Satakunnan ammattikorkeakoulu

Anita Kemppinen

TIETOSUOJA HYVINVOINTIALAN SOVELLUKSESSA JA SAAS-OHJELMISTOPALVELUTUOTANNOSSA CASE: TUHA

Tietojenkäsittelyn koulutusohjelma

2007

TIETOSUOJA HYVINVOINTIALAN SOVELLUKSESSA JA SAAS-OHJELMISTOPALVELUTUOTANNOSSA CASE: TUHA

Kemppinen, Anita
Satakunnan ammattikorkeakoulu
Tietojenkäsittelyn koulutusohjelma
Huhtikuu 2007
Hentunen, Ilmari
UDK: 004.056, 004.41, 004.65, 658.89
Sivumäärä: 80

Asiasanat: asiakkuudenhallinta, ohjelmistotuotanto, tietojärjestelmät, toiminnanohjaus, yksilönsuoja

---

Tämän opinnäytetyön aiheena oli selvittää sosiaali- ja terveydenhuollon sähköisiin järjestelmiin rekisteröityjen asiakkaiden tietosuojaa sääntelevät normit. Lisäksi selvitettiin, mitä vaatimuksia tietosuoja aiheuttaa Internet-verkossa käytettävän hyvinvointialan toiminnanohjaus- ja asiakashallintasovelluksen suunnitteluun sekä toteutukseen. Selvityksen pohjalta toteutettiin Codebird Oy:n TUHA-sovelluksen ja sen ohjelmistopalvelun tietosuoja-arviointi. Arviointitulosten perusteella laadittiin kehitysehdotukset tietosuojan parantamiseksi. Projekti toteutettiin talven 2006 ja kevään 2007 aikana.

Tietosuojaan liittyvät asiat selvitettiin lainsäädännöstä sekä kahdesta tietosuojaa ja tietoturvallisuutta käsittelevästä standardista. Toinen standardeista oli tietosuojan yleisstandardi ja toinen, vasta luonnosvaiheessa oleva, yleisesti käytetty tietosuojaa sosiaali- ja terveydenhuollon näkökulmasta tarkasteleva standardi. Normiston tarkastelussa ja sen ohjelmistotuotantoon soveltamisessa hyödynnettiin aiheeseen liittyvää kirjallisuutta, verkkomateriaalia sekä asiantuntijalausuntoja.

Normiston pohjalta tehty case-arviointi toteutettiin kehittävän laadullisen tutkimusotteen tapaan. Arvioitu TUHA-sovellus on hyvinvointialan yksityisille sekä säätiö- ja järjestöpohjaisille palveluntuottajille suunnattu Internet-verkossa käytettävä sovellus. Sovellusta markkinoidaan SaaS-mallin mukaisena palvelukokonaisuutena. Arvioinnissa löytyi eräitä tietosuojan kannalta ongelmallisia seikkoja, joihin laadittiin eettisesti ja liiketaloudellisesti kestävät kehitysehdotukset. Arviointi ja laaditut kehitysehdotukset kuuluvat opinnäytetyön tilaajan liikesalaisuuden piiriin, joten ne kirjattiin tämän työn liiteosioiksi. Nämä liiteosiot luovutettiin Satakunnan ammattikorkeakoulun opinnäytetyöohjeen julkisuussäännösten mukaisesti vain Codebird Oy:lle.

Normistossa annetaan yksityiskohtaisia ohjeita sosiaali- ja terveydenhuollon asiakas- ja potilastietojen sisällöistä sekä tietojen käsittelystä, salassapidosta, säilytyksestä ja luovutukseen liittyvistä asioista. Ohjeet näiden teknisistä toteutustavoista sähköisissä järjestelmissä ovat nykyisellään tulkinnanvaraisia. Tavoittelemalla tietoturvastandardien mukaisia toimintatapoja ohjelmistotuotantoa voidaan ohjata tietosuojaa toteuttavien käytäntöjen mukaisiin ratkaisuihin. Lakiin sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä liittyvään asetukseen tullaan säätämään tietosuojaan ja näiltä osin myös tietoturvallisuuteen liittyviä tarkempia ohjeita. Asetus astunee voimaan vuoden 2007 loppuun mennessä.

PRIVACY PROTECTION IN WELFARE SERVICES APPLICATION AND SAAS-SERVICE CASE: TUHA

Kemppinen, Anita
Satakunta University of Applied Sciences
Degree Programme in Business Information Systems
April 2007
Hentunen, Ilmari
UDK: 004.056, 004.41, 004.65, 658.89
Number of pages: 80

Keywords: customer relationship management, software engineering, data systems, enterprise resource planning, individual protection

---

The subject of this thesis was to define norms of privacy protection in electronic systems. The concern was especially in registered customers of social welfare and health care. In addition to this it was defined what kind of requirements privacy protection influences to the designing and implementation of welfare services' enterprise resource planning and customer relationship management application using over the Internet. The Codebird Ltd's TUHA application as well as the software delivery was then evaluated according to this definition. The focus of this evaluation was on privacy protection. The proposal for better privacy protection was produced on the grounds of the evaluation results. The project was put into practice during winter 2006 and spring 2007.

The privacy protection analysis was based on current legislation as well as on two standards concerning information security. The first standard was the general standard of information security and the second standard, one that is still being drafted, covers common information protection practices used in social welfare and health care. Subject matter literature, web material and expert opinions were utilized on considering the norms and adapting to the software engineering.

Case-evaluation based on the norms was put into practice in the manner of a qualitative research. The TUHA application, which was evaluated, is a web based application designed for private and foundation sector welfare service providers. The application is being marketed based on SaaS-service (Software as a Service) model. The evaluation uncovered some information security issues that were problematic, but which were met by establishing development schemes that are sustainable both from ethical as well as economical view points. Evaluation and development proposals are a business secret of the subscriber of this thesis. Therefore those were written into the appendices. These appendices were turned over only to Codebird Ltd according to Satakunta University of Applied Sciences guideline of thesis and it's principle of publicity.

The norms define detailed instructions about social welfare and health care customer and patient information, data processing, concealment as well as facts about safekeeping and extradition. Specifications how to realize these instructions in electronic systems are nowadays open to interpretations. Software engineering may be guided to the solutions with better privacy protection by seeking methods accordant with data security standards. Specific instructions of privacy protection and data security will be enacted in the statute related to the law of social welfare and health care customer information data processing. The statute will come into operation by the end of year 2007.

SISÄLLYS

LYHENNELUETTELO

API	Application Programming Interface
ASP	Application Service Provider, myös Active Server Pages
CGI	Common Gateway Interface
DAO	Data Access Object
FinSoc	Sosiaalipalvelun arviointiryhmä
HE	Hallituksen esitys
HetiL	Henkilötietolaki
HTML	HyperText Markup Language
IEC	International Electrotechnical Commission
IP	Internet Protocol
ISO	International Organization for Standardization
J2EE	Java 2 Enterprise Edition
JAAS	Java Authentication and Authorization Service
JDBC	Java Database Connectivity
JDK	Java Developer Kit
JSP	Java Server Pages
JUHTA	Julkisen hallinnon tietohallinnon neuvottelukunta
MVC	Model - View - Controller
OID	Object Identifiers
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PotA	Sosiaali- ja terveysministeriön asetus potilasasiakirjojen laatimisesta sekä niiden ja muun hoitoon liittyvän materiaalin säilyttämisestä
PotL	Laki potilaan asemasta ja oikeudesta
RAR	Roshal Archive file format
SaaS	Software as a Service
SHAL	Laki sosiaalihuollon asiakkaan asemasta ja oikeuksista
SoTeSKL	Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä

SQL	Structured Query Language
SSL	Secure Socket Layer
SVTSL	Sähköisen viestinnän tietosuojalaki
SähkAL	Laki sähköisistä allekirjoituksista
TCP	Transmission Control Protocol
URL	Uniform Resource Locator

1 JOHDANTO

Julkiset sosiaali- ja terveydenhuollon organisaatiot hyödyntävät tietoteknologiaa yhä laajemmin omassa toiminnassaan. Asiakkaiden ja potilaiden tiedot ovat lähes kaikki sähköisessä muodossa. Sosiaali- ja terveysalan tutkimus- ja kehittämiskeskuksen eli Stakesin tutkimuksen mukaan terveydenhuollossa vuoden 2005 aikana käytettiin pääasiallisesti sähköistä potilastietojen dokumentointia tai siihen oltiin siirtymässä kaikissa organisaatioissa. Yksityisillä lääkäripalvelujen tuottajilla sähköiset järjestelmät olivat käytössä 89 % vastaajista. (Winblad, Reponen, Hämäläinen & Kangas 2006, 13, 36, 53.) Melkein kaikki kunnat käyttivät sosiaalihuollon toiminnassaan erilaisia sähköisiä järjestelmiä, mutta sovellusten sisältö ja käyttöaste vaihtelivat. Sähköistämisen suurimpana esteenä pidettiin yhteisten sosiaalialan käsitemäärittelyjen puuttumista. (Sosiaali- ja terveysministeriö 2005, 17.)

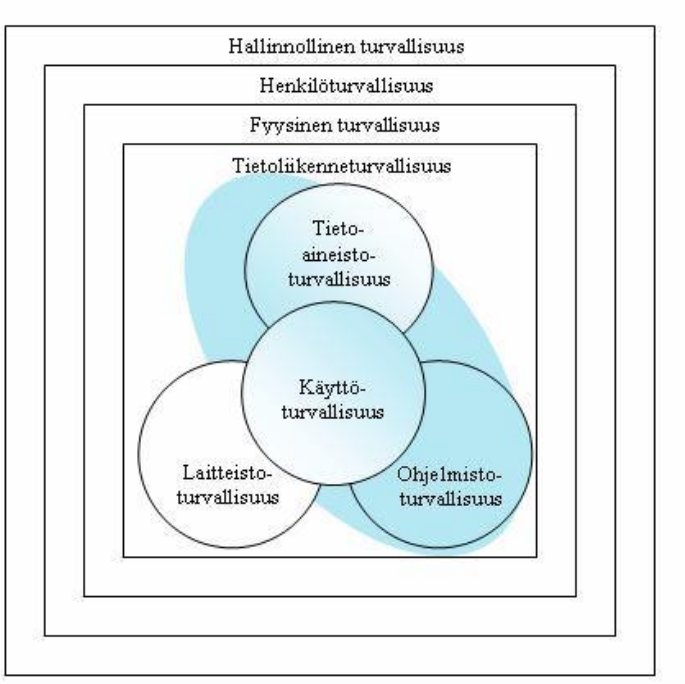
Sähköinen muoto mahdollistaa tiedon jäsentelyn ja hyödyntämisen erilaisiin tarkoituksiin. Kertaalleen kirjattua tietoa hyödynnetään paitsi tiedon tallentamiseen ja viestintään, myös ammatillisen toiminnan valvontaan, tutkimus- ja koulutustoimintaan sekä organisaation sisäiseen suunnittelutyöhön. Työnkuvan mukaan rajatut käyttöoikeudet ja tietojärjestelmän käytöstä kerääntyvät lokitiedot tekevät sähköisestä tiedonkäsittelystä omalla tavallaan tietoturvallisempaa kuin manuaalinen tiedonkäsittely. Toisaalta verkossa liikkuva tieto on entistä helpommin saatavilla, jos osaava henkilö niin haluaa ja jos tietoturvasta ei ole huolehdittu riittävässä laajuudessa.

Tietosuojalainsäädännön ja alan eettisten periaatteiden mukaan sosiaali- ja terveydenhuollon asiakkailla on oikeus laadukkaaseen asioidensa hoitoon. Siihen sisältyy olennaisesti arkaluontoisten tietojen yksityisinä säilyminen. Henkilörekisteristä, sen sisältämistä tiedoista ja niiden käytöstä vastaa aina rekisterinpitäjä. Vastuu säilyy, vaikka rekisterinpidon tekninen osuus ulkoistettaisiin toimeksiantosopimuksella. Sosiaali- ja terveysministeriö, Stakes ja tietosuojavaltuutetun toimisto ovat tuottaneet rekisterinpitäjille erilaisia ohjeita helpottamaan lain tulkintaa ja soveltamista käytäntöön. Tietosuojasta on julkaistu myös hyvää kirjallisuutta. Tietosuojavaltuutetun toimistossa työskentelevät ylitarkastaja Arto Ylipartanen ja toimistopäällikkö Maija Kleemola, oikeusministeriön

erityisavustaja Irma Pahlman sekä Teknisen korkeakoulun projektipäällikkö Raija Tervo-Pellikka ovat julkaisuissaan käsitelleet sosiaali- ja terveydenhuollon tietojärjestelmiä tietosuojan toteutumisen näkökulmasta.

Tässä opinnäytetyössä tarkastellaan niitä vaatimuksia, joita tietosuoja ja sen laadukas toteutuminen asettaa hyvinvointialalle suunnattujen Internet-verkossa käytettäville tietojärjestelmien suunnittelulle ja toteutukselle. Asiaa tarkastellaan erityisesti ohjelmistotoimittajan näkökulmasta. Työssä kootaan kaikki ne lait, asetukset ja muut normit, jotka ohjeistavat asiakkaiden tietosuojaan liittyviä asioita sekä pohditaan normien asettamia käytännön vaateita ja vaikutuksia tietojärjestelmätuotantoon. Työn toisessa osiossa analysoidaan Codebird Oy:n TUHA-sovelluksen tietosuojan toteutumista. TUHA:a tarkastellaan ohjelmistoarkkitehtuurin, tietosisältöjen, tietokantaratkaisujen, ohjelmointikoodin, käytetyn tietoliikenneprotokollan sekä koko sovelluskehitysprosessin osalta. Mikäli analyysissä löytyy olennaisia tietosuojaa vaarantavia seikkoja, etsitään näihin ongelmakohtiin eettisesti ja liiketaloudellisesti kestäviä ratkaisuja. TUHA-sovelluksen jakelukanavana käytetään SaaS-mallin (Software as a Service) mukaista ohjelmistopalvelua, joten tietosuojaa koskevassa tiedonhaussa, analyysissä ja kehitysehdotusten laadinnassa huomioidaan myös ohjelmistopalvelun ulottuvuus. TUHA-sovellusta käsittelevät osiot kuuluvat opinnäytetyön tilaajan liikesalaisuuden piiriin. Tämän vuoksi sekä analysointitulokset että kehitysehdotukset esitetään erillisissä liitteissä. Liite-osiot luovutetaan vain työn tilaajalle.

Aihealueen laajuuden vuoksi eräitä tietosuojaan ja sen toteutumiseen liittyvistä osa-alueista rajataan tarkastelun ulkopuolelle. Tarkastelun ulkopuolelle jätetään kahden rekisterinpitäjän välinen ja muu tietojen luovuttaminen. Tietojen luovuttaminen on sovelluksen käyttäjän omaa toimintaa, eikä se näin ollen liity ohjelmistotoimittajan toimialaan. Kirjanpitoon tai työelämän tietosuojaan liittyviä asioita ei myöskään käsitellä. Rekisterinpitäjän ja muihin hallinnolliseen toimintaan liittyviä asioita käsitellään vain niiltä osin, kun ne koskevat SaaS-ohjelmistopalvelutuotantoa. Tietoturvaa käsitellään vain osana tietosuojan toteuttamista. SaaS-palveluntuottajan fyysistä, laitetason tai verkkojen tietoturvaa ei käsitellä lainkaan. Tarkastelun ulkopuolelle jää myös sovelluksen käytettävyys ja tehokkuus. Kuviossa 1 havainnollistetaan tämän opinnäytetyön aihealueen sijoittumista eri tasoista koostuvaan tietoturvallisuuden kokonaiskenttään.



Kuvio 1. Tämän opinnäytetyön aiheen (kuvattu sinivihreänä) sijoittuminen tietoturvallisuuskenttään (mukailtu Paavilainen 1998, 26)

TUHA on hyvinvointialan yksityisille ja nk. kolmannen sektorin palveluntuottajille suunnattu toiminnanohjaus- ja asiakashallintajärjestelmä. Asumispalveluun liittyvien toimintojen lisäksi TUHA-sovelluksessa on huomioitu avopalvelujen tarpeet. TUHA on kehitetty osana satakuntalaisen kehittäjäorganisaatio Prizztech Oy:n koordinoimaa hyvinvointi ja teknologia -hanketta, jonka tavoitteena oli löytää hyvinvointiyrityksille selainpohjaisen teknologian avulla uusia mahdollisuuksia toimintaprosessien tehostamiseen (Rintala 2005). Hanke toteutettiin vuosina 2005–2006.

TUHA:a markkinoidaan Saas-ohjelmistopalveluna. SaaS-ohjelmistopalvelussa hyvinvointialan yrittäjä ostaa käyttöoikeuksia Internetin välityksellä toimivaan sovellukseen. Ohjelmistopalvelu tarjoaa asiakkaalle mahdollisuuden käyttää sähköistä tietojärjestelmää ilman investointeja ohjelmistokehitykseen, palvelin- ja verkkoinfrastruktuuriin tai tietotekniseen osaamiseen. Palvelun käyttäminen edellyttää asiakkaalta suurta luottamusta ohjelmistotoimittajaan. Toiminnanohjaus ja asiakashallinta ovat hyvinvointiyrittäjän ydinprosesseja, joiden tietosisällöt kuuluvat arkaluonteisiin tietoihin. Näiden tietojen luovuttaminen toisen yrityksen haltuun edellyttää, että hyvinvointiyrityksen on voitava varmistua tietosuojan ja tietoturvan toteutumisesta. (Sääksjärvi, Nordström, Santonen & Lassila 2004, 4-5.) SaaS-mallin mukainen liiketoimintamalli on yleistymässä

myös suomalaisessa ohjelmistokehityksessä. Enimmäkseen ohjelmistopalvelua tarjoavat suuret ohjelmistotoimittajat. (Kontio, Lassila & Maula 2006.) Hyvinvointialalle suunnatuista toiminnanohjauksen ja asiakashallinnan sovelluksista TUHA on tällä hetkellä tiettävästi ainoa, jota tarjotaan Saas-ohjelmistopalveluna.

Tietojärjestelmien tietosuojasta on olemassa vain vähän tutkimuksia tai niitä ei ole tuotu julkisuuteen. USA:ssa Pennsylvaniassa Hassol ym. (2004) tutkivat asiakkaiden tyytyväisyyttä Internetissä käytettävän terveystietoja sisältävän sovelluksen käyttöön. Tutkimuksen mukaan vain vähemmistö vastaajista oli huolissaan terveystietojensa luottamuksellisuuden säilymisestä. Pohjois-Karjalan keskussairaalassa on tutkittu henkilöstön näkökulmaa tietoturvallisuuden toteutumisesta suljetussa verkossa. Samassa tutkimuksessa sivuttiin myös tietosuojan toteutumiseen liittyviä asioita. (Reponen 2006, 8.) Makropilotissa, joka oli sosiaali- ja terveysministeriön tietoteknologian kehittämis- ja kokeiluhanke vuosina 1999–2001, ei Ohtosen (2002, 13, 34-35, 118) mukaan tietosuojaan liittyviä asioita voitu arvioida lainkaan, vaikka hankkeen yhtenä tavoitteena oli sosiaali- ja terveydenhuollon asiakkaiden tietosuojan ja tietoturvan hyvien käytäntöjen kehittäminen. Arvioinnin esteenä oli mm. teknisten ratkaisujen viivästyminen. Makropilotin ansiona Ohtonen näkee kuitenkin tietosuoja-aiheisten keskustelujen alkamisen.

2 TIETOSUOJA HYVINVOINTIALAN SOVELLUKSESSA JA SAAS-OHJELMISTOPALVELUTUOTANNOSSA

2.1 Keskeiset käsitteet

Tietosuojalla tarkoitetaan henkilötietojen käsittelyä koskevien vaatimusten huomioon ottamista yksityisen henkilön yksityisyyden ja oikeusturvan varmistamiseksi (Ylipartanen 2004, 17). Tammisalo (2005, 7) määrittelee tietosuojalla tarkoitettavan henkilötietojen suojaamista valtuudettomalta ja henkilöä vahingoittavalta käytöltä ja käsittelemiseltä. Hänen mukaansa tietosuoja on yksilön suojaa. Heiliön ja Ylipartasen (2006a, 628) mukaan sosiaali- ja terveydenhuollossa tietosuoja suojelee ihmisen yksityisyyden lisäksi

luottamuksellista asiakassuhdetta. Tietosuojan tarkoituksena on hyvän käsittelytavan luominen ja toteuttaminen henkilötietojen käsittelyn kaikissa eri vaiheissa, rekisteröityjen oikeuksien kunnioittaminen ja toteuttaminen sekä rekisteröityjen ja rekisterinpitäjien oikeusturvan varmistaminen. Tietosuojan toteutumista pyritään toteuttamaan tietoturvalla. Tietoturva voidaan määritellä tietoturvavaatimuksina, joita ovat luottamuksellisuus, käytettävyys, eheys, kiistämättömyys ja pääsynvalvonta (Hakala, Vainio & Vuorinen 2006, 5). Näiden vaatimusten toteutuminen tarkoittaa tiedon säilymistä vain niihin oikeutettujen henkilöiden käytössä, tiedon oikeellisuutta, aitoutta, ajantasaisuutta sekä tiedon saatavuutta, oikea-aikaisuutta ja hyödynnettävyyttä (Pahlman 2005, 14).

Henkilötiedon käsite on määritelty henkilötietolaissa. Henkilötietolaista käytetään tässä työssä lyhennettä HetiL. Henkilötietoja ovat kaikki ne tiedot ja merkinnät, jotka koskevat luonnollista henkilöä, hänen ominaisuuksiaan tai elinolojaan ja jotka voidaan tunnistaa henkilöä, hänen perhettään tai hänen kanssaan yhteisessä taloudessa eläviä koskeviksi. Henkilötietojen käsittelyä ovat henkilötietoihin kohdistuvia toimenpiteitä, kuten henkilötietojen keräämistä, tallettamista, järjestämistä, käyttöä, siirtämistä, luovuttamista, säilyttämistä, muuttamista, yhdistämistä, suojaamista, poistamista ja tuhoamista. (HetiL 3 §.) Tässä työssä käytetään käsitettä henkilötietojen käsittely kuvaamaan kaikkia näitä toimintoja lukuun ottamatta henkilötietojen luovuttamista.

Henkilörekisteri määritellään henkilötietolaissa käyttötarkoituksensa vuoksi yhteenkuuluvien merkintöjen tietojoukoksi, jota käsitellään osin tai kokonaan automaattisen tietojenkäsittelyn avulla. Henkilörekisteri on järjestetty kortistoksi, luetteloksi tai muulla näihin verrattavalla tavalla niin, että jotakin tiettyä henkilö koskevat tiedot löytyvät nopeasti. (HetiL 3 §.) Loogisesti samaan henkilörekisteriin katsotaan kuuluvaksi kaikki samaan tarkoitukseen käytettävät tiedot riippumatta siitä, miten ja mihin tiedot on tallennettu. Loogisesti samaan rekisteriin luetaan kuuluvaksi myös rekisterinpitäjän samaan käyttötarkoitukseen tarkoitetut lyhytaikaiset tiedostot, sähköisestä järjestelmästä tulostetut tulosteet sekä tallenteiden eri sukupolvet. (Ylipartanen 2004, 18, 47.) Rekisteröidyllä tarkoitetaan henkilöä, jota tieto koskee. Rekisterinpitäjällä tarkoitetaan yhtä tai useampaa henkilöä, yhteisöä, laitosta tai säätiötä, jonka käyttöä varten henkilörekisteri perustetaan ja jolla on oikeus määrätä rekisterin käytöstä tai jonka tehtäväksi rekisterinpito on lailla säädetty. (HetiL 3 §.)

Terveydenhuollossa asiakkaan tietoja käsitteleviä asiakirjoja kutsutaan potilasasiakirjoiksi. Laki potilaan asemasta ja oikeudesta eli potilaslaki (PotL) määrittelee potilasasiakirjat potilaan hoidon järjestämisessä ja toteuttamisessa laadituiksi, käytettäviksi tai saapuneiksi asiakirjoiksi tai teknisiksi tallenteiksi, jotka sisältävät hänen terveydentilaansa koskevia tai muita henkilökohtaisia tietoja (PotL 2 §). Keskeisin potilasasiakirja on potilaskertomus, joka kattaa aikaisemmat terveys- ja sairauskertomukset sekä potilaasta laadittavan aikajärjestyksessä etenevän jatkuvan potilaskertomuksen. Eri ammattiryhmät tekevät työnsä vaatimat merkinnät jatkuvaan potilaskertomukseen jokaisesta avohoito- ja kotihoitokäynnistä sekä osastohoitojaksosta. Potilaskertomukseen kuuluvat hoidon järjestämisessä ja toteutumisessa syntyneet asiakirjat, kuten erilaiset lausunnot ja lähetteet. Potilasasiakirjoja ovat lisäksi röntgen-, magneetti- ja ultraäänikuvat, sydän- ja aivosähkökäyrä-tallenteet, leikkaus- ja toimenpidekertomukset, yhteenvedot, loppulausunnot sekä ajanvaraus- ja potilaspäiväkirjat. (Ylipartanen 2004, 19; Pahlman 2005, 13.)

Sosiaalihuollossa asiakkaan tietoja käsitteleviä dokumentteja kutsutaan asiakasasiakirjoiksi. Sosiaalihuollon asiakaslaissa, tässä SHAL, määritellään sosiaalihuollon tarkoittavan sosiaalihuoltolaissa (710/1982) 17 §:ssä mainittuja sosiaalipalveluja, tukitoimia, toimeentulotukea, elatustukea, sosiaalista luottoa sekä mainittuihin palveluihin liittyviä toimenpiteitä, joiden tarkoituksena on edistää ja ylläpitää henkilön sekä perheen sosiaalista turvallisuutta ja toimintakykyä. Sosiaalihuollon asiakirja on viranomaisen tai yksityisen järjestämän sosiaalihuoltoon liittyvä, viranomaisen toiminnan julkisuudesta annetussa laissa (621/1999) mainittu asiakirja, joka sisältää asiakasta tai muuta yksityistä henkilöä koskevaa tietoa. (SHAL 3 §.)

Hyvinvointialan palveluilla tarkoitetaan ei-julkisten palveluntuottajien, kuten yritysten, järjestöjen ja säätiöiden, tuottamia sosiaali- ja terveydenhuollon palveluita. Niiden tarkoituksena on täydentää julkisen sektorin toimintaa. Hyvinvointialan palveluiden osuus on noin viidennes kaikista tuotetuista palveluista. Suuri osa palveluista rahoitetaan julkisin varoin, sillä kunnat ostavat palveluita ostosopimuksilla. Säätiöt voivat saada toimintaansa tukea Raha-automaattiyhdistykseltä. Osin palveluiden käyttäjät itse maksavat saamistaan palveluista. (Kauppinen & Niskanen 2003, 5, 19; Larjovuori 2004, 17.) Hyvinvointialan palvelutuotanto on tiukasti säädeltyä toimintaa. Sitä ohjaa sosiaali- ja terveysministeriö. Valvontavastuussa ovat lääninhallitukset ja kunnat. (Pajukoski 2004, 80.)

Hyvinvointialan palveluntuottajat toimivat hyvin monimuotoisilla sosiaali- ja terveydenhuollon toimialoilla (Kuvio 2). Tässä työssä hyvinvointialan palveluntuottajilla tarkoitetaan niitä yrittäjä-, järjestö- tai säätiöpohjalta toimivia palveluntuottajia, jotka toimivat sosiaalihuollon majoituksen sisältävien sosiaalipalveluiden sekä sosiaalihuollon avopalveluiden parissa.

Sosiaalipalvelut	Terveydenhoitopalvelut
Majoituksen sisältävät sosiaalipalvelut	**Sairaalapalvelut**
Lasten ja nuorten laitokset	Varsinaiset sairaalapalvelut
Kehitysvammalaitokset	Kuntoutuslaitokset ja sairaskodit
Vanhusten laitokset	**Lääkäripalvelut**
Päihdehuoltolaitokset	Kunnalliset terveyskeskukset
Palvelutalot ja ryhmäkodit	Muut lääkäripalvelut
Ensi- ja turvakodit	**Hammashoito**
Muut laitokset ja asumispalvelut	**Muut terveydenhuoltopalvelut**
Sosiaaliset avopalvelut	Fysioterapia
Lasten päivähoito	Laboratoriotutkimukset
Päivätoiminta	Kuvantamistutkimukset
Kotipalvelut	Sairaankuljetuspalvelut
Työtoiminta ja työhön kuntoutus	Muu terveyspalvelu
Neuvolat	
Avomuotoinen päihdekuntoutus	
Muu sosiaalitoiminta	

Kuvio 2. Sosiaali- ja terveydenhuollon toimialat toimialaluokituksen mukaan (sosiaali- ja terveysalan tietoyhteiskuntayksikkö 2006)

Hyvinvointialan toiminnassa syntyvät asiakirjat ovat suppea yhdistelmä julkisen sosiaali- ja terveydenhuollon asiakas- ja potilasasiakirjoista. Asiakirjamerkinnät liittyvät asiakkaiden asumiseen ja elämiseen. Sosiaalihuollon asiakirjat ja terveydenhuollon potilasasiakirjat eroavat toisistaan paitsi sisällöllisesti myös tiedon lähteiden, salassapito-, säilytys- ja hävittämissäännösten suhteen. Sosiaalialan toiminnassa on huomioitava, että terveydenhuollon ammattihenkilön toteuttaessa terveyden- ja sairaanhoitoa, asiakirjamerkintöihin sovelletaan potilasasiakirjamerkintöjä koskevia säännöksiä riippumatta toimipaikan tai palveluntuottajan toimialasta (Pahlman 2005, 79).

SaaS-ohjelmistopalvelulla tarkoitetaan Internetissä tarjottavaa ohjelmistopalvelua. Ohjelmistopalvelussa tarjotaan asiakkaalle sovelluksen käyttöoikeutta ja käytön edellyttämiä tukipalveluja. Sovellusta ylläpidetään toimittajan omilla tai toimittajan hallinnoimilla palvelimilla. Liiketoimintamalli voi vaihdella eri toteutuksissa, mutta sovelluksen omistusoikeus pysyy aina toimittajalla. Toimittaja kantaa kokonaisvastuun palvelun

edellyttämien toimintaketjun osista sekä niissä esiintyvistä virheistä ja häiriöistä. Asiakas solmii palvelusopimuksen, jonka avulla koko sovelluskokonaisuus palveluineen on hänen käytettävissään. Sovelluksen käyttöpalvelua tarjotaan samanlaisena usealle eri asiakkaalle. Asiakaskohtaista räätälöintiä ei tehdä. Toimintamalli mahdollistaa edullisen hinnoittelun, eikä asiakkaan tarvitse osallistua sovelluksen kehitysriskien kantamiseen. Asiakkaan kaikki tietojärjestelmän käytöstä aiheutuvat kulut ovat ennustettavissa. Usein sovellus on rakennettu siten, että käyttäjäkohtaisten asetusten tekeminen on mahdollista. SaaS-ohjelmistopalvelu nähdään yleensä sovellusvuokrausta (ASP, Application Service Provider) kehittyneempänä toimintamuotona. (Sääksjärvi ym. 2004, 1-4.) Palvelujen suurimmat erot ovat sovelluksen rakenteessa sekä liiketoiminnan toteuttamisessa. Perinteiset ASP-sovellukset ovat useimmiten client-server -tyyppisiä toteutuksia, kun taas onnistuneet Saas-ohjelmistoratkaisut ovat skaalautuvia, konfiguroitavia ja moni-asiakasympäristöön soveltuvia tietojärjestelmiä. (Chong & Carraro 2006; Terrar 2006.)

2.2 Normisto

Tietosuojaa säätelevien normien taustalla on pitkät perinteet. Lääkintäetiikassa Hippokrateen ajoista 400 eKr. aina 1900-luvulle asti potilaan osallistumista hoitoonsa koskevaan päätöksentekoon pidettiin tarpeettomana. Itsemääräämisoikeus, suostuminen tai hoidosta kieltäytyminen tulivat periaatteiksi vasta Nürnbergin sotilasoikeudenkäyntien yhteydessä vuonna 1947. (Heiliö & Ylipartanen 2006b, 633.)

Kansalliset tietosuojanormit noudattavat kansainvälisten ihmisoikeussopimusten henkeä. Normistoa voidaan kuvata kolmikulmiona (Kuvio 3). Kärjessä olevat kansainväliset ihmisoikeussopimukset, Euroopan yhteisön asetukset ja direktiivit sekä kansalliset perusoikeusoikeussäännökset ovat väljästi muotoiltuja ja ne ohjaavat hierarkiassa alempana olevia säännöksiä. Alempana olevien normien tehtävänä on täsmentää ylempiä säännöksiä. Lakeja ja asetuksia heikommin velvoittavia normeja ovat esimerkiksi lakien valmisteluasiakirjat perusteluineen, ylimpien tuomioistuinten ennakkopäätökset, yleiset oikeudelliset periaatteet, oikeuskirjallisuudessa esitetyt kannanotot, laatusuositukset, kunnallisten viranomaisten antamat soveltamisohjeet sekä eri ammattiryhmien omat eettiset ohjeet. (Ylipartanen 2004, 34-36.)

Kuvio 3. Tietosuojan normihierarkia (Ylipartanen 2004, 34)

Normit voivat olla keskenään ristiriitaisia. Jollei normissa ole erityisiä säädöksiä suhteesta muihin normeihin, määräytyy sovellettava käytäntö toisen asteen metanormien perusteella. Lex superior -säännön nojalla ylemmän asteinen normi syrjäyttää alemman asteen normin, esimerkiksi asetuksella ei voida antaa ristiriitaisia ohjeita lakeihin nähden. Jos kaksi samassa tasossa olevaa normia ovat ristiriidassa toisiinsa nähden, sovelletaan lex posterior -sääntöä, jolloin myöhemmin annettu normi syrjäyttää aikaisemmin annetun normin. Lex specialis -periaatteen mukaan erityisnormisto syrjäyttää yleisen tason normit. (Pajukoski 2004, 17.)

2.2.1 Ylimmän asteen normit

Kansainvälisistä ihmisoikeussopimuksista merkittävimpiä ovat Yhdistyneiden kansakuntien ja Euroopan neuvoston jäsenmaiden hyväksymät ihmisoikeussopimukset. Vuonna 1976 Suomessa tulivat voimaan Yhdistyneiden kansakuntien kaksi yleissopimusta. Nämä sopimukset olivat kansalais- ja poliittisia oikeuksia koskeva KP-sopimus ja taloudellisia, sosiaalisia ja sivistyksellisiä oikeuksia koskeva TSS-sopimus. Vuonna 1991 saatettiin voimaan lapsen oikeuksia koskeva yleissopimus, jossa selkeytettiin lapsen kehitystasonsa mukaisia itsenäisiä oikeuksia suhteessa omiin huoltajiinsa. Euroopan ihmisoikeussopimuksen yksityis- ja perhe-elämän, kodin sekä kirjeenvaihtoon kohdistuvasta suojasta Suomi allekirjoitti sopimuksen vuonna 1990. (Ylipartanen 2004, 37-38.)

Euroopan yhteisön henkilötietodirektiivin tarkoituksena on taata, että jäsenmaat turvaavat yksilöiden perusoikeudet henkilötietojen käsittelyssä sekä oikeudet yksityisyyteen. Direktiivi täsmentää Euroopan neuvoston vuoden 1981 yleissopimusta yksilön suojelusta automaattisen tietojenkäsittelyn avulla tapahtuvasta henkilötietojen käsittelystä. Suomi sitoutui noudattamaan näitä sopimuksia vuonna 1992. Direktiivi saatettiin voimaan henkilötietolailla vuonna 1999. (Heiliö & Ylipartanen 2006b, 636-637.)

Yksityiselämän perusoikeudet sisältyvät Suomen perustuslakiin. Perustuslaissa säädetään myös, että henkilötietojen käsittelystä voidaan antaa ohjeita vain lain tasolla. Kaikki viranomaisten asiakirjat ja muut tallenteet on säädetty julkisiksi, joten yksityisellä henkilöllä on oikeus saada tietoa valmisteilla olevista asioista ja hän voi vaikuttaa itseään koskeviin asioihin. Muista poiketen sosiaali- ja terveydenhuollon asiakastiedot on säädetty julkisuuslailla sekä sosiaali- ja terveydenhuollon erityislaeilla salassa pidettäviksi yksityisyyden suojan varmistamiseksi. (Heiliö & Ylipartanen 2006b, 635.)

2.2.2 Henkilötietojen käsittelyä koskevat yleislait

Suomessa ei ole varsinaista tietoturvallisuuslainsäädäntöä. Sen sijaan tietoturvallisuutta koskevia säädöksiä sisältyy useihin eri lakeihin. (Tammisalo 2005, 7.) Tietosuojaa käsittelevistä yleislaeista käsitellään tässä tarkemmin henkilötietolakia. Sosiaali- ja terveydenhuollon tietosuojaa käsittelevistä erityislaeista tarkastellaan seuraavassa luvussa lakia potilaan asemasta ja oikeuksista, lakia sosiaalihuollon asiakkaan asemasta ja oikeuksista sekä sosiaali- ja terveysministeriön antamaa asetusta potilasasiakirjojen laatimisesta. Lopuksi tarkastellaan muutamia muita säädöksiä ja normeja, jotka on huomioitava hyvinvointialan tietojärjestelmiä suunniteltaessa.

Henkilötietolaki (523/99) ohjaa hyvään henkilötietojen käsittelytapaan perustuviin käytäntöihin sekä turvaa yksityisyyttä koskevat perusoikeudet. Yleislakina sitä sovelletaan, ellei muualla lainsäädännössä ole säädetty tästä poikkeavalla tavalla. Lain keskeiset periaatteet ovat suunnitteluvelvoite, käyttötarkoitussidonnaisuus, huolellisuus- ja suojaamisvelvoite sekä tarpeellisuus- ja virheettömyysvaatimus. (Ylipartanen 2004, 179; Pahlman 2005, 23.)

Suunnitteluvelvoitteen mukaan rekisteritietojen kerääminen tulee olla suunnitelmallista ja käsittelyn tarkoitus tulee olla määritetty toimialan perusteella. Tämä tarkoittaa, että vain toiminnan kannalta oleellisia tietoja saa kerätä. Sosiaali- ja terveydenhuollossa perusteltuja tietoja ovat tiedot, jotka liittyvät asiakkaan hoidon suunnitteluun, toteutukseen ja seurantaan. Perusteltua on kerätä tietoja, jotka liittyvät ammattihenkilöiden toimien valvontaan ja asianmukaisuuden arviointiin, oman toiminnan suunnitteluun, ohjaukseen, johtamiseen ja valvontaan sekä lakisääteisten tilastotietojen keräämiseen valtakunnallisiin rekistereihin. Perusteltua on myös laskutukseen liittyvien tietojen kerääminen (Kleemola & Tervo-Pellikka 1998, 51) sekä tietojen käyttäminen tutkimus- ja opetustoimintaan tietyin edellytyksin. Muussa kuin välittömästi asiakkaan asioiden hoitamiseen liittyvässä käsittelyssä tietoja tulee käyttää niin, ettei asiakkaan yksilöinti ole mahdollista. (HetiL 6 §; Ylipartanen 2004, 47.)

Henkilötietolain käyttötarkoitussidonnaisuusperiaatteen mukaan tietoja saa käyttää vain siihen tarkoitukseen, johon ne on kerätty. Sosiaali- ja terveydenhuollossa saa käsitellä arkaluonteisia tietoja, jos niiden käsittely on tehtävän toteuttamisen kannalta välttämätöntä. Arkaluonteisia tietoja ovat tiedot, jotka kuvaavat

- rotua tai etnistä alkuperää
- yhteiskunnallista, poliittista tai uskonnollista vakaumusta tai ammattiliittoon kuulumista
- rikollista tekoa, rangaistusta tai muuta rikoksen seuraamusta
- terveydentilaa, sairautta, vammaisuutta tai henkilöön kohdistettuja hoitotoimenpiteitä tai niihin verrattavia toimia
- seksuaalista suuntautumista tai käyttäytymistä
- sosiaalihuollon tarvetta, saatuja palveluja, tukitoimia tai muita sosiaalietuuksia.

Käyttöoikeuden edellytyksenä on hoito- tai asiakassuhde, jonka perusteella asiakas on tietoinen itseään koskevien asioiden käsittelystä. (HetiL 7, 9, 11-12 §; Ylipartanen 2004, 45-48; Heiliö & Ylipartanen 2006b, 639-641.)

Henkilörekisteri voi koostua erillisistä osarekistereistä. Käytännöllisintä on muodostaa osarekisterit toiminnallisista lähtökohdista tehtävien organisoinnin mukaisesti. Käyttöoikeudet määritellään työtehtävien edellyttämässä laajuudessa, vain omaa työtä koskevia tietoja saa käsitellä. Tietojen käsittelijästä, käsittelijän ammatillisesta asemasta ja käsittelyn ajankohdasta tulee jäädä merkinnät. (Ylipartanen 2004, 47.)

Huolellisuusvelvoite velvoittaa rekisterinpitäjää huolehtimaan, että henkilötietoja käsitellään huolellisesti niin, ettei rekisteröidyn yksityiselämän suojaa loukata tai muita perusoikeuksia rajoiteta ilman lain mukaista perustetta. Arkaluontoisten tietojen käsittelyssä on noudatettava korostettua huolellisuutta. Suojaamisvelvoite velvoittaa rekisterinpitäjää huolehtimaan tarpeellisista teknisistä toimenpiteistä, kuten suojaamaan asiattomalta tietoihin pääsyltä, laittomalta tai vahingossa tapahtuvalta tietojen hävittämiseltä, muuttamiselta, luovuttamiselta tai siirtämiseltä. Huolellisuus- ja suojaamisvelvoitteet ulottuvat myös tekniseen rekisterinpitäjään. Tekninen rekisterinpitäjä huolehtii rekisterinpidon käytännön toimenpiteistä. Tietojenkäsittelyn ulkoistamisesta on sovittava aina kirjallisella toimeksiantosopimuksella. Palvelun ostaja eli rekisterinpitäjä vastaa tietosuojasta varmistumalla, että toimeksiantotehtävässä tietosuoja toteutuu. Toimeksiantajan ja -saajan tulee tehdä ilmoitukset tietosuojavaltuutetun toimistolle ulkoistetusta tietojenkäsittelypalvelusta. (HetiL 5, 32, 36 §; Ylipartanen 2004, 25, 66-67, 82-83.)

Virheettömyysvaatimus edellyttää rekisterinpitäjän huolehtimaan, etteivät rekisterissä olevat tiedot ole epätäydellisiä, vanhentuneita tai virheellisiä. Tieto on virheetöntä, kun se vastaa todellisuutta sekä antaa oikeaa ja riittävän laajaa informaatiota niistä seikoista, joita sillä on haluttu kuvata. Jos tieto perustuu muuhun kuin ammattihenkilön omiin tutkimuksiin ja havaintoihin, tiedon yhteyteen on merkittävä tiedonlähde. Asianomaisella on tarkastusoikeus omiin tietoihinsa. Virheelliset, puutteelliset tai vanhentuneet tiedot on oikaistava, täydennettävä tai poistettava. Tarpeettomat tiedot poistetaan rekisteristä kokonaan. Virheelliset merkinnät korjataan siten, että alkuperäinen ja korjattu tieto sekä korjaaja ja korjausajankohta ovat myöhemmin selvitettävissä. (HetiL 9, 26 §; Kleemola 1999, 168-169; Ylipartanen 2004, 55, 139-144; Heiliö & Ylipartanen 2006b, 644-646.)

Henkilötietolaki määrittelee rekisterinpitäjälle velvollisuuden laatia pitämistään rekistereistä rekisteriselosteen ja pitämään tätä selostetta jokaisen saatavilla. Tätä kutsutaan laissa informointivelvollisuudeksi. Rekisteriselosteesta tulee tulla ilmi mm. rekisterinpitäjän tiedot, henkilötietojen käsittelyn tarkoitus, rekisterin sisältämien tietojen laatu, tietojen säännönmukaiset luovutukset sekä rekisterin suojauksen perusperiaatteet. (HetiL 24 §; Narikka 2006, 697-698.)

Henkilötietoja käsittelevällä henkilöstöllä on henkilötietolain mukaan laaja vaitiolovelvollisuus. Vaitiolovelvollisuus sitoo rekisterinpitäjän lisäksi kaikkia rekisterinpitäjän

palveluksessa olevia henkilöitä sekä sopimukseen perustuvia tehtäviä suorittavia henkilöitä. Näitä voivat olla esimerkiksi tietojenkäsittelytehtävissä työskentelevät henkilöt. Vaitiolovelvollisuus säilyy, vaikka työtehtävä tai palvelussuhde päättyy. (HetiL 3 §; Ylipartanen 2004, 62.)

Henkilötietolaissa säädetään henkilörekisteririkkomuksesta ja vahingonkorvausvastuusta. Rangaistusuhan kohdistaminen epäasiallista henkilötietojen käsittelyä vastaan jo suunnitteluvaiheessa on ennaltaehkäisevässä mielessä perusteltua. Henkilörekisteririkkomuksella tarkoitetaan mm. tietojen suojaamisen ja rekisteritietojen hävittämisestä annettujen säädösten rikkomista. Rikkomuksesta voidaan tuomita sakkorangaistukseen. Vahingonkorvausvastuun mukaan rekisterinpitäjä on vastuullinen korvaamaan aiheuttamansa taloudellisen tai muun vahingon, jonka lain vastainen toiminta on rekisteröidylle aiheuttanut. (HetiL 47-48 §; Ylipartanen 2004, 150-156.) Lampolan ym. (2003, 35, 46) mukaan ohjelmistopalveluntuottajan vastuu on sopimusoikeudellista vastuuta, joten palveluntuottaja vastaa rikkomuksistaan vain siinä määrin kuin ohjelmistopalvelusopimuksessa on määritelty.

Henkilötietojen käsittelyä koskevia yleisluonteisia ohjeita on myös julkisuus- ja arkistointilaissa. Julkisuuslaissa (621/99) ovat säädökset viranomaisten toiminnan julkisuudesta ja eräiden asioiden salassa pidettävyydestä. Arkistolaki (831/94) antaa ohjeet julkisten viranomaisten asiakirjojen säilyttämisestä (Pahlman 2005, 145). Lakien velvoitteet koskevat yksityistä ja kolmannen sektorin palveluntuottajia vain niiltä osin, kun ne toimivat julkisen organisaatioon lukuun toimeksiantosopimuksella. (Ylipartanen 2004, 51.) Toimeksiantosopimuksella kunta tai muu julkinen organisaatio sopii sille lakisääteisesti määrättyjen tehtävien hoitamisesta (Tietosuojavaltuutetun toimisto 2001, 23), joten näitä lakeja ei käsitellä tässä yhteydessä.

2.2.3 Henkilötietojen käsittelyä koskevat erityislait ja -asetukset

Laissa potilaan asemasta ja oikeudesta (785/1992), tässä opinnäytetyössä potilaslaki eli PotL, annetaan määräyksiä potilasasiakirjojen laatimisesta ja salassa pidettävyydestä. Potilaslakia sovelletaan kaikkiin julkisessa tai yksityisessä terveydenhuollossa toimiviin henkilöihin ammatillisesta koulutuksesta tai toimipaikan toimialasta huolimatta.

Potilasasiakirjat ovat terveydenhuollossa syntyviä terveydenhuollon asiakirjoja. Potilaslain mukaan myös sosiaalihuollon terveyden- ja sairaanhoitoon liittyvissä tehtävissä syntyneet asiakirjat ovat potilasasiakirjoja. Potilasasiakirjoina niitä koskevat potilaslain mukaiset määräykset. (PotL 12-13 §; Heiliö & Ylipartanen 2006b, 648.)

