähköinen allekirjoitus	Palvelinvarmenteiden avulla totetutettu.	
Tietojen turvaamisen menetelmät	Potilastiedot ovat arkaluonteisia ja tietoturvaan on kiinnitetty erityistä huomiota. Kaikki katselmoidaan ja kuvataan. Tämä tulee esille laitteiden, palomuurien ja niiden sijoittelun, tietoliikenteen suojaamisessa, pääsynvalvonnassa, ohjelmien laittoman käytön estämisessä, tietojen kryptaamisessa sekä lokitiedoissa tietojen käytöstä.	
Järjestelmän tietoturvaratkaisujen suunnittelu ja dokumentointi	Adapterit / liittymät katselmoidaan.	
Ulkopuolisten tahojen käytön esto	Kirjautumisyritysten määrä rajattu.	
7. Lokit ja valvonta		
Tapahtumatietoloki	Kaikki järjestelmän käyttötapahtumat tallentuvat lokiin. Asiakastietojen katsomisesta, käytöstä ja luovutuksesta muodostuu seurantalokiin käyttäjätieto.	
Käyttäjäloki	Käyttäjän tekemät teot on jäljitettävissä.	Käyttäjärekisterit -> säännöllinen seuranta ja raportointi. Ylläpito-oikeuksien seuranta ja valvonta -> säännöllinen seuranta ja raportointi.
Asiakkaan tarkastusoikeus	Asiakkaan hetulla voidaan tarkistaa, ketkä ovat potilaan tietoja katselleet.	Jokaisella henkilöllä on oikeus saada tietää mitä häntä koskevia tietoja on seurantalokiin tallennettu. Tarkastuspyyntölomake ja sen käyttö ohjeistettu.
Suostumukset	Lokimerkintä	
Luovutusloki	Potilaan tietojen luovutuksesta jää järjestelmän lokiin merkintä.	
Käytön seuranta ja valvonta	Viitetietojen katselusta jää aina lokiin merkintä.	Valvojat joka organisaatiossa. Valvonnasta tiedotettu käyttäjille. Preventiivisesti katsellaan lokeja -> loki vaatii syyn, valvontaan. Myös valvontatoimista jää merkintä, pitää olla syy.
Väärinkäytökset: prosessi sekä tiedottaminen		Väärinkäyttö johtaa kussakin organisaatiossa tietoturva- ja tietosuojaohjeissa

		mainittuihin kurinpitotoimenpiteisiin.
Valvonnan vastuut		Organisaatioissa on omat ATJ:n käyttöä valvovat henkilöt – valvojat.
Kurinpitotoimet		Kurinpitotoimet rikoslain mukaiset.
Tietoturvaloukkausten seuranta		Järjestelmän käyttöä seurataan.