



TERVEYDENHUOLLON TOIMIKORTTI

Käyttöönotto Tampereen seudulla

Tiina Apponen

Opinnäytetyö
Helmikuu 2012
Tietojenkäsittely
Terveysalan tietohallinta

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tietojenkäsittely
Terveysalan tietohallinta

TIINA APPONEN:

Terveystietohallinnon toimikortti
Käyttöönotto Tampereen seudulla

Opinnäytetyö 37 sivua, josta liitteitä 2 sivua
Helmikuu 2012

Kansallinen terveysarkisto koostuu neljästä kokonaisuudesta: Sähköisestä potilastietojärjestelmästä, sähköisestä apteekkijärjestelmästä, sähköisestä potilastietoarkistosta ja potilaan omien tietojen katselusta. Kansallinen terveysarkisto otetaan vaiheittain käyttöön. Julkisella sektorilla sähköinen lääkemääräys otetaan käyttöön Tampereella keväällä 2012, potilastiedon arkisto tulee valmistua vuoteen 2014 mennessä. (Kanta 2012.)

Kansallisen terveysarkiston käyttöönotto on yksi suurimmista tietotekniikan kehityksistä Suomessa. Suomen lait ovat yksi suurimmista syistä, jotka ovat johtaneet kehittämään julkisen sektorin tietojen käsittelyn ja tallennuksen tapoja. Julkinen sektori tulee kohtaamaan suuria muutoksia: Uuden järjestelmän käyttöönoton myötä terveydenhuollon ammattihenkilöt tulee kouluttaa tehokkaampaan tietoturvakäyttäytymiseen, työntekijät tulee kouluttaa uusiin työskentelytapoihin ja potilaita tulee informoida avautuneista mahdollisuuksista seurata omia tietoja.

Kansallisen terveysarkiston suunnittelu ja toteutus on vienyt useita vuosia. Yksi suurimmista syistä on suomalaisuus. Suomalaiset haluavat tuottaa kerralla hyvän ja toimivan järjestelmän. Yhteisen rajapinnan löytäminen kuntien potilastietojärjestelmille on ollut vaikeaa ja aikaa vievää. Pääsääntöisesti jokaisella sairaanhoitopiirillä on oma potilastietojärjestelmänsä. Näiden järjestelmien yhteensopivuus on miltei mahdotonta. Sairaanhoitopiirejä on Suomessa 20 kappaletta. (Suomen Kuntaliitto 2012.)

Opinnäytetyön laatiminen on lähtenyt koulutustarpeesta terveydenhuollon ammattihenkilöille. Tampereen seudun terveydenhuollon piiriin kuuluu noin 5 000 ammattihenkilöä (Karttunen 2012), joiden tulee hallita terveydenhuollon toimikortin käyttö kevästä 2012 alkaen. Koulutusmateriaaliksi on luotu selkeä ja nopealukuinen visuaalinen ohje, joka opastaa terveydenhuollon toimikortin käyttöönotossa ja mahdollisissa ongelmatilanteissa. Kirjallisen ohjeen tueksi on laadittu neljä opetusvideota.

Opinnäytetyön kirjallisen osion pääpaino on tietoturva-asioissa, kansallisen terveysarkiston rakentumisessa, sähköisessä lääkemääräyksessä, sähköisessä allekirjoituksessa ja toimikortin teknisissä ominaisuuksissa. Nämä asiat ovat perustana kansallisen terveysarkiston ja terveydenhuollon toimikortin olemassaololle.

Asiasanat: terveydenhuollon toimikortti, kansallinen terveysarkisto, sähköinen lääkemääräys, sähköinen allekirjoitus, toimikortti

ABSTRACT

Tampere University of Applied Sciences
Degree Programme in Information Technology
Option of Data Management in the Field of Health Care

TIINA APPONEN:
The Health Care Smart Card
The Introduction in the Tampere Region

Bachelor's thesis 37 pages, appendices 2 pages
February 2012

The National Archive of Health Information contains four parts: the electronic prescription, the national pharmaceutical database, the electronic archive of patient records and online access by citizens to their personal prescription and medical data.

The National Archive of Health Information will be published in stages. The electronic prescription will be published in the city of Tampere in the spring 2012. The public sector must be able to use the electronic archive of patient records in 2014. (Kanta 2012.)

The National Archive of Health Information is one of the biggest information technology developments in Finland. The Finnish laws are one of the most important reasons to update public sectors' data handling and saving methods. The public sector will confront big changes: Health care employees need to be educated to use the new system and obey new effective information security, employees need education for new working habits, citizens need to be informed and educated to use online access to their personal prescription.

To plan and implement the National Archive of Health Information took so many years. One of reasons why the implementation did take so many years is the Finnish people way of working: The Finnish people want to build an effective, easy working system – the Finnish people want repair good at once. To find an interface for all the Finnish municipalities' health care systems has been a demanding project. More or less every health care district has its own patient record archive. These data systems hardly communicate together. There are 20 different health care districts in Finland. (Kuntaliitto 2012.)

The purpose of this thesis was to create education material for employees in health care. There are 5 000 health care employees in Tampere surroundings (Karttunen 2012). They have to know how to manage the health care smart card from 2012. The education material contains a manual which is easy to read and fast to learn. The manual will guide the user how to use health care smart card. There are four educational videos to support the manual.

The emphasis of the thesis is on the information security issues, planning and implementing the National Archive of Health Information, the electronic prescription and the health care smart card technical issues. These are the main principles of providing the existence of the National Archive of Health Information and the health care smart card.

Key words: health care smart card, National Archive of Health Information, electronic prescription, electronic signature, smart card

SISÄLLYS

1	JOHDANTO.....	5
2	TIETOSUOJA JA TIETOTURVA	6
	2.1 Tietosuoja.....	6
	2.2 Tietoturva.....	6
	2.3 Lait terveydenhuollon tietoturvan takaajina	8
	2.4 Tietoturva terveydenhuollossa	10
3	KANSALLINEN TERVEYSARKISTO	14
	3.1 Sähköisen potilastiedon arkisto	15
	3.2 Sähköinen lääkemääräys	16
	3.3 Apteekkijärjestelmä	18
	3.4 Kansallisen terveystietojärjestelmän tuomat edut	19
4	TERVEYDENHUOLLON TOIMIKORTTI	21
	4.1 Terveydenhuollon toimikortti	21
	4.2 Varmenne	22
	4.3 Sähköinen allekirjoitus	24
	4.4 Toimikortista yleisesti.....	25
	4.4.1 Toimikorttien turvallisuus.....	28
	4.4.2 Toimikortin lukija	30
5	POHDINTA.....	31
	LÄHTEET.....	34
	LIITTEET	36

1 JOHDANTO

Suomen kehittyvä teknologiaosaaminen on tuonut maallemme mainetta, mutta julkinen sektori on laahannut kehityksen perässä vuosikymmeniä. Viimein julkisella sektorilla saadaan käyttöön yksi suurimmista hankkeista ja kehitysaskelista kohti parempaa tietoturvallista tietojen käsittelyä.

Kansallinen terveystietokanta on kääntänyt terveydenhuollon vanhat käytännöt pääläelle. Mittava muutos tulee vaikuttamaan terveydenhuollon ammattihenkilöstöön ja asiakkaisiin. Lakimäärityksillä turvataan jokaisen kansalaisen tietosuojaterveystietokannan piirissä ja annetaan merkki muuttuvista toimintatavoista – enää ei ole suvaittavaa urkkia. Terveydenhuollon organisaatioissa lokitiedostoja seurataan laissa määrätyn tietosuojavastavien toimista (Tietosuojavastavien toimien kuva, tehtävät ja asema 2010) ja terveydenhuollon ammattihenkilöstöä koulutetaan yhä vaativimpiin tietoturvallesi toimintatavoihin. Perään kuulutetaan yksilön oikeuksia.

Pitkään harkittu, suunniteltu ja vaiheittain rakennettu järjestelmä on valmiina valtakunnalliseen käyttöön. Miten kansallinen terveystietokanta muodostuu? Mikä on terveydenhuollon toimikortti ja miten toimikortti toimii? Lakimääritykset ovat tuoneet tietoyhteiskunnan kehitystä vahvasti eteenpäin ja maailmalla tapahtuneet tietoturvaiskut ovat herättäneet kansalaisten tietouden omasta yksityisyydestään ja sen suojaamisesta.

2 TIETOSUOJA JA TIETOTURVA

Tietoturva-asiat koskevat nykyään jokaista tietokoneen käyttäjää. Yritysmaailmassa ja julkisella sektorilla sähköisen asioinnin lisääntyessä on kiinnitettävä huomio lisääntyviin tietoturvatarpeisiin ja ennaltaehkäistävä mahdollisia tietovuotoja. Yrityksen tulee olla aikaansa edellä tietoturva-asioissa, sillä pienikin virhe yrityksen tallennusjärjestelmässä saattaa aiheuttaa mittavia vahinkoja niin yritykselle kuin yksityiselle henkilölle. Tietoturvaongelmia vastaan on pidettävä kiinni yrityksen tietoturvasuojauksesta ja kouluttaa yrityksen henkilökuntaa käyttämään työvälineitään oikein. Kun mahdolliset puutteet huomioidaan, voidaan ongelmatilanteisiin puuttua ajoissa.

2.1 Tietosuoja

Tietosuoja rakentuu asiakkaan yksityisyyden suojaamiseen ja luottamukseen yrityksen ja asiakkaan välillä. Luottamusta on, että annetut tiedot pysyvät tallessa ja tiedot ovat käytettävissä vain niille määrätyillä henkilöillä.

Seppälän (2011) luentomateriaalin mukaan terveydenhuollossa asiakas- ja potilassuhde perustuu tiedon luottamuksellisuuteen ja salassapitoon. Tarkoituksena on suojata potilaan yksityisyys, edut, oikeusturva ja terveydenhuollon toimintayksikön ja henkilökunnan oikeusturva. Näin ollen varmistetaan potilastietojen hyvä käsittelytapa kaikissa käsittelyn eri vaiheissa. Tietosuojassa ei siis ole ensisijaisesti kyse tietojen konkreettisesta suojauksesta, vaan asiakkaan yksityisyyden suojasta, luottamuksellisesta potilassuhteesta ja eri tahojen oikeusturvasta. Käytännön toimet, joilla tietosuoja toteutetaan, kutsutaan vuorostaan tietoturvaksi. (Seppälä 2011.)

2.2 Tietoturva

Tietosuoja ei voi toteutua ellei tietoturvallisuudesta ole huolehdittu. Tietoturvallisuudella tarkoitetaan tietojen, palvelujen, järjestelmien ja tietoliikenteen suojaamista ja varmistamista niihin kohdistuvien riskien hallitsemiseksi sekä normaali- ja poikkeusoloissa hallinnollisilla, teknisillä ja muilla toimenpiteillä. Onnistunut tietoturva vaatii koko työ-

yhteisöltä paneutumista asiaan ja yhteisiä sovittuja toimenpiteitä. Järjestelmän käyttäjä on suurin uhka laaditulle tietoturvalle. Tietoturvan uhkia ovat mm. käyttövaltuuksien ylittäminen, huolimattomuus, suojausten murtaminen, ylikuormitustilanteet, sähkönsyötön häiriöt, virukset sekä verkon kautta ulkopuolelta tapahtuvat hyökkäykset ja häirinnät. (Tietojärjestelmähankinnat terveydenhuollossa ja sosiaalitoimessa 2008, 30–31.)

Tietoturvan tavoitteena on turvata tietojenkäsittelyn toimivuus erilaisia uhkia vastaan ja suojata tietoja oikeudettomilta muutoksilta. Tietoturvan tavoite ei siis ole pitää tietoja salassa vaan tarkoituksena on pitää annetut tiedot oikeellisina. (Järvinen 2003, 29.) Tietoturva mahdollistaa reaaliaikaisen valvonnan järjestelmän käyttäjiä kohtaan, joka tuo suuren hyödyn: Reaaliaikainen valvonta mahdollistaa nopeat reagoinnit riskeihin ja edesauttavat riskienhallintaa.

Järvinen (2003, 29–34) luettelee tietoturvan kuusi tärkeintä ominaisuutta seuraavanlaisesti:

Luottamuksellisuus

Luottamuksellisuus antaa pääsyn tietoon käsiksi vain niille, joilla on oikeus käsitellä annettua tietoa. Luottamuksellisuuden taustalla on esimerkiksi yrityssalaisuuden suojeleminen.

Eheys

”Tiedot on suojattu oikeudettomilta muutoksilta.” Tiedon täytyy säilyä eheänä käsittelyn, siirron ja tallennuksen ajan. Eheys ja luottamuksellisuus eroavat toisistaan siten, että salattu tieto on siirronkin jälkeen luottamuksellista, vaikka osa tiedosta olisi hävinnyt siirron aikana. Virus saattaa lisätä itsensä lähetettyyn sähköpostiviestiin (virus kotikoneella), jolloin lähetetyn viestin eheys kärsii. Viestin luottamuksellisuus on edelleen taattu, mutta viesti ei ole enää alkuperäisessä muodossaan eli sellaisena kuten viestin oli tarkoitus olla lähetettäessä.

Saatavuus

Salaus ja saatavuus eivät liity toisiinsa. Saatavuus koskee lähinnä materiaa ja teknisyyttä esimerkiksi varmuuskopioita, turvattua sähkönsyöttöä, kahdennettuja levyasemia ja luotettavia verkkoyhteyksiä. Kriittisimmät osat turvataan varajär-

jestelmillä. Saatavuudesta on hyvä käytännön esimerkki: Jos unohdat salasanan, järjestelmän tiedosto ei aukea.

Pääsynvalvonta

Pääsynvalvonnalla valvotaan, että käyttäjä pääsee vain tiettyihin, hänelle ennalta määrättyihin tietoihin käsiksi. Yrityksen työntekijät pääsevät siis käsittelemään samaa tietoa eri tavoin. Tämä tarkoittaa sitä, että henkilö A:lla on oikeus muokata, poistaa ja tallentaa tietoja kun henkilö B:llä on oikeus katsella tietoja.

Kiistämättömyys

Kiistämättömyys tarkoittaa tietojärjestelmissä sitä, että tehtyä toimintoa voidaan tarkastella myöhemmin ja toiminnoista tehdyt merkinnät on tehty luotettavalla tavalla. Sähköinen allekirjoitus perustuu kiistämättömyyteen. Sähköinen allekirjoitus sitoo allekirjoittajan eli allekirjoitusta ei voi perua jälkikäteen eikä sitä voi yrittää siirtää toisen henkilön nimiin.

Todennus

Todennus varmistaa henkilöiden henkilöllisyyden ja tietokoneiden ja ohjelmien aitouden. Todennus on tietoturvan kriittisin ja vaikein osa-alue. Jos todennuksessa on tapahtunut virhe eli ulkopuolinen henkilö on päässyt järjestelmään väärällä henkilöllisyydellä, muilla yllä mainituilla tietoturvan päämäärillä ei ole enää tarvetta.

Mielestäni tietoturvan ongelmana on kuitenkin loppukäyttäjä: Mittavista, aikaavievistä ja kalliista muutoksista ei ole tarvittavaa hyötyä, jos järjestelmän käyttäjä ei toimi tietoturvallisten määritysten mukaisesti. Järvisen mukaan järjestelmän käyttäjä voi toimia kiireessä, välinpitämättömyyden tai osaamattomuuden vuoksi virheellisesti ja aiheuttaa vakavia seurauksia (Järvinen 2003, 29).

2.3 Lait terveydenhuollon tietoturvan takaajina

Suomen voimakkaasti kehittynyt teknologia, kansan valvetuneempi tietoisuus oikeuksistaan ja julkisen sektorin kehitysmuutokset ovat vaatineet uudistuksia lakimääritteitä myöten niin henkilön yksityisyydensuojaan kuin sähköiseen asiointiin.

Terveystietojen tietoturvallisuuden taustalla on monia erilaisia tietoturvavelvoitteita, sillä Suomessa ei ole yhtä tietoturvalakia. Tietoturvaa koskevat säännökset sisältyvät useisiin eri lakeihin. (Laukkanen 2008, 18.) Säännöksiä perustana toimii henkilötietolaki (523/1999), joka antaa ohjenuoran yleisille toimintatavoille.

”Henkilötietolain tarkoitus on toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia henkilötietojen käsittelyssä sekä edistää hyvän tietojenkäsittelytavan kehittämistä ja noudattamista (1§). Henkilötietolaki on yleislaki, jota on noudatettava henkilötietojen käsittelyssä, jollei muualla laissa toisin säädetä.” (Pahlman 2010, 22.)

Henkilötietolaki astuu sivuun muun lain antaessa määreet henkilötietojen käsittelystä. Esimerkiksi julkisuuslaki (621/1999) määrää, että julkiset asiakirjat ovat kaikkien saatavilla. Näin saavutetaan avoimuutta ja hyvää hallintotapaa viranomaisten toiminnassa ja yksityinen henkilö saa mahdollisuuden tarkistaa, valvoa ja vaikuttaa etuuksiinsa. Julkisen lain piiriin eivät kuulu sosiaali- ja terveydenhuollon asiakirjat, sillä asiakirjatiedot ovat arkaluontoisia ja salassa pidettäviä. (Pahlman 2010, 21–22.)

Potilaslaki on astunut voimaan 1.3.1993, joka on määritelty täydentämään muuta terveydenhuollon lainsäädäntöä. Potilaslaki toimii yleislakina potilaan asemasta ja potilaan oikeuksista. Potilaslaki antaa määritelmät potilaasta, terveyden- ja sairaanhoidosta, terveydenhuollon ammattihenkilöstä, terveydenhuollon toimintayksiköistä ja potilasasiakirjoista. (Pahlman 2010, 23 & 785/1992.) Potilaslaki määrää, että terveydenhuollon asiakirjat ovat salassa pidettäviä.

Pahlman kiteyttää potilaslaista, että potilasasiakirja muodostuu potilaan hoidon järjestämisessä ja toteuttamisessa käytetyistä, laadituista tai saapuneista asiakirjoista tai teknisistä tallenteista (mm. laboratorio- ja röntgenläheteet, tulokset, lausunnot, kortistot, atk-tallenteet, ääni-, filmi- ja videotallenteet), jotka sisältävät potilaan terveydentilaa koskevia tai muita henkilökohtaisia tietoja. (Pahlman 2010, 23.)

Potilaslaissa säädetään potilasasiakirjoihin sisältyvien tietojen salassapidosta eli tiedot potilasasiakirjoissa ovat salassa pidettäviä. Salassapitovelvollisuus terveydenhuollossa katsotaan velvollisuudeksi ja sitä on noudatettava. Kaikki terveydenhuollon ammattihenkilöt, jotka osallistuvat potilaan hoitoon suoraan tai välillisesti kuuluvat salas-

sapitovelvollisiin. Salassapitovelvollisuus tarkoittaa vaikenemista kaikista potilaan liittyvistä asioista. (Pahlman 2010, 24.) Yksityisyyden suojaaminen koskee yleistä puhetta potilasasioista (Laukkanen 2008, 17), siksi potilaiden asioista keskustelu on kielletty jos potilaaseen ei ole hoitosuhdetta. Potilaiden asioista keskustelemissa tulee noudattaa hyvän maun sääntöä.

On hyvä huomioda, että vaikka laki kieltää potilaiden yksityisistä asioista keskustelun, on mahdollista saada luovuttaa tietoja eteenpäin. Potilastietolaissa määrätään, että jos potilas tai hänen laillinen edustaja antaa luvan, potilasiakirjojen salassa pidettäviä tietoja voidaan luovuttaa tai jos luovutukseen on lakiin perustuva oikeus. Tosin ns. tarpeettomia potilastietoja ei ole lupa käsitellä eikä luovuttaa, vaikka potilas olisikin antanut luvan. (Pahlman 2010, 25.)

Annetut lakimääritykset määrittelevät vaihe vaiheelta tietosuojakäytäntöjä ja tietosuojan huomioonottamista sähköisessä tiedon välityksessä ja niin yksittäisen henkilön kuin potilaan oikeuksista. Lakien oikeaoppisella noudattamisella saadaan aikaan vahva tietoyhteiskunta, joka mahdollistaa turvallisen tietojen käsittelyn ja välittämisen terveydenhuollon piirissä.

2.4 Tietoturva terveydenhuollossa

Terveydenhuollon suurimpia tietoturvavuotoja ja riskejä ovat olleet potilasasiakirjat, jotka ovat tallennettu paperille. Paperinen potilastietokansio mahdollistaa huomaamattoman urkinnan verrattuna sähköiseen, selailutiedot tallentavaan järjestelmään. Terveydenhuollossa tapahtuneet lakimuutokset ovat tuoneet positiivisen muutoksen vaikka kustannukset ovat olleet korkealla.

Edellä mainituista tietoturvan kuudesta periaatteesta neljällä on tärkeä rooli terveydenhuollon toimikortin toimivuudella: luottamuksellisuus, pääsynvalvonta, kiistämättömyys, todennus. Terveydenhuollon toimikortin käyttöönotolla pyritään ehkäisemään tietoturvariskejä ja pitämään asiakkaiden eli potilaiden tietosuoja järkkymättömänä.

Seppälän (2011) julkaiseman luentomateriaalin mukaan myös hoitohenkilökunnan oikeudet selkiintyvät. Toimikorttia voi verrata esimerkiksi kulkuavaimeen, joka antaa

pääsyn vain ennaltamäärättyihin tiloihin tietyllä käyttäjälle. Terveysthuollon toimintayksikössä määritellään yksityiskohtaisesti jokaiselle terveydenhuollon organisaatiossa työskentelevälle käyttöoikeudet. Tämän johdosta jokaiselle potilaan hoitoon tai siihen liittyviin tehtäviin osallistuvat saavat käsitellä potilasasiakirjoja vain siinä laajuudessa kuin heidän työtehtävänsä ja vastuunsa sitä edellyttävät. (Seppälä 2011.)

Terveysthuollon toimikortti vaatiikin jokaiselta käyttäjältä yksilöinnin ja tunnistautumisen: käyttäjän todennus, esimerkiksi sähköinen allekirjoitus, on juridisesti kiistämätön.

Seppälä (2011) kertoo terveydenhuollon tietoturvan päämääränä olevan varmistus siitä, että kukaan ei pääse käsiksi tietoon, jonka käyttöön henkilöllä ei ole valtuuksia. Näin huomioidaan, että kukaan ei muuta tietoja tai tee toimenpiteitä järjestelmässä, johon henkilöllä ei ole oikeuksia. Sosiaali- ja terveydenhuollon tietojenkäsittelyn erityispiirteitä on, että salassapidettäviä tietoja ei saa luovuttaa tai siirtää ulkopuolisille ilman potilaan allekirjoittamaa kirjallista tai sähköistä suostumusta.

Seppälä tiivistää, että tietojen luovuttajalla on selkeä vastuu: Tietojenluovuttaja vastaa luovutuksen laillisuudesta ja tietojen oikeellisuudesta. Tietojenluovuttamisessa on poistettava mahdollisuus, jolloin ulkopuolinen voi nähdä, selata tai muuttaa tietoja. (Seppälä 2011.)

Seppälä (2011) on luetellut haasteita, jotka tulevat ilmenemään sähköisen potilastietojärjestelmän käytössä:

- Kommunikaatio yli organisaatorajojen ja tietoturva-alueiden välillä on välttämätöntä
- Käyttäjien roolit ja vastuut ovat erilaisia, roolit ja vastuut voivat myös vaihdella tilanteen mukaan
- Potilaan yksityisyys on erittäin tärkeää
- Hoitohenkilökunnalla tulee olla kaikki tarvittava tieto reaaliajassa
- Tiedon suojaaminen ja turvallisuus on kyettävä takaamaan
- Hallinnollinen tietoturva
- Ohjelmistoturvallisuus
- Tietoliikenneturvallisuus, lokit ja valvonta

Haasteet tuovat uusia mahdollisuuksia turvallisuuden takaamiseen ja kehittämiseen. Haasteiden lisääntyessä on annettu laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007) ja laki sähköisestä lääkemääräyksestä (61/2007). Nämä lait edellyttävät, että jokainen sosiaali- ja terveydenhuollon palvelujen antaja, apteekki, Kansaneläkelaitos ja Terveydenhuollon oikeusturvakeskus nimeävät tietosuojavastaavan. (Tietosuojavastaavan toimenkuva, tehtävät ja asema 2010.)

Tietosuojavastaavan tehtävänä on toimia rekisterinpitäjän tukena ja toimia korkealla tasolla organisaatiossa päätösten tekotasolla. Rekisterinpitäjänä voidaan pitää esimerkiksi terveydenhuollon organisaatiota. Tietosuojavaltuutettu nimitetään tehtävään organisaation sisäisesti. Tietosuojavaltuutetun tehtäviin kuuluu yllämainituista haasteista potilaan yksityisyyden suojaamisesta lokien seurantaan. (Tietosuojavastaavan toimenkuva, tehtävät ja asema 2010.)

Kommunikaatio organisaatorajojen yli on aina tietoturvariski vaikka yhteydet olisivat salattuja. Parempaan, tehokkaampaan ja turvallisempaan tietojen siirtoon on pyritty esimerkiksi HL7 –standardilla. Health Level 7 eli HL7-standardi on terveydenhuollon tiedonsiirtostandardi, jonka määrätyksiä noudattamalla eri tietojärjestelmät voivat vaihtaa tietoa keskenään, esimerkiksi laboratoriojärjestelmästä potilastietojärjestelmään. (Tietojärjestelmähankinnat terveydenhuollossa ja sosiaalitoimessa 2008, 36.)

Valitettavasti yksi standardi ei sovi kaikille terveydenhuollon järjestelmille. Rajapintojen etsiminen on ollut aikaa vievä prosessi, sillä poikkeavuudet sovelluksissa ovat olleet merkittäviä. Tietoturva-asioiden ollessa pääprioriteettina ei ole voitu myöskään luoda järjestelmää, joka ei täytä standardin ominaisuuksia.

Järjestelmien yhteensopivuutta olisi pitänyt pohtia jo kaksivuosisikymmentä sitten, jolloin oli ensimmäisiä viitteitä näkyvissä, että suuret pääkoneet tulevat ylikuormittumaan. Samaa havaintoa olisi voitu käyttää terveydenhuollossa, jos tilannetta olisi tarkasteltu pitkän aikavälin tulevaisuuteen. Uutta, alusta loppuun asti rakennettu -järjestelmää ei voida suunnitella, sillä tietoa, jota on vuosia kerätty ei voida enää käyttää. Nyt ongelmana on kehittää tallennustapa, joka pystyy tallentamaan ja siirtämään massoittain tietoa kymmenien vuosien ajan.

Terveydenhuollon toimikortti otetaan käyttöön vähentämään tietojen selailu ja urkinta -väärinkäytöksiä ja parantamaan tiedon eheyden, luottamuksellisuuden ja kiistämättömyyden tunnistamista. Terveydenhuollon toimikortti tuokin käyttöönotossaan monia haasteita ja uhkia.

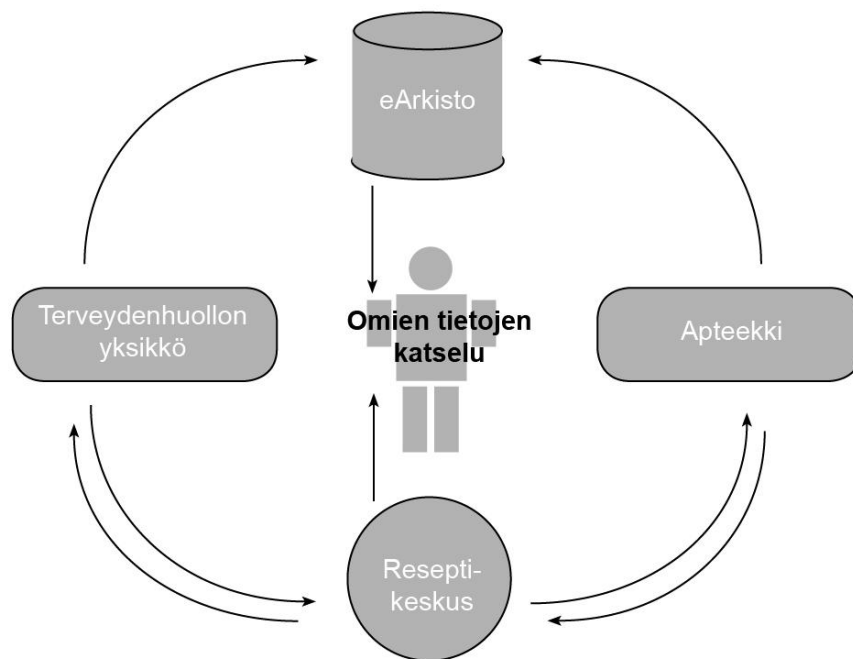
Mahdollisia tietoturvariskejä tulee olemaan mm. toimikortin ja PIN-tunnusluvun luovuttaminen väliaikaiseen käyttöön kollegalle. Tällainen tilanne voi syntyä, kun kollegan toimikortti on unohtunut työpaikan ulkopuolelle. Riskejä kartuttaa PIN-tunnuslukujen säilyttäminen ulkopuolisten näkyvillä työpaikalla ja työpaikan ulkopuolella. Toimikortin unohtaminen toimikortin lukijaan ulkopuolisten saataville voi olla yleisimpiä tietoturvariskejä.

Mahdollisuudet ovat rajattomat pohdiskellessa tietoturvariskejä, jotka voivat liittyä terveydenhuollon toimikortin käyttöön. Näitä mahdollisia ongelmia vastaan on terveydenhuollon henkilökuntaa koulutettava. Koulutus ja muuttuneet järjestelmät tulevat takamaan yhä eheämmän ja luotettavamman tietosuojan potilaalle ja antavat nykyaikaisen kuvan tietoturvakäytännöistä.

3 KANSALLINEN TERVEYSARKISTO

Kansallinen terveysarkisto (KanTa) koostuu neljästä kokonaisuudesta: Sähköisestä potilastietojärjestelmästä, sähköisestä apteekkijärjestelmästä, sähköisestä potilastietoarkistosta ja potilaan omien tietojen katselusta (Kuvio1).

Kansaneläkelaitos on vastuussa Reseptikeskuksesta ja kansallisesta potilastietoarkistosta. Potilastietojärjestelmien tiedot tallentuvat kansalliseen potilastietoarkistoon eli eArkistoon. Apteekkijärjestelmät hakevat tarvitsemansa tiedot Reseptikeskuksesta. Potilaan omien tietojen katselu koostuu eArkiston ja Reseptikeskuksen yhteisistä tiedoista eli potilastietokertomuksista ja sähköisistä lääkemääräyksistä.



KUVIO 1. (Suomen Kuntaliitto 2012, muokattu)

Kansaneläkelaitoksella on suurin rooli valtakunnallisen arkistointipalvelun ja katselupalvelun tarjoajana. Arkistointipalvelu järjestetään Kansaneläkelaitoksen toimesta terveydenhuollon palvelujen tarjoajille ja antajille. Arkistointipalvelu sisältää potilasasiakirjojen säilytyksen ja käytön, hakemistopalvelun potilasasiakirjojen luovutusta varten ja säilytyksen arkistointipalvelussa. (Pahlman 2010, 123.)

Kansallinen terveystietokanta sisältää neljä erilaista palvelua: sähköinen lääkemääräys, potilastietojen sähköinen tallentaminen (eArkisto), potilaan omien tietojen katselu ja potilaan tiedonhallintapalvelu (Sosiaali- ja terveysministeriö 2012). Kansallisen terveystietokannan tehtävänä on luoda yhtenäinen palvelukokonaisuus niin yksityiselle henkilölle kuin hoitohenkilökunnalle.

Vaativia muutoksia on tehty vaiheittain kunnissa, jotta yhteinen koko kansaa palveleva tietoverkosto saadaan käyttöön julkisella sektorilla viimeistään 2014 valtakunnallisen aikataulun mukaisesti (Kansallinen terveystietokanta 2011). Koska uusi järjestelmä on otettu käyttöön vaiheittain, ensimmäiset käyttöönotossa toimineet kunnat ovat olleet pilotointitilassa. Näin on varmistettu, että mahdollisiin toiminnallisiin virheisiin on nopeampaa ja tehokkaampaa puuttua.

Sosiaali- ja terveysministeriön laatimassa oppaassa (Opas sähköisen potilaskertomuksen rakenteesta 2006) on kerrottu sähköisen potilaskertomuksen tuomista eduista. Ote toimii hyvin selitteenä, miksi kansalliseen terveystietokantaan siirrytään:

”Siirryttäessä sähköisen potilaskertomuksen käyttöön on saavutettavissa joukko etuja. Näitä ovat mm. kustannusten säästö, tiedon saatavuus ja jakaminen ajasta ja paikasta riippumatta 24h/7d, työntekijöiden tukeminen sekä uusien toimintamallien ja prosessien mahdollistaminen. Sähköiseen käsittelyyn siirryttäessä on myös varmistuttava siitä, että ratkaisut ovat turvallisia ja luotettavia. Tähän liittyviä uhkia ovat mm. digitaalinen tieto voi korruptoitua, digitaalista tietoa voidaan käyttää, jakaa, kopioida jälkiä jättämättä ja tietokoneviruksista johtuvat haitat.”

Sähköisen asioinnin yleistyessä tulee yllämainittuja asioita huomioida yhtäläisillä kuin rakentaessa koko valtakunnan yhteistä tietopankkia. Kansalliseen terveystietokantaan siirtymisen taustalla ovat lakivelvoitteet. Yhteiskunnan kehittyttyä laajempaan tietoisuuteen tietosuojan merkityksestä, kansalaiset ovat nykyään valvettuneimpia omasta yksityisyydestään. Yritykset ja yksityiset henkilöt osaavat vaatia oikeuksiaan.

3.1 Sähköisen potilastiedon arkisto

Sähköinen potilastiedon arkisto tulee tarjoamaan esimerkiksi sairaaloille, yksityisille lääkäriasemille ja terveyskeskuksille arkistointimahdollisuuden sähköisille potilastiedoille. Sähköistä potilastiedon arkistoa tullaan käyttämään hoitotietojen vaihtamiseen

organisaatorajojen yli. Tämä mahdollistaa nopean tiedon saannin ja oikeiden hoitomenetelmien käyttämisen. Tietojen välitykseen tarvitaan potilaan suostumus. (Kansallinen terveysarkisto 2011.)

Termi sähköinen potilastiedon arkisto (jatkossa eArkisto) tarkoittaa siis muutakin kuin arkistointiominaisuutta. eArkisto on sähköisten potilastietojen valtakunnallinen arkisto, jonka kautta terveydenhuollon organisaatiot voivat tallentaa ja katsella potilastietoja. Tietojen katselu ja siirtäminen mahdollistetaan yhtenäisillä järjestelmien tallennusmetodeilla. Näin tiedot saadaan siirtymään reaaliajassa järjestelmästä riippumatta. Kansallisen terveysarkiston ja eArkiston palveluun kuuluu, että potilas voi katsoa eArkistoon tallennettuja potilastietoja internetin välityksellä. Palveluun kirjaudutaan henkilökohtaisella pankkitunnuksella tai sähköisellä henkilökortilla. (Kansallinen terveysarkisto 2011.)

Palveluntarjoajana Kansaneläkelaitoksen vastuulla on varmistaa, että arkistointipalvelusta ei voida luovuttaa potilastietoja lain vastaisesti ja että luovutuksesta jää tallennettu lokitieto luovutusrekisteriin. Kansaneläkelaitoksella ei ole oikeutta käsitellä potilastietoja laajemmin kuin mitä ylläpidon tehtäviin kuuluu eikä Kansaneläkelaitoksella ole oikeutta määrätä arkistointipalveluun kuuluvista potilastiedoista. (Pahlman 2010, 131–132.)

Jotta potilastietojen luovuttaminen sujuu lainmukaisesti, tulee potilaalta saada suostumus tietojen luovutukseen. Lupa luovutukseen tarvitaan, kun talletettuja tietoja ollaan luovuttamassa toiselle rekisterinpitäjälle. Lupaa ei siis tarvitse anoa silloin, kun kyseessä on rekisterinpitäjä, joka on tallettanut kyseenomaiset potilastiedot. Potilas voi rajata tietojen luovutuksen laajuutta, sillä annettu suostumus on voimassa toistaiseksi ja se kattaa kaikki jo talletetut potilastiedot sekä tulevat talletteet. (Kansallinen terveysarkisto 2011.)

3.2 Sähköinen lääkemääräys

Sähköinen lääkemääräys eli eResepti on lääkemääräys, joka on lääkärin laatima ja hyväksymä. Sähköisen lääkemääräyksen eroavaisuus tavalliseen lääkemääräykseen on, että lääkemääräys tulee olemaan sähköisessä muodossa ja lääkemääräys tallentuu valtakunnalliseen tietokantaan Reseptikeskukseen. Sähköisen lääkemääräyksen käyttöönoton

jälkeen paperinen lääkemääräys poistuu käytöstä. Asiakkaan on kuitenkin mahdollista saada paperinen lääkemääräys lääkärin vastaanotolta poistuttaessa. Sähköisen lääkemääräyksen sisältö on noudettavissa potilaan itse valitsemasta apteekista. Sähköinen lääkemääräys on saatavilla Reseptikeskuksesta 30 kuukauden ajan. (Kansallinen terveystietokanto 2011.)

Muutosprosessia Reseptikeskuksen luontiin valvotaan tarkoin lakimäärittein. Laissa määrätään, että niin potilastietojen kuin sähköisten lääkemääräyksiä katseluun organisaatiosta riippumatta tarvitaan hoitosuhde tai potilaan suostumus (785/1992).

Kansaneläkelaitoksen (2011) julkaisemassa julkaisussa kerrotaan, että jos potilas haluaa, voidaan sähköinen lääkemääräys jättää tallentamatta Reseptikeskukseen. Potilaalla on oikeus kieltäytyä sähköisestä lääkemääräyksestä ilmoittamalla siitä hoitavalle lääkärille lääkemääräyksen kirjoittamisen yhteydessä. Tällaisessa tilanteessa potilas saa puhelinlääkemääräyksen tai paperilääkemääräyksen, koska niitä ei tallenneta sähköiseen muotoon Reseptikeskukseen.

Reseptikeskuksen käyttöönotossa toimitaan samoin kuin kansallisen terveystietokannan kanssa, eli käyttäjältä vaaditaan sähköinen tunnistautuminen ja sähköinen allekirjoitus. Näillä toiminnoilla varmistetaan, että lääkkeen määränneellä ja toimittaneella henkilöllä on ammattihenkilölakiin perustuva oikeus määrätä tai toimittaa lääkkeitä. Tämä koskee myös hammaslääkärin ja sairaanhoitajan virkaa. (Sähköinen lääkemääräys vaatimusmäärittely 2011, 9.)

Sähköinen lääkemääräys tulee ehkäisemään lääkkeiden haitallisia yhteisvaikutuksia sekä tulee poistamaan lääkkeiden väärinkäytöksiä. Sähköiset lääkemääräykset ovat helpommin valvottavissa, sillä lääkemääräykset tallentuvat valtakunnalliseen palvelimeen – näin poistetaan ongelma lääkemääräyksiä haitallisesta väärinkäytöstä ja tahallinen saman lääkemääräyksen uusiminen eri lääkäreiden vastaanotolla.

Paperisten lääkemääräyksiä seuranta on ollut mahdotonta yhtenäisen tietopalvelujärjestelmän puuttuessa (esimerkiksi lääkemääräyksiä päällekkäisyys eli ns. ”tuplalääkitys”). Paperisen lääkemääräyksen väärinkäyttö on ollut mahdollista (väärennös, lääkkeen kaksinkertaiset annostukset, ristiin lääkintä). Sähköinen lääkemääräys tuleekin vähentämään mahdollisen lääkkeiden väärinkäytön.

Reseptikeskuksen käyttöönotto tuo mukanaan uusia käytäntöjä. Aikaisemmin potilaan on pitänyt itse huolehtia lääkemääräyksen uusimisesta tai mahdollisesti potilas on voinut sopia apteekin kanssa erillissopimuksen, jolloin apteekki huolehtii reseptien uusinnasta. Reseptikeskuksen tuoma muutos on hyvin käytännöllinen. Kansaneläkelaitoksen (2011) julkaisun mukaan apteekki lähettää uusimispyynnön potilaan ilmoittamaan terveydenhuollon yksikköön. Osoitetun terveydenhuollon yksikön ei tarvitse olla sama yksikkö, jossa potilas on asioinut hakiessaan lääkemääräystä. Uusimispyyntö siirtyy apteekista Reseptikeskukseen, josta lääkemääräys siirtyy terveydenhuollon organisaation potilastietojärjestelmään. Potilaan on edelleen mahdollista uusia lääkemääräys asioidessaan terveydenhuollon yksikössä. Näin toimiessa tallennetaan potilastietojärjestelmään pyyntö uudistaa potilaan tarvitsemat sähköiset lääkemääräykset.

Sähköisestä lääkemääräyksestä annetaan potilaalle mukaan potilasohje, joka sisältää tiedot kirjoitetusta sähköisestä lääkemääräyksestä. Potilasohje luodaan Reseptikeskuksen tietojen perusteella. Joissain tapauksissa potilastietojärjestelmä tulostaa potilasohjeen Reseptikeskuksen muodostaman tiedoston pohjalta. (Sähköinen lääkemääräys vaatimusmäärittely 2011, 17, 20.)

3.3 Apteekkijärjestelmä

Apteekkien toiminta eli sähköisten lääkemääräyksien käsittely tapahtuu apteekkijärjestelmässä. Apteekkijärjestelmä hakee sähköiset lääkemääräykset Reseptikeskuksesta ja tallentaa Reseptikeskukseen apteekin tekemät toimitusmerkinnät. Reseptikeskukseen ei tallenneta paperi-, faksi- tai puhelinreseptejä ja niiden toimituksia eli luovutuksia asiakkaalle. (Sähköinen resepti apteekissa 2009.)

Apteekkien ja Reseptikeskuksen välinen tiedonsiirto on salattu. Apteekissa varmistetaan aina lääkkeen määrääjän oikeus laatia lääkemääräys ja lääkkeen toimittajan henkilöllisyys. (Reseptin toimitus 2011.) Asiakas voi noutaa lääkärin määräämän sähköisen lääkemääräyksen valitsemastaan apteekista. Lääkkeen toimittajalla tarkoitetaan farmaseuttia tai proviisorita (Sähköinen resepti apteekissa 2009).

Julkaisussa kerrotaan, että järjestelmään pääsee vain kirjautumalla myönnettyllä ammatikortilla, jolloin järjestelmän käyttö täyttää tietoturvallisuuden kriteerit. Farmasian

opiskelijoilla on vähemmän käyttöoikeuksia apteekkijärjestelmässä. Farmasian opiskelijan toiminnot annetaan farmaseutin tai proviisorin hyväksyttäväksi, jonka jälkeen toiminnot voivat siirtyä eteenpäin.

Apteekit noudattavat tarkkoja toimintaohjeita sähköisen lääkemääräyksen luovuttamisessa asiakkaalle. Farmaseutilla ja proviisorilla on terveydenhuollon varmentajan myöntämä ammattikortti, joka on farmaseutin tai proviisorin henkilöllisyyden ja oikeudellisuuden varmistaja käyttää apteekkijärjestelmää. Valtakunnalliseen järjestelmään pääsee kirjautumaan vain ammattikortilla. Ammattikortti toimii siis henkilön tunnistajana ja sähköisen allekirjoituksen laatijana. (Sähköinen resepti apteekissa 2009.) Ammattikortti on ajaa saman toimintaperiaatteen kuin terveydenhuollon toimikortti.

Ennen lääkkeen luovuttamista asiakkaalle apteekkijärjestelmä tarkistaa, että lääke löytyy Lääketietokannasta ellei lääke ole apteekissa valmistettu. Lääketietokanta sisältää lääkkeen määräämisen ja toimittamisen kannalta keskeiset lääketiedot (hintaa, korvattavuus, lääkevalmisteen vaihtokelpoisuus, korvattavat perusvoiteet, kliiniset ravintovalmisteet). (Sanasto, Kansallinen terveysarkisto 2010.) Toimitus eli lääkkeen luovuttaminen asiakkaalle allekirjoitetaan sähköisesti.

3.4 Kansallisen terveysarkiston tuomat edut

Valtakunnallista järjestelmää suunniteltaessa on ollut huomioitava, että esimerkiksi potilastietoja säilytetään potilaan koko eliniän hoitotapahtumasta lähtien ja kymmenen vuotta potilaan kuolemasta. Potilasasiakirjoja käytetään myös tutkimukselliseen analysointiin, joiden aineistolla on eri säilytysmääritteet. Koska jokaisesta kansalaisesta tullaan tallentamaan kaikki terveydelliset tiedot sähköiseen muotoon, tulee suurkoneiden tallennuskapasiteetti olla mittava ja laadullisesti eheä vuosikymmenten ajan.

Valtakunnallinen terveysarkisto tuo tullessaan positiivisia muutoksia: Monimutkaisten lakimääritteiden tarkoituksena on ollut kehittää ja parantaa potilastietojen tallennus, muokkaus, siirto ja säilyttämismahdollisuutta. Terveydenhuollon henkilökunnan lisäksi myös kansalaisille tarjotaan nykyaikainen tapa katsella omia potilastietoja reaaliaikaisesti.

Seppälän (2011) luentomateriaalissa on tuotu esille terveydenhuoltolain (1326/2010) tuomat muutokset yksinkertaistettuna:

- Sairaanhoidopiirin sisällä olevat eri rekisterit muodostavat alueen yhteisen potilasrekisterin
- Tietojen saatavuuden tulisi parantua sairaanhoidopiirin sisällä
- Potilaan suostumusta tietojen luovuttamiseen ei pääsääntöisesti tarvita sairaanhoidopiirin sisällä
- Tietotekniset vaatimukset tietojen luovutukselle eivät varsinaisesti muutu

Kansallinen terveystietokanto mahdollistaa potilaan tietojen katselun toisella paikkakunnalla terveydenhuollon organisaatiosta riippumatta. Kun potilastietoja katsellaan toisessa terveydenhuollon organisaatiossa tarvitaan katseluun potilaan suostumus. Myös luovutuksen pyytäjä, joka on hoitosuhteessa potilaan kanssa, on varmistettava tietoteknisesti. (Seppälä 2011.)

Kun potilaan suostumus on saatu, pystytään saaduilla tiedoilla helpottamaan työskentelyä potilaan hyväksi ja saavutetaan nopeampien hoitopäätösten tekeminen. Potilaalle pystytään antamaan oikeanlaista hoitoa, kun potilastietokertomukset ovat heti saatavilla.

Uudistuksen myötä potilaan vastuu omasta hoidosta vähenee. Potilaalla on erilaisia potilastietokertomuksia eri terveydenhuollon organisaatioissa, jolloin lääkäri on joutunut luottamaan potilaan suusanalliseen potilastietokertomukseen hoidoista, joita potilaalle on tehty.

Kansallisen terveystietokannan luomiseen on kulunut erilaisten tietolähteiden mukaan miljoonia euroja. Kalliin ja pitkäkestoisen hankkeen viimein ollessa lähellä käyttöönottoa olen vakuuttunut, että nykyaikainen työskentelyväline tulee olemaan korvaamaton.

4 TERVEYDENHUOLLON TOIMIKORTTI

4.1 Terveystenhuollon toimikortti

Lakimäärityksien ja kansallisen terveystarkiston myötä terveydenhuollon potilastietojärjestelmään kirjautuminen tulee muuttumaan. Tietoturvallisten muutosten edetessä, on valtakunnallisesti siirrytty sähköisen varmenteen ja terveydenhuollon toimikortin käyttöön. Vahva tunnistautuminen on edellytyksenä tietoturvalisuuden ja tietosuojan toteutumiselle.

Tampereen seudun terveydenhuollon organisaatioissa otetaan käyttöön terveydenhuollon toimikortti kevään 2012 aikana (Tampereen kaupunki 2012). Terveystenhuollon toimikortti mahdollistaa pääsyn potilastietojärjestelmästä kansalliseen terveystarkistoon ja Reseptikeskukseen hyväksytyn kirjautumisen jälkeen.

Terveystenhuollon toimikortti sisältää terveydenhuollon ammattihenkilön tiedot, jotka haetaan valtakunnallisesta Terhikki-palvelusta. Terhikki-palvelu on terveydenhuollon ammattihenkilöiden keskusrekisteri. Jokainen terveydenhuollon ammattilainen varmentetaan, eli heidän tiedot tarkistetaan ja henkilöt todennetaan ennen toimikortin luovuttamista haltijalle. (Väestörekisterikeskus 2011.)

Terveystenhuollon toimikorttia voi käyttää vain tunnuslukujen PIN1 ja PIN2 kanssa, jotka annetaan ammattihenkilöiden käyttöön. Terveystenhuollon toimikortin tunnusluvut, PIN1- ja PIN2-tunnusluku, kysytään jokaisen järjestelmään kirjautumisen aikana ja eri käyttötilanteissa. Toimikortin tunnusluku ei tallennu järjestelmään. Terveystenhuollon ammattihenkilöllä on oikeus muuttaa tunnusluvut itselleen sopiviksi tietoturvallisiksi tunnusluvuiksi annettujen ohjeiden mukaisesti.

Terveystenhuollon toimikortin sisältämä varmennekäytäntö takaa tietoturvallisen lähtökohdan potilaiden sähköisten asiakirjojen käsittelyyn ja tiedon siirtoon verkon yli. Varmente on terveydenhuollossa toimivien henkilöiden luotettava tunnistautuminen ja sisältää sähköisen allekirjoituksen. Väestörekisterikeskuksen julkaisu täsmentää, että terveydenhuollon varmennekortteja eli toimikortteja ovat ammattikortti, henkilöstökortti, toimijakortti ja varakortti (Väestörekisterikeskus 2011). Vaatii tarkkuutta erottaa toimi-

kortit toisistaan, sillä eri terveydenhuollon ammattinimikkeellä on erilaiset toimikortit käytössä.

Terveydenhuollon toimikorteille rakennetaan valtakunnallinen sulkulista. Sulkulista on järjestelmä, johon kootaan ja ilmoitetaan varmenteet, jotka ovat joutuneet ulkopuolisen käsiin tai kun terveydenhuollon toimikortti on hukkunut. Sulkulistalta löytyvät ne varmenteet, jotka ovat esimerkiksi toimikortin katoamisen vuoksi suljettu pois käytöstä. Vain sulkulistalle ilmoitetut toimikortit vapauttavat toimikortin haltijan oikeudellisesta vastuusta. (Väestörekisterikeskus 2011.)

Tampereen terveydenhuollon alueella sulkulista toimii samalla periaatteella: Jos toimikortin haltija huomaa, että toimikorttia on käyttänyt toinen osapuoli tai toimikortti on anastettu, tulee toimikortin haltijan ilmoittaa mahdollisesta rikkeestä välittömästi organisaation rekisteröintipisteeseen tai valtakunnalliseen sulkupalveluun.

4.2 Varmenne

Väestörekisterikeskus on toiminut 19.11.2010 lähtien terveydenhuollon valtakunnallisena valvontaviranomaisena. Väestörekisterikeskuksen tehtävä on hoitaa terveydenhuollon palvelujen antajien sekä näiden palvelujen antamiseen osallistuvien henkilöiden ja tietoteknisten laitteiden varmennepalvelua. Tähän kuuluvat tunnistamisessa, todentamisessa ja sähköisessä allekirjoittamisessa tarvittavat varmenteet ja näihin liittyvät palvelut. (Pahlman 2010, 130.)

Väestörekisterikeskus toimii varmennerekisterin rekisterinpitäjänä. Varmennerekisteriä pidetään Väestörekisterikeskuksen myöntämistä henkilövarmenteista, vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista (983/2010).

Varmenteen käyttäjästä oletetaan, että hänen tiedot ja käyttöoikeudet ovat tarkistettuja ja ne ovat oikeanmukaiset. Myös varmenteen myöntäjään suhtaudutaan luottamuksellisesti eli varmenteen myöntäjän toimia ei kyseenalaisteta. (Järvinen 2003, 159.)

Järvisen (2003, 159–160) mukaan varmenteeseen voidaan luottaa, kun alla luetellut seikat toteutuvat:

- Varmenteen myöntäjä on luotettava:
Ollaan varmoja siitä, että varmenteen myöntäjä on tarkistanut tietojen aitouden ennen varmenteen myöntämistä.
- Varmenteen myöntäjän yksityinen avain on pysynyt ja pysyy salassa:
Ulkopuolinen hyökkääjä pystyy huomaamatta luomaan väärennettyjä varmenteita, jos varmenteen myöntäjän avain saadaan haltuun.
- Varmenteen myöntäjän julkinen avain on saatu luotettavalta taholta:
Jos julkinen avain on saatu epäluotettavalta taholta, on varmenteen myöntämien varmenteiden aitous ja väärinkäyttö mahdollista.
- Varmenteessa käytetty salaustekniikka on riittävän turvallista:
Algoritmien ja salauspituuksien tulee olla tietoturvallisia.

Sähköinen todistus on varmenne eli sertifikaatti. Sähköinen todistus sisältää erilaisia tietoja, jotka on varmennettu eli tarkistettu oikeiksi luotettavan varmenteen myöntäjän taholta. Varmenteen käyttöön tarvitaan julkinen avain, joka purkaa varmenteeseen sisällytetyn tiedon ja tarkistaa, että varmenteessa oleva tieto on aito ja luotettava. Varmenne on siis kahden todennetun asian liittämistä yhteen: todennetulla haltijalla (eli käyttäjällä) on avain, jolla varmennetta voidaan käyttää. Varmenteella on kolme päätehtävää: todentaa varmenteen haltijan identiteetti, suorittaa allekirjoitus yksityisellä avaimella ja purkaa salattuja viestejä julkisella avaimella. (Järvinen 2003, 159–160.)

Monitahoisen aitouden varmistamisen vuoksi varmenteet ovat monikäyttöisiä ja niihin luotetaan. Kun varmennetta käytetään, on tietojen todistaminen oikeaksi turvallisempaa ja osapuolten identiteetistä voidaan olla varmoja. (Järvinen 2003, 160.)

Liikenne- ja viestintäministeriön julkaisussa kerrotaan, että julkisen avaimen menetelmä (PKI = Public Key Infrastructure) on perustana varmennepohjaiselle tunnistusmenetelmälle. Menetelmällä generoidaan kahdesta avaimesta koostuva avainpari: Julkinen avain (avainpari 1) on kaikkien nähtävillä, yksityinen avain (avainpari 2) on vain haltijan tiedossa.

Yksityisellä avaimella salataan tietoa. Kun tieto on purettu onnistuneesti julkisella avaimella, voidaan olla varmoja siitä, että alkuperäisen tiedon salanneella taholla on ollut hallussaan avainparin yksityinen avain. Tästä menetelmästä muodostuu sähköinen allekirjoittaminen ja allekirjoituksen tarkastaminen. Jotta menetelmä pysyy luotettavana on yksityinen avain pysyttävä vain haltijan tiedossa.

Liikenne- ja viestintäministeriön julkaisun mukaan yksityiselle avaimelle on luotu suojaus, jolla yksityistä avainta ei pystytä kopioimaan tai lukemaan. Suojauksen tarkoituksena on lukittaa yksityinen avain niin, että sillä pystytään tekemään toimenpiteitä. Varmenne toimii yksityisen avaimen luotettavuuden mittarina. Varmenne toimii tutkitusti vahvana saavutettuna tietoturvana. Laatuvarmenne ja varmenne ovat perustana luotettavuudelle, tunnistautumiselle ja juridisesti kiistämättömälle sähköiselle allekirjoitukselle. (Sähköisen tunnistamisen menetelmät... 2003, 11, 30.)

4.3 Sähköinen allekirjoitus

Sähköinen allekirjoitus on osa kansallisen terveysarkiston tuomia muutoksia. Kansalliseen terveysarkistoon ja Reseptikeskukseen kirjaudutaan terveydenhuollon toimikortilla. Terveydenhuollon toimikortti on varmentaja käyttäjän henkilöllisyydestä ja oikeudellisuudesta, mutta se toimii myös kiistattomana sähköisen allekirjoituksen välittäjänä.

Vahvan sähköisen tunnistamisen ja sähköisen allekirjoituksen laki (617/2009) tuli voimaan vuonna 2009. Laki sisältää muun muassa säännökset vahvan sähköisen tunnistamispalvelun tarjoajaan ja sen tarjoamaan palveluun kohdistuvasta vaatimuksista. Vahva sähköinen tunnistaminen kohdistuu luonnollisten henkilöiden tunnistamiseen.

Liikenne- ja viestintäministeriön julkaisun mukaan sähköisten allekirjoitusten avulla pystytään tehostamaan sähköistä asiointia verkon yli. Sähköisen allekirjoituksen vahvuutena on kiistämättömyys, joka varmistaa allekirjoittajan identiteetin. Ollakseen varmoja allekirjoittajan identiteetistä, tulee sähköinen allekirjoitus olla tehty välineellä, joka voi olla vain käyttäjän omassa hallinnassa. Näin sähköisen allekirjoituksen tekijä ja allekirjoitettu tieto yksilöidään. (Turvalliset sähköisen allekirjoituksen... 2004, 9.)

Sähköinen allekirjoitus on juridisesti yhtä pätevä ja kiistämätön kuin kynällä allekirjoitettu sopimus, asiakirja, lääkärintodistus tai sähköinen lääkemääräys. Sähköinen allekirjoitus on teknisesti tunnistamista monimutkaisempaa: Tunnistamisella tarkoitetaan käyttäjän tunnistamista nimen tai asiakasnumeron perusteella. Tunnistamiseen käytetään esimerkiksi käyttäjätunnusta. Todennus vuorostaan tarkoittaa sitä, että käyttäjä todennetaan oikeaksi eli henkilö on se kuten väittääkin olevansa. Todennuksena käytetään esimerkiksi salasanaa. (Järvinen 2003, 204, 206.)

Koska sähköinen allekirjoitus on oikeudellisesti pätevä, toimikortin haltijaa sitoo vastuu allekirjoitetuista sähköisistä asiakirjoista, vaikka haltija haluaisikin kiistää ne. Toimikortin, niin terveydenhuollon kuin muun yleisen sektorin, haltijan vastuulle siirtyvät myös sähköiset allekirjoitukset, jotka on suoritettu ilman haltijaa haltijan nimissä. Tämä tarkoittaa sitä, että jos toimikortti varastetaan tai se joutuu ulkopuolisen käsiin, on toimikortin haltija niin kauan vastuussa toimikortilla tapahtuvista tapahtumista kunnes toimikortin haltija ilmoittaa toimikortin sulkulistalle. (Järvinen 2003, 209.)

Terveydenhuollon toimikortin sähköistä allekirjoitusta käytetään sähköisen dokumentin, (sähköisen lääkemääräyksen, lääkärintodistuksen) allekirjoittamiseen ja aitouden todentamiseen. Terveydenhuollon toimikortin sähköinen allekirjoitus tapahtuu valitussa potilastietojärjestelmässä PIN2-tunnusluvulla.

4.4 Toimikortista yleisesti

Terveydenhuollon toimikortti on yleinen toimikorttimalli, jonka standardikoko on ID-1. Standardikoko vastaa luottokortin ja pankkikortin kokoa. Toimikortti säilyttää varmenteet upotetulla mikropiirillä eli sirulla. Mikrosiru on tuttu matkapuhelinten SIM-kortista. Mikrosirua voisi verrata tietokoneeseen: Mikrosiru sisältää prosessorin, monenlaista muistia sekä väylän tietoliikennettä varten. Mikrosirun ympärillä oleva PVC-muovi on käytön helpottamista varten. Toimikortin käyttäminen olisi vaikeaa, jos mikrosirun ympärillä ei olisi muovikorttia.

Toimikortin siru muotoutuu kahdeksasta pienestä palasta, eli kontaktinastasta, yhdeksi kokonaisuudeksi. Toimikortin siru kytkeytyy toimikortin lukijaan kahdeksalla kontaktinastalla. Kun toimikortti laitetaan lukijaan, toimikortin prosessori aktivoituu toimin-

toon sähkönsyötön ja kellopulssin jälkeen. Nasta numero seitsemän on tietoliikenteen yhdistäjänä eli keskustelijana toimikortin ja isäntälaitteen välillä (Kuvio 2).

Kahdeksan kontaktinastan järjestys on määritelty ISO 7816 -standardiperheessä. Kahdeksasta nastasta kuusi on käytössä ja kaksi on jätetty vapaiksi mahdollisia tulevaisuudessa tapahtuvia laajennoksia varten (nastapaikat 4 ja 8). (Järvinen 2003, 173–174.)

Käyttöjännite 1	Vcc		GND	5 Maa
RESET (nollaus) 2	RST		Vpp	6 EEPROM-muistin ohjausjännite
Kellosignaali 3	CLK		I/O	7 I/O-väylä (tiedonsiirto)
Varattu (vapaa jatkokäytölle) 4	RFU		RFU	8 Varattu (vapaa jatkokäytölle)

KUVIO 2. (Järvinen 2003, 174)

Toimikortin siru sisältää erilaisia muistipaikkoja eri käyttötarkoituksia varten: Vakiosovellukset ja käyttöjärjestelmä ovat ROM-muistissa (Read-Only Memory). ROM vie vähiten tilaa piisirulla ja on kustannuksellisesti halvin toteuttaa. RAM (Random Access Memory) toimii työmuistina eli muistia käytetään lähinnä välitulostusten tallentamiseen käsittelyn aikana. RAM vie kymmenkertaisesti enemmän muistin tilaa kuin ROM ja nelinkertaisesti EEPROM:n (Electrically Erasable Programmable Read Only Memory) verrattuna – siksi RAM:n tyypillinen käyttökoko on parista kilotavusta kymmeneen kilotavuun. (Järvinen 2003, 175 & Rinne 2002, 29.) RAM pystyy suoriutumaan perussovellusten käyttötarpeista helposti, mutta siirryttäessä vaativimpiin sovelluksiin loppuu RAM:n kapasiteetti kesken. (Rinne 2002, 29.)

PROM-muisti ei ole saanut menestyksellistä asemaa toimikorttien käyttöönotossa. Dataa viedään PROM-muistiin (Programmable Read-Only Memory) valmistusvaiheen jälkeen. PROM-muistiin voidaan siis tallentaa jälkeinpäin dataa, mutta dataa ei pystytä enää poistamaan PROM:sta. PROM-muistia kannattanee käyttää ennemmin tallennuspaikkana esimerkiksi salausavaimille. (Rinne 2002, 30.)

Toimikortin valmistuksen yhteydessä luodaan EEPROM-muistialue, joka jätetään myöhemmää käyttötarvetta (talletettavaa dataa) varten tyhjäksi. EEPROM-muistin tallennus-

ja poistokerrat on rajoitettuja. Muistin tallennuskyky vähenee sitä mukaa kuin ohjelmointioperaatio lisää muistille talletettujen elektronien määrää. Jossain kohtaa kirjoitus- ja poistokertojen jälkeen elektronien määrä on kasvanut niin suureksi, että muistin sähkömagneettiset ominaisuudet ei enää kykene toteuttamaan ohjelmointioperaatioita. EEPROM-muisti on kallein käytettävistä muistialueista. EEPROM-muistin osuus määrittelee toimikortin kokonaishinnan. (Rinne 2002, 30.)

Rinne (2002) kertoo, että toimikorttien taustalla toimii ISO 7816-4- standardi. Standardi määrittelee hierakkisen tiedostorakenteen ja komentokielen, jolla hallitaan tiedostoja ja hakemistoja. Tiedostoilla on kaksi luokkaa: Hakemistotiedosto (DF, dedicated file) ja datatiedostot (EF, elementary file). Jokaisella toimikortilla on yksi juurihakemisto (MF, master file). Datatiedostot on jaettu kahteen omaan luokkaan: sisäiseen datatiedostoon (internal EF) ja työtiedostoihin (workin EF). Korttisovellusten ja käyttöjärjestelmien käyttämä tieto talletetaan sisäisiin datatiedostoihin. Näihin tiedostoihin talletetaan myös tiedot, joita ei käytetä tai siirretä toimikortin ulkopuolelle, esimerkiksi kryptofunktioihin käytettävät avaimet tai sovelluskoodit. Työtiedostoihin talletetaan vuorostaan tietoa, joka on siirrettäväksi toimikortin ulkopuolelle esimerkiksi toimikortin lukijalle lähetettävät komennot. Näitä komentoja tai komentojen vasteita ovat esimerkiksi sähköinen allekirjoitus. Sähköinen allekirjoitus muodostuu toimikortin sisällä ja se lähetetään tarkistettavaksi allekirjoituksen vastaanottajalle. (Rinne 2002, 33.)

Yksityinen avain jää sirun sisälle, kun toimikorttia käytetään. Julkinen avain luetaan vuorostaan toimikortilta ulos. EEPROM-muistiin kirjoitetaan kortin tiedot varmenteeksi. (Järvinen 2003, 176.)

Järvinen (2003) kertoo myös, että toimikortti sidotaan haltijaansa PIN-tunnusluvulla. Toimikortilla suoritettavat operaatiot vaativat käynnistykseen PIN-tunnusluvun syöttämisen. Oikein syötetyn PIN-tunnusluvun jälkeen sirun salausprosessori suostuu käsittelemään saamiaan tietoja. Toimikortti lukkiutuu viiden väärän PIN-tunnusluvun syöttämisen jälkeen, jonka jälkeen lukkiutunut toimikortti pystytään avaamaan kahdeksan numeroisella PUK-avaustunnusluvulla. (Järvinen 2003, 176.)

4.4.1 Toimikorttien turvallisuus

Järvisen mukaan toimikorttien turvallisuuden suurin haittatekijä on käyttäjä itse. Toimikorttien valmistus on toteutettu niin ettei yksityistä avainta tulisi voida paljastaa mikroskoopilla tutkimalla tai huijaamalla ulkoisilla häiriötekijöillä. (Järvinen 2003, 177.) Siksi on helpompaa yrittää saada toimikortin haltijan tunnusluku käyttöön kuin hakkeroida toimikortti.

Rinne (2002) vuorostaan kertoo julkaisussaan, että toimikortin yksinkertaisella rakenteella ja pienellä kapasiteetilla on helpompi saavuttaa vahvempi tietoturvallisuus kuin muilla tietokonetyypeillä. Rinteen mukaan toimikorteille asetetaan suuria tietoturvalisuuden odotuksia.

Rinne (2002) jatkaa, että toimikortin tietoturvaluuteen voidaan vaikuttaa jo suunnittelu- ja kehitysvaiheessa. Mikroprosessorin ja käyttöjärjestelmän koodin tulee olla virheetöntä ja noudattaa korkeaa laatua kaikissa työn etenemisen vaiheissa. Toimikorttien mikroprosessori- ja käyttöjärjestelmäkehityksessä ns. takaportteja ei käytetä. Takaportteja jätetään eri käyttöjärjestelmien mahdollisia huoltotöitä varten.

Tietoturvahyökkäykset toimikorttia kohtaan kohdistuvat lähinnä mikroprosessoriin, muisti- ja osoiteväyliin tai suoraan muistialueisiin. Näiden alueiden tietoturvahyökkäykset vaativat erikoisvälineitä ja syvällistä tuntemusta mikroprosessorien tekniikasta ja rakenteesta.

Rinne (2002) kertoo, että hyökkäysmenetelmät ovat vaikea taseisia: Muistin sisällön muuttaminen on mahdollista valaisemalla prosessoria voimakkaalla ultraviolettivalolla. Tällaisen operaation onnistuminen vaatii äärettömä tarkkuutta, sillä ultraviolettivalo tulee saada kohdistettua esimerkiksi tiettyyn muistiosoitteeseen. Ultraviolettihyökkäyksessä tulee löytää oikea muistiosoite, joka on äärettömän vaikeaa: Hyökkäystä muistialueita vastaan on suojauduttu peittävillä kerroksilla, jotka vähentävät ultraviolettivalon vaikutusta muistisoluihin.

Vaikka hyökkäykset kuulostavat maalaisjärjellä äärettömän vaikeilta, aikaa vieviltä ja jopa mahdottomilta toteuttaa, on hyökkäyksiä varten suojauduttava. Jos hyökkääjä nä-

kee hyökkäyksen onnistumisella tarpeeksi suuren arvon, hyökkäys tullaan toteuttamaan – riippumatta kuinka paljon se maksaa ja vie aikaa. (Rinne 2002, 63, 65–67.)

Linden (2002) on jakanut toimikortteja vastaan tehdyt hyökkäykset neljään eri osaan:

Anturointi:

Anturointi on aktiivinen hyökkäys, joka suoritetaan erikoistyyvälinein varustetussa laboratoriossa ja jossa toimikortin sirua manipuloidaan fyysisesti. Siru irrotetaan kortista ja sitä suojaavat kerrokset poistetaan typpihapolla. Tämän jälkeen sirun arkkitehtuuria voidaan tutkia mikroskoopilla ja sen väylien signaaleja mitata ja muuttaa mikroanturilla. Tarvittavien välineiden hinnat alkavat käytettyinä kymmenestä tuhannesta eurosta. Monimutkaisemmilla välineillä, kuten fokusoidulla ionisuihkulla (focused ion beam, FIB) päästään käsiksi myös syvemmällä sirussa oleviin johtimiin.

Ohjelmistohyökkäys:

Ohjelmistohyökkäykset ovat passiivisia hyökkäyksiä, jotka eivät vahingoita sirua. Toimikorttisovelluksen käyttämistä tietoturvaprotokollista, salausalgoritmeista ja niiden toteutuksista etsitään virheitä ja heikkouksia, jotka avaavat hyökkääjälle esimerkiksi pääsyn toimikortin sisältämiin tietoihin.

Signaalien kuuntelu:

Signaalien kuuntelu kiinnittää huomiota toimikortin kontaktipintojen signaalien analogisiin ominaisuuksiin ja prosessorin tuottamaan sähkömagneettiseen säteilyyn. Toimikortin virrankulutuksesta ja sen muutoksista voidaan edullisissa olosuhteissa tehdä päätelmiä toimikortin sisäisestä rakenteesta ja toiminnasta sekä sen käsittelemästä tiedosta.

Virheiden generointi:

Virheiden generoinnissa toimikortin kontaktipintojen signaaleihin aiheutetaan transientteja, jotka ovat nopeita muutoksia esimerkiksi toimikortin analogisissa signaaleissa, kuten kello- ja virtasignaaleissa. Sopivalla tavalla valittu transientti saattaa johtaa hyökkääjän tavoittelemaan vikatoimintoon, kuten kortille talletettujen tietojen tulostumiseen kortinlukijalle.

Linden kiteyttää, että toimikortin turvallisuus perustuu siruosan peukalointia sietävään rakenteeseen. Toimikortti tarjoaa hintaansa nähden varsin hyvän suojan sisältämilleen tiedoille. Murtovarmaa toimikorttia ei kuitenkaan ole. (Linden 2002, 21.)

Päivittäiset toimikortin turvallisuusuhat piilevätkin toimikortin haltijassa. Kortinhaltijan tärkeimpiä turvatoimenpiteitä on PIN-tunnuslukujen salassa pitäminen ja toimikortin fyysisestä turvallisuudesta huolehtiminen. Kortinhaltijaa pyydetäänkin säilyttämään toimikorttia turvallisessa, lukollisessa paikassa myös työajan ulkopuolella. Järvinen (2003) viittaakin, jos toimikortti päätyy sivullisen käsiin, sähköiseen tunnistamiseen tarkoitetulla toimikortilla voi saada vaikeasti peruuttamatonta vahinkoa aikaan toimikortin haltijalle. Järvinen painottaa, että sähköisesti allekirjoitetut asiakirjat ovat sitovia ja niiden kiistäminen jälkeenpäin on työlästä. (Järvinen 2003, 33.)

4.4.2 Toimikortin lukija

Linden (2002) kertoo, että toimikortin käyttö on suojattu. Toimikortin lukija ei aktivoitu ja käynnistä haluttua ohjelmaa, jos toimikortti on väärinpäin lukijassa. Tämä johtuu siitä, että toimikortin siru tarvitsee kontaktinastoja tiedonsiirtoon. Linden jatkaa, että toimikortti tarvitsee aina toimikortin lukijan antaakseen tietoja toimikortilta, sillä toimikortit käyttävät ulkoista jännitelähdettä ja kellopulssia sekä tulostus tapahtuu sarjamuotoisen signaalin välityksellä. (Linden 2002, 23.) Vaikka toimikortin laittaisi lukijaan väärinpäin, järjestelmä ei aktivoidu, koska se ei tunnista sirua lukijassa.

Kun toimikortti laitetaan lukijaan, toimikortin lukijan nastat painuvat toimikortin kontaktipintoja vasten. On myös olemassa kontaktittomia toimikortteja jolloin kommunikointi kortinlukijan välillä tapahtuu sähkömagneettisen induktion välityksellä maksimissaan kymmenen senttimetrin etäisyydellä lukijasta. (Linden 2002, 23.)

5 POHDINTA

Opinnäytetyön visuaalisen osuuden toteuttaminen on ollut haastavaa ja mielenkiintoista, sillä opinnäytetyö on rakennettu todellisen käyttötarpeen ympärille. Tiiviissä yhteistyössä Tampereen KanTo-projektin projektipäälliköiden kanssa on luotu 5 000:lle terveydenhuollon ammattihenkilölle koulutusmateriaali. Koulutusmateriaali opastaa ammattihenkilöitä terveydenhuollon toimikortin käyttöönotossa ja mahdollisissa ongelmatilanteissa. Yhteispäätös on ollut luoda neljä opetusvideota, jotka toimivat kirjallisen ohjeen tukena.

Opinnäytetyön keskeisimpiä tavoitteita on ollut valmistaa terveydenhuollon ammattihenkilöstö kattavalla koulutusmateriaalilla uuden toimintatavan oppimiseen eli terveydenhuollon toimikortin käyttöönottoon. Laajalla koulutusmateriaalilla on pyritty ehkäisemään mahdollisia epäselvyyksiä terveydenhuollon toimikortin käyttöönotossa. Opetusvideot havainnollistavat kirjallisen ohjeen vaihteita.

Opetusvideoon olisi voinut sisällyttää enemmän tietoturvallisten asioiden käsittelyä, jotta käyttäjälle rakentuu laajempi kuva tietoturvallisten asioiden tärkeydestä ja tietoturvallisten toimintatapojen edellytyksistä. Opinnäytetyön tavoitteena oli kuitenkin luoda terveydenhuollon toimikortin käyttöönotosta koulutusmateriaali. Syvällisemmät tietoturva-asiat on hyvä sisällyttää erilliseen koulutusmateriaaliin.

Opetusvideot pidettiin lyhyenä (kesto 2–3 min), jotta käyttäjän mielenkiinto pysyy yllä ja opetusvideot eivät sisällä liikaa informaatiota yhdellä kerralla. Opetusvideoiden sisältämät ääniraidat ja hitaasti etenevät kuvakaappaukset antavat jokaiselle käyttäjälle mahdollisuuden opiskella uutta asiaa rauhassa ja ymmärrettävästi. Opetusvideot laadittiin niin, että terveydenhuollon toimikortin käyttöä voi harjoitella samanaikaisesti yksittäisen opetusvideon ollessa käynnissä.

Koulutusmateriaalin laatimisessa on noudatettu tarkkaan Väestörekisterikeskuksen laatimia kirjallisia ohjeita terveydenhuollon toimikortin käyttöönotosta. Koulutusmateriaali on hyväksytetty Tampereen KanTo-projektissa Tampereen toimikorttien käyttöönotosta vastaavalla osaprojektiryhmällä ja Väestörekisterikeskuksen edustajalla.

Opinnäytetyön kirjallisessa osuudessa käydään läpi lakimääritteiden ja kansallisen terveysarkiston keskeisimmät asiat. Ne ovat pohjana sähköisen lääkemääräyksen kehittämiseksi, sähköiselle allekirjoitukselle ja terveydenhuollon toimikortille.

Kansallisen terveysarkiston käyttöönotto on jaoteltu osiin. Tällaisella menettelytavalla mahdollistetaan onnistunut uuden järjestelmän käyttöönotto ja mahdollisten virhetilanteiden minimointi: Pilottiosuuden suorittanut kunta raportoi järjestelmän käyttöongelmista, jotka korjataan ennen järjestelmän käyttöönottoa toisessa kunnassa. Vaiheittain tapahtuvaan käyttöönottoon on siirrytty myös siksi, että järjestelmän ylikuormittumista pyritään välttämään. On mahdotonta tuoda uusi järjestelmä valtakunnalliseen käyttöön ilman pilotointia tai järjestelmän todellista testaamista käytännössä.

Kansallisen terveysarkiston suunnittelu ja toteutus on vienyt vuosia. Vaiheittain rakentamisella ja kuntien vankkumattomalla yhteistyöllä on pystytty laatimaan Suomen terveydenhuollon suurimmista yhtenäisistä järjestelmistä. Ongelmia on tuonut yhteisen järjestelmän laatiminen ja yhteisten rajapintojen löytäminen: Alustana on ollut useiden sairaanhoitopiirien yksittäiset, muiden järjestelmien kanssa yhteensopimattomat potilastietojärjestelmät.

Opinnäytetyötä kirjoittaessa h-hetki on lähellä: Kansallisen terveysarkiston julkistaminen tuo pysyviä muutoksia julkisen sektorin tiedon käsittelyyn. Sähköinen lääkemääräys otetaan käyttöön Tampereen seudulla keväällä 2012. Kansallisen terveysarkiston palveluihin siirtyminen on kohdannut mediamylläkkää ja huhupuheita järjestelmän toimimattomuudesta. Kevään 2012 aikana tulemme huomaamaan kuinka kestävä uusi järjestelmä on.

Myös potilaalta tullaan odottamaan uusia käytäntöjä järjestelmän käyttöönoton jälkeen. Potilas voi noutaa tarvitsemansa lääkkeensä valitsemastaan apteekista kevästä 2012 lähtien Tampereen seudulla. Lääkärin laatima sähköinen lääkemääräys kulkeutuu valtakunnalliseen sähköiseen potilastietoarkistoon. Farmaseutti tai proviisori toimittaa asiakkaan tarvitsemat lääkkeet valtakunnallisen tietokannan tiedon mukaan. Jatkossa asiakas voi huoletta jatkaa matkaansa ottamatta mukaansa lääkemääräystä, sillä sähköinen lääkemääräys pysyy tallessa valtakunnallisessa tietokannassa 30 kuukautta.

Sähköinen lääkemääräys ja muut kansallisen terveystietokannan palvelut vaativat sähköisen, vahvan tunnistautumisen. Vahvana tunnistautumisena pidetään esimerkiksi terveydenhuollon toimikortin tunnusluvuilla tapahtuvaa todentamista.

Opinnäytetyössä käydään laajasti läpi tärkeät tietoturvalliset vaiheet, joiden toteutuminen mahdollistaa tietoturvallisten yhteyden luomisen terveydenhuollon toimikortin ja sen haltijan välille. Opinnäytetyössä on huomioitu, että toimikortin käyttäjä itse voi olla tietoturvallisten lähtökohtien toimimattomuuden syynä. On turha tehdä valtavia investointeja tietoturvallisiin välineisiin, jos välineiden käyttäjät eivät noudata tietoturvallisia toimintatapoja tai heitä ei kouluteta oikeisiin toimintatapoihin.

Terveydenhuollon toimikortti on rinnastettavissa muihin toimikortteihin kuten pankki- ja luottokortteihin. Opinnäytetyö käy läpi toimikortin rakenteen ja miltei pettämättömän toimikortin tietoturvallisuuden. Salaustekniikoiden käsittely olisi antanut laajemman kuvan toimikortin eduista ja mahdollisuuksista suojautua tietoturvahyökkäyksiä vastaan. Opinnäytetyön käsitellyt asiat antavat kuitenkin riittävän kuvan terveydenhuollon toimikortin pätevyydestä suojella potilaiden yksityisyyttä ja ehkäistä tietoturvahyökkäyksiä kuntien sisällä virtaavaa tietoa vastaan.

LÄHTEET

Henkilötietolaki 22.4.1999/523.

Järvinen, P. 2003. Salausmenetelmät. 1. painos. Porvoo: WS Bookwell, 29–34, 159–160, 173–177, 204, 206, 209.

Kansallinen terveystietojärjestelmä. 2009. Sähköinen resepti apteekissa. Luettu 01.02.2012. <https://www.kanta.fi/sahkoinen-resepti-apteekissa>.

Kansallinen terveystietojärjestelmä. 2010. Potilaan oikeudet. Luettu 03.02.2012. <https://www.kanta.fi/potilaan-oikeudet>.

Kansallinen terveystietojärjestelmä. 2011a. KanTa-palvelujen käyttöönotto. Luettu 31.01.2012. <https://www.kanta.fi/kanta-palveluiden-kayttoonotto>.

Kansallinen terveystietojärjestelmä. 2011b. Reseptin toimitus. Luettu 01.02.2012. <https://www.kanta.fi/reseptin-toimitus>.

Kansallinen terveystietojärjestelmä. 2011c. Sähköinen lääkemääräys vaatimusmäärittely. Luettu 23.01.2012. https://www.kanta.fi/c/document_library/get_file?uuid=008f6ef1-2fab-479c-8bfe-5c63ae240b63&groupId=10206.

Kansallinen terveystietojärjestelmä. 2011d. Sähköinen potilastiedon arkisto. Luettu 14.12.2011. <https://www.kanta.fi/fi/sahkoinen-potilastiedon-arkisto>.

Karttunen, T. projektipäällikkö. 2012. Työelämän edustajan lausunto opinnäytetyöstä. Sähköpostiviesti. tiina.t.karttunen@tampere.fi. Luettu 02.02.2012.

Laki potilaan asemasta ja oikeuksista 17.8.1992/785.

Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä 9.2.2007/159.

Laki sähköisestä lääkemääräyksestä 2.2.2007/61.

Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista 617/2009.

Laki viranomaisten toiminnan julkisuudesta 21.5.1999/621.

Laki väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista annetun lain muuttamisesta 19.11.2010/983.

Laukkanen, V. 2008. Hoitohenkilöstön tietoturvatietoisuus ja tietoturvaosaaminen. Kuopion yliopisto. Terveystietojärjestelmän ja -talouden laitos. Pro gradu -tutkielma.

Linden, V. 2002. Julkisen avaimen järjestelmä, toimikortit ja niiden soveltaminen organisaatiossa. Tampereen Teknillinen yliopisto. Lisensiaatintutkimus.

Pahlman, I. 2010. Asiakastietojen käsittely, salassapito ja asiakkaan tiedonsaantioikeus sosiaali- ja terveydenhuollossa. Helsinki: Edita, 21–25, 123, 130–132.

Rinne, T. 2002. Älykortit – tekniikka, sovellukset ja käyttöönotto. Jyväskylä: Gummerus Kirjapaino Oy, 29, 30, 33, 63, 65–67.

Seppälä, A. 2011. Terveystietosuojan tietosuojat ja tietoturva. Tampereen yliopisto.

Sosiaali- ja terveysministeriö. 2006. Opas sähköisen potilaskertomuksen rakenteesta. Luettu 20.01.2012. <http://www.vtt.fi/virtual/hl7/cda/opas-spk-rakenne-2006-02-28.doc>.

Sosiaali- ja terveysministeriö. 2012. Usein kysyttyjä kysymyksiä tietojärjestelmähankkeista. Luettu 31.01.2012. <http://www.stm.fi>.

Suomen Kuntaliitto. 2012. KanTa pähkinän kuorella. Luettu 09.01.2012. <http://www.kunnat.net/fi/asiantuntijapalvelut/soster/tietojarj-sahkoiset-palv/Kunto/kanta/Sivut/default.aspx#anchor-details>.

Sähköisen tunnistamisen menetelmät ja niiden sääntelyn tarve. 2003. Liikenne- ja viestintäministeriön julkaisuja 44/2003. Helsinki: Pikapaino, 11, 30.

Tampereen kaupunki. 2012. Sähköinen resepti. Luettu 01.02.2012. <http://www.tampere.fi/terveyspalvelut/eresepti.html>.

Tietojärjestelmähankinnat terveydenhuollossa ja sosiaalitoimissa. 2008. Suomen Kuntaliitto. Helsinki: Kuntatalon paino, 30, 31, 36.

Tietosuojavaltuutetun toimisto. 2010. Tietosuojavastaavan toimenkuva, tehtävät ja asema. Luettu 06.12.2011. http://www.tietosuojat.fi/uploads/939r21bdr3_1.pdf.

Terveystietosuojat 30.12.2010/1326.

Turvalliset sähköisen allekirjoituksen luomisvälineet. Vaatimusten arviointi. 2004. Liikenne- ja viestintäministeriön julkaisuja 52/2004. Helsinki: Pikapaino, 9.

Väestörekisterikeskus. 2011. Varmennepolitiikka terveydenhuollon ammattivarmennetta varten. Luettu 09.11.2011. <http://fineid.fi/default.aspx?docid=5029&action=publish>.

Väestörekisterikeskus. 2012. Sulku- ja neuvontapalvelu. Luettu 25.01.2012. <http://fineid.fi/default.aspx?id=318>.

Väestörekisterikeskus. 2012. Varmennepalvelu. Luettu 01.02.2012. <http://fineid.fi/default.aspx?id=316>.



TAMPERE



Terveystietojärjestelmän toimikortin käyttöohjeet ~ Pegasos

Toimikortilla tarkoitetaan pankkikortinkokoista ja vertaista sirullista korttia. Väestörekisterikeskuksen myöntämällä toimikortilla ja perustunnusluvulla tunnistaudutaan potilastietojärjestelmään ja eReseptikeskukseen.

Toimikortti lunastetaan rekisteröintipisteestä. Toimikorttia lunastettaessa täytetty henkilöllisyys todistaa. Henkilöllisyystodistuksina käytävät voimassa oleva poliisin myöntämä henkilökortti, 1.10.1990 jälkeen myönnetty ajokortti tai passi.

Tunnuslukukuori (kuva 1) sisältää seuraavat tiedot:

Perustunnusluku (PIN1) = Pegasos-potilastietojärjestelmään kirjaututaan toimikortilla ja perustunnusluvulla eli PIN1-tunnusluvulla.

Sähköinen allekirjoitus (PIN2) = Sähköinen allekirjoitus eli PIN2-tunnusluku on juridisesti kiistan allekirjoitus. Sähköinen allekirjoitus varmentaa digitaalisen dokumentin tai muun tiedoston (esimerkiksi lääkärintodistus, sähköinen lääkemääräys) aitouden, eheyden ja kiistämättömyyden.

PUK-avaustunnusluku = PUK-avaustunnusluvulla avataan lukittunut toimikortti (tunnusluku PIN1 tai PIN2).

Säilytä toimikortti, tunnusluvut ja PUK-avaustunnusluku huolellisesti myös työajan ulkopuolella.

Toimikorttia ja tunnuslukuja ei saa luovuttaa sivullisen käyttöön.

Säilytä toimikorttia ja tunnuslukuja huolellisesti, mutta erillään toisistaan eri paikoissa. Toimikortti ja tunnusluvut tulee säilyttää turvallisessa säilytyspaikassa myös työajan ulkopuolella, esimerkiksi lukollisessa kaapissa tai vastaavassa.

Toimikortin käyttö

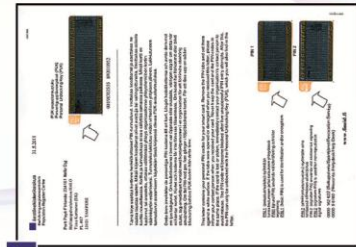
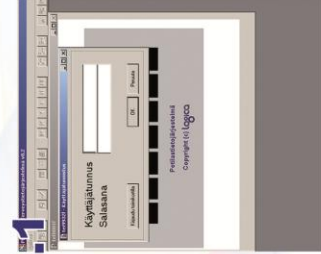
- Avaa Pegasos-potilastietojärjestelmän sisäänkirjautumis-ikkuna. Laita toimikortti lukijaan siruosa edellä (ks. kuva 2). Klikkaa Kirjaudu toimikortilla -painiketta (ks. kuva 2.1). Näytölle avautuu Syötä perustunnusluku -ikkuna. Anna perustunnusluku eli PIN1 pyydettyyn kohtaan. Klikkaa OK-painiketta. Olet kirjautunut järjestelmään.

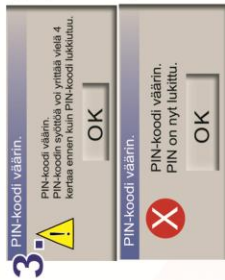
Jos järjestelmä antaa virheilmoituksen (esimerkiksi "PIN-koodi väärin" tai lukija ei tunnista toimikorttia tällöin näytön oikeassa alalaidassa sirun muotoinen symboli ei näy keltaisena), poista toimikortti lukijasta, aseta toimikortti lukijaan uudelleen ja yritä kirjautua järjestelmään uudelleen. Toista toiminnot tarvittaessa.

Kun poistut tietokoneelta, ota toimikortti lukijasta aina mukaasi. Muista myös kirjautua ulos Pegasos-potilastietojärjestelmästä.

2.

2.1





3. Toimikortin lukkiutuminen

Toimikortti lukkiutuu, jos tunnusluku näppäilyä viisi (5) kertaa peräkkäin väärin (kuva 3).

Järjestelmä ilmoittaa kuinka monta tunnusluvun syöttökertaa on jäljellä. Jos toimikortti lukkiutuu, lukkiutunut toimikortti avataan PUK-avaustunnusluvulla.

Kun vaihdat PIN-tunnusluvun (PIN1 tai PIN2) on uuden PIN-tunnusluvun oltava helposti muistettava 4-8 numeron sarja.

Vältä helposti päätettävää numerosarjoja esim. syntymäpäivä, numerosarjat 0000, 1111, 1234, 2580.

Tunnusluvun vaihto

- Laita toimikortti lukijaan. Avaa tietokoneen näyttöltä DigiSign-ohjelma.
- Valitse näytölle avautuneesta uudesta ikkunasta Tunnistus-välilehti (kuva 4).
- Klikkaa tarvitsemaasi vaihtoehtoa Tunnistustietojen kohdassa: Voit vaihtaa perustunnusluvun tai (sähköisen) allekirjoitustunnusluvun. Huom! Malliesimerkkiä käytetään molempiin vaihtoehtoihin.
- Syötä käytössä oleva PIN-tunnusluku Nykyinen PIN -riville.
- Uuden PIN-tunnusluvun tulee olla 4-8 numeron sarja. Syötä haluamasi uusi PIN-tunnusluku Uusi PIN -riville.
- Vahvista PIN-tunnusluku syöttämällä se uudestaan alemmalle riville.
- Klikkaa Vaihda-painiketta. Järjestelmä antaa ilmoituksen onnistuneesta PIN-tunnusluvun vaihdosta ja voit jatkaa työskentelyä kirjautumalla Pegason-potilasjärjestelmään.

Lukkiutuneen toimikortin avaaminen

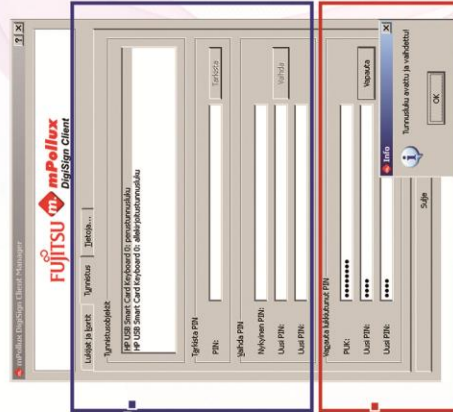
Voit avata lukkiutuneen toimikortin DigiSign-ohjelman avulla.

- Laita toimikortti lukijaan.
- Avaa tietokoneen näyttöltä DigiSign-ohjelma
- Avaa Tunnistus-välilehti.
- Syötä PUK-riville (kuva 5) kahdeksan (8) numeron PUK-avaustunnusluku, jonka olet saanut tunnusluvun kuoren mukana.
- Lukituksen avaaminen vaatii myös PIN-tunnusluvun vaihdon!

Vaihda PIN-tunnusluku syöttämällä valitsemasi 4-8 numeron sarja Uusi PIN -riville.

- Vahvista uusi tunnusluku syöttämällä se uudestaan alemmalle riville.
- Klikkaa Vapauta-painiketta. Järjestelmä antaa ilmoituksen onnistuneesta toimikortin tunnusluvun vapauttamisesta ja tunnusluvun vaihdosta.
- Sulje ohjelma Sulje-painikkeella. Voit jatkaa työskentelyä kirjautumalla Pegason-potilasjärjestelmään.

Säilytä PUK-avaustunnusluku huolellisesti mahdollista seuraavaa käyttökertaa varten.



Toimikortin haltijan vastuu kadonneesta tai anastetusta toimikortista päättyy vasta, kun hän on tehnyt katoamisilmoituksen soittamalla oman organisaation toimikorttien rekisteröintipisteeseen tai sen ollessa suljettuna valtakunnalliseen sulkupalveluun.

Valtakunnallinen sulkupalvelunumero +358 800 162 622. Kuulorajoitteisten tekstipuhelimen sulkupalvelunumero 0800 302288 (maksuton). Toimikorttiin liittyvää lisämaksutonta neuvontapalvelua on saatavana kaikkina päivinä klo 08-22 numerosta 0600 9 6160 (pvm mpm).

Katso lyhyet opastevideot toimikortin käytöstä loora.fi -sivulta!