Potilaslain mukaan potilasasiakirjoihin merkitään kaikki potilaan hoidon järjestämisen, suunnittelun, toteuttamisen ja seurannan kannalta oleelliset tiedot. Potilasasiakirjat säilytetään hoidon toteuttamisen ja järjestämisen, mahdollisten korvausvaatimusten sekä tieteellisen tutkimuksen edellyttämän ajan. Tämän jälkeen potilasasiakirjat tulee hävittää asianmukaisesti. Ohjeet säilyttämisajoista ovat sosiaali- ja terveysministeriön asetuksessa potilasasiakirjojen laatimisesta sekä niiden ja muun hoitoon liittyvän materiaalin säilyttämisestä (99/2001). Tietoja saa säilyttää asetuksen määrittämän säilytysajan jälkeen, jos säilyttäminen on välttämätöntä hoidon järjestämisen kannalta. (PotL 12 §; Heiliö & Ylipartanen 2006b, 649, 653.)

Potilasasiakirjatietojen salassapitovelvoite on laaja. Salassa pidettäviä ovat kaikki tiedot, eivät pelkästään henkilötietolain määrittelemät arkaluonteiset tiedot. Velvoite koskee kaikkia toimintayksikössä työskenteleviä, myös opiskelijoita ja harjoittelijoita, tai toimeksiantosopimuksen perusteella tietoja käsitteleviä henkilöitä. Salassapitovelvoite säilyy henkilötietolain salassapitovelvoitteen tapaan myös työtehtävän, palvelussuhteen tai ammatinharjoittamisen päättymisen jälkeenkin. (PotL 13 §; Heiliö & Ylipartanen 2006c, 659.)

Sosiaali- ja terveysministeriön asetus potilasasiakirjojen laatimisesta sekä niiden ja muun hoitoon liittyvän materiaalin säilyttämisestä (99/2001) tarkentaa potilaslakia ja sen määräyksiä. Asetuksesta käytetään tässä työssä lyhennettä PotA. Yksityiskohtainen sääntely perustuu sekä alan käytännön toimijoiden että viranomaisten esittämiin toiveisiin. Sääntely edistää osaltaan palvelujen hyvää laatua sekä rekisteröidyn oikeusturvaa. (Pahlman 2005, 78-79.) Asetuksessa annetaan ohjeita potilasasiakirjojen tekniseen toteutukseen liittyvistä seikoista, rekisterinpitäjän vastuista, potilasasiakirjoihin tehtävistä merkinnöistä ja niiden korjaamisesta sekä säilyttämisestä.

Potilasasetuksen mukaan rekisterinpitäjän vastuulla on huolehtia, että potilasasiakirjajärjestelmä on toteutettu siten, että sen rakenne vastaa rekisterin käyttötarkoitusta ja

hoitoon osallistuvien henkilöiden tehtäviä. Erityisesti on huolehdittava tietojen eheydestä ja käytettävyydestä tietojen säilytysaikana. (PotA 3 §.) Eheys on laajasti käsitettynä sitä, että tiedot ovat paikkansa pitäviä eivätkä sisällä virheitä. Käytettävyys tarkoittaa tietojen tallentamista sellaisessa muodossa, että tiedot on saatavissa käyttöön kaikissa tilanteissa ja tarkoituksenmukaisessa ajassa. (Hakala ym. 2006, 4.) Tietojärjestelmän käyttöoikeuksia tulee voida määritellä yksityiskohtaisesti. Tietojärjestelmän käyttöä vain ammattitehtävien hoitoon liittyvinä välttämättöminä toimina on voitava valvoa riittävin teknisin menetelmin. Rekisterinpitäjän tulee myös varmistua, että salassapito- ja vaitiolovelvollisuutta noudattavat sekä hoitoon osallistuva että ulkoistettujen tietojenkäsittelypalveluiden henkilöstö. (PotA 4 §.)

Merkintöjä potilasasiakirjoihin saavat ja ovat velvollisia tekemään kaikki hoitoon osallistuvat terveydenhuollon ammattihenkilöt. Ammattihenkilöiden ohjeiden perusteella muut hoitoon osallistuvat henkilöt, kuten esimerkiksi opiskelijat, saavat tehdä merkintöjä potilasasiakirjoihin. Merkintöjen tulee olla selkeitä, virheettömiä ja käsitteiden ymmärrettäviä sekä yleisesti tunnettuja. Tietojen alkuperä tulee kirjata, jos tieto perustuu johonkin muuhun kuin kirjaajan omiin havaintoihin. Merkinnät kirjataan viivytyksettä. (PotA 6-7 §; Pahlman 2005, 79-81.)

Potilasasetuksen edellyttämät merkinnät potilaan hoidosta ovat yksityiskohtaisia. Tietoihin on kirjattava mm. potilaan perustiedot, keskeiset hoitotiedot sekä sairauden ja hoidon kulkuun liittyvät seikat, riskit, hoidon haitalliset vaikutukset ja epäillyt hoitovahingot. Lisäksi on kirjattava konsultaatiot ja hoitoneuvottelut, potilaan tiedonsaantiin ja hoitoon liittyvät kannanotot sekä tietojen luovuttamiseen liittyviä asioita. Osastohoitojaksoista edellytetään lisäksi merkittävän eräitä hoitoa tarkentavia seikkoja. Tietyt perustiedot ovat pakollisia. Osa potilastiedoista merkitään vain, jos ne ovat merkityksellisiä potilaan hoidon kannalta. Kuvioon 4 on kerätty potilasasetuksen vaatimat keskeiset potilasasiakirjojen tietosisällöt niiltä osin, kun ne koskevat avo- ja asumispalvelua tarjoavan hyvinvointiyrityksen potilaskirjauksia. Näiden tietojen lisäksi on pystyttävä esimerkiksi työvuorolistoista selvittämään, ketkä terveydenhuollon ammattihenkilöt ovat osallistuneet potilaan hoitoon. (PotA 10-19 §; Pahlman 2005, 83-87.)

Pakolliset perustiedot	Tarvittaessa merkittävät perustiedot
Nimi, syntymäaika, henkilötunnus Kotikunta, yhteystiedot Hoidon toteuttanut ammattihenkilö Kirjaajan nimi, asema ja ajankohta Saapuneiden asiakirjojen saapumispäivä ja lähde	Lähiomainen tai muu yhteyshenkilö, sukulaissuhde, yhteystiedot Alaikäisen huoltaja tai laillinen edustaja, yhteystiedot Potilaan äidinkieli, asiointikieli, ammatti Hoidosta vastaava lääkäri Potilaan suostuminen tietojen luovuttamiseen
Keskeiset hoitotiedot jokaisesta avohoitokäynnistä, kotihoitokäynnistä ja osastojaksosta	
Tulosyy, esitiedot Nykytila, havainnot, tutkimustulokset, ongelmat Taudinmääritys, terveysriski, johtopäätökset Hoidon suunnittelu, toteutus, seuranta Sairauden kulku, tehdyt hoitopäätökset perusteluineen Lääkemääräykset, lausunnot, todistukset antamisajankohtineen Loppulausunto sisältäen jatkohoito-ohjeet ja potilaan tilan kuvaus	
Riskit, hoidon haitalliset vaikutukset, epäillyt hoitovahingot	
Lääkeaineallergiat, materiaaliallergiat, yliherkkyydet ja muut vastaavat Tutkimus- ja hoitotoimenpiteiden haitalliset vaikutukset, hoidon tehottomuus Epäillyt potilas-, laite- ja lääkevahingot, kuvaukset vahingosta, mukana olleista ammattihenkilöistä ja epäillyt vahingon syyt	
Osastohoitojakso	
Potilaan tilan muutokset aikajärjestyksessä Tehdyt tutkimukset, annetut hoidot Seurantatiedot potilaan tilasta, hoitotoimista ja muista vastaavista seikoista, seurantayhteenveto	
Konsultaatiot ja hoitoneuvottelut	
Ajankohta, osallistuneet henkilöt, tehdyt päätökset Päätösten toteuttaminen	
Potilaan tiedonsaantiin ja hoitoon liittyvät kannanotot, tietojen luovutukset	
Selvitys tehdyistä tutkimuksista ja annetuista hoidoista, mahdollisen kieltäytymisen peruste Potilaan kieltäytyminen hoidosta tai tutkimuksesta, luovutuksesta Hoitotahto Merkintä yhteisymmärryksestä alaikäistä lasta hoidettaessa Potilaan antama lupa kertoa hoidettavana olosta Mihin, kenelle, milloin tietoja on luovutettu, luovuttaja, peruste,	

Kuvio 4. Potilasasetuksen (10-19 §) edellyttämät potilasasiakirjojen keskeiset tietosisällöt niiltä osin, kun ne koskevat avo- ja asumispalvelua tarjoavan hyvinvointiyrityksen potilaskirjauksia

Terveydenhuollon toimintayksikön tulee asetuksen mukaan pitää kustakin potilaastaan aikajärjestyksessä etenevää potilaskertomusta (PotA 9 §, Ylipartanen 2004, 56-57; Pahlman 2005, 82). Kertomuksen tulee olla alkuperäinen eli edes osia siitä ei saa korvata kopioilla. Merkintöjen korjaukset tulee tehdä niin, että myös alkuperäinen merkintä on mahdollista jälkikäteen selvittää. Korjaus voidaan tehdä esimerkiksi siirtämällä alkuperäinen tieto taustatiedostoon. Korjauksiin on aina merkittävä korjauspäivä, korjaajan nimi, korjaajan ammatillinen tehtävä sekä korjauksen peruste. (PotA 20 §; Pahlman 2005, 82, 91.)

Tietyt potilasasiakirjamerkinnät edellyttävät laatijan omakätistä allekirjoitusta. Allekirjoitusta vaativat lähete, hoidon loppulausunto, hoidon yhteenveto, lausunto ja muut vastaavan luonteiset asiakirjat. Asetus hyväksyy myös sähköisen varmennetun allekirjoituksen, jos se ”täyttää hallinnon sähköistä asiointia koskevassa lainsäädännössä asetetut vaatimukset”. (PotA 7 §.) Laki sähköisistä asioinnista hallinnossa (1318/1999) korvattiin vuonna 2003 voimaan astuneella lailla sähköisestä asioinnista viranomaistoiminnassa (13/2003) (Pajukoski 2004, 18). Pahlmanin (2005, 81) mukaan potilasasetuksessa tarkoitetaan vuonna 2003 voimaan astuneen lain sähköisistä allekirjoituksista mukaista laatuvarmenteeseen perustuvaa sähköistä allekirjoitusta. Sosiaali- ja terveydenhuollon sähköisestä asiakirjakäsittelystä säädetään uudella lailla, joka on erityislain asemassa suhteessa edellä mainittuihin.

Potilasasetus määrää potilasasiakirjojen säilyttämisvastuun sille toimintayksikölle, jonka toiminnassa tiedot ovat syntyneet. Toimintayksikkö on velvollinen säilyttämään potilasasiakirjoja potilaan kuoleman jälkeen vielä 10 vuotta. Jos kuolinpäivästä ei ole tietoa, potilasasiakirjoja on säilytettävä 100 vuotta potilaan syntymästä. Samanaikaisesti hoidon päättymisestä tulee olla vähintään 10 vuotta. Hoitojaksokohtaiset tiedot samoin kuin lähetteet, muualta saapuneet asiakirjajäljennökset, laboratoriotutkimustulokset sekä lääkärinlausunnot ja -todistusjäljennökset voidaan hävittää 10 vuoden kuluttua hoidon päättymisestä. Tämä edellyttää, että potilaan hoidon kannalta olennaisista tiedoista on tehty tiivistelmä, joka sisällytetään muihin jatkuvakäyttöisiin potilasasiakirjoihin. Ajanvaraus- ja hoidon varaustiedot voidaan hävittää kahden vuoden kuluttua käynnin tai hoidon toteutumisesta. Säilyttämisajat ovat vähimmäisaikoja. Potilasasiakirjoja voidaan säilyttää pidempään, jos säilyttäminen on tärkeää hoidon tai sen järjestämisen kannalta. Säilyttämistarve arvioidaan vähintään viiden vuoden välein. Potilasasiakirjojen hävittäminen on toteutettava niin, ettei kukaan sivullinen saa niistä tietoa. (PotA 22-23 §, Liite; Pahlman 2005, 94-95.)

Laki sosiaalihuollon asiakkaan asemasta ja oikeuksista, sosiaalihuollon asiakaslaki, on potilaslain tavoin henkilötietolakia täydentävä. Asiakaslain tavoitteena on vahvistaa asiakkaan asemaa ja oikeusturvaa. Sitä sovelletaan sekä julkiseen että yksityiseen sosiaalihuoltoon, mutta osa säännöksistä koskee vain julkista tai vain yksityistä sosiaalihuoltoa. Tässä työssä käsitellään vain yksityistä palveluntarjoajaa koskevia säännöksiä. (SHAL 2 §; Pahlman 2005, 112; Heiliö & Ylipartanen 2006b, 649.)

Asiakaslaki määrittelee asiakasasiakirjat salassa pidettäviksi. Sosiaalihuollon asiakastiedot ovat arkaluonteisia tietoja, joten niiden salassapito- ja vaitiolovelvollisuus on laaja. Yksityistä sosiaalihuoltoa järjestettäessä tulee palvelu perustua aina palveluntuottajan ja asiakkaan väliseen kirjalliseen sopimukseen. Palvelua tuotettaessa kaikille asiakkaille on laadittava palvelu-, hoito- tai kuntoutussuunnitelma. Suunnitelmaa ei tarvitse laatia, jos palvelu on tilapäistä toimintaa. Asiakkaalla on itseään koskevien tietojen tarkastusoikeus. (SHAL 6-7, 14-15 §; Heiliö & Ylipartanen 2006c, 660.)

Sosiaalihuollon asiakasasiakirjojen laatimisesta tai säilyttämisestä ei ole olemassa yksityiskohtaisia normistoja. Asiakirjojen laatimisessa ja tietojen korjaamisessa voidaan Heiliön ja Ylipartasen mukaan kuitenkin noudattaa soveltuvin osin potilasasetuksen mukaisia toimintaohjeita ja sääntöjä. Yksityisen sosiaalihuollon asiakasasiakirjoja voidaan heidän mukaan säilyttää niin kauan kuin asiakassuhde kestää. Asiakassuhteen katsotaan katkenneen, kun asiakas ei enää asu toimintayksikössä tai käytä sen palveluja. Määräaikaista katkosta ei lueta asiakassuhteen katkeamiseksi. Jos asiakastietojen säilyttämiselle ei ole muuta laillista perustetta, tiedot on hävitettävä. Hävittämistavan tulee olla luotettava. (Pahlman 2005, 116; Heiliö & Ylipartanen 2006b, 650, 654.)

2.2.4 Muut huomioitavat normit

Lakia sähköisistä allekirjoituksista (14/2003), tässä SähkAL, sovelletaan kaikkiin sähköisiin allekirjoituksiin. Tässä yhteydessä sen keskeisimmät säännökset ovat sähköisen allekirjoituksen ja kehittyneen sähköisen allekirjoituksen määritelmät. Sähköinen allekirjoitus asiakirjaan liitettynä yksilöi allekirjoittajan ja on todiste sekä asiakirjan että allekirjoittajan aitoudesta. Sähköisellä allekirjoituksella myös varmistetaan asiakirjan eheys. Käytännössä allekirjoitus tehdään epäsymmetrisellä salauksella, jossa asiakirjan tiiviste salataan allekirjoittajan salaisella avaimella. Allekirjoitus puretaan allekirjoittajan ilmoittamalla julkisella avaimella. Allekirjoitus on matemaattisesti kiistämätön, sillä tiivistefunktio ei salli asiakirjaan tehtäviä muutoksia. (Tammisalo 2005, 104.)

Laki sähköisistä allekirjoituksista määrittelee sähköisen allekirjoituksen sähköisessä muodossa olevaksi tiedoksi, joka on liitetty tai loogisesti liittyy muuhun sähköiseen tietoon ja jota käytetään allekirjoituksen tekijän henkilöllisyyden todentamiseen.

Kehittynyt sähköinen allekirjoitus liittyy allekirjoittajaan yksiselitteisesti, allekirjoittaja voidaan yksilöidä sen avulla. Kehittynyt sähköinen allekirjoitus luodaan menetelmällä, joka on vain allekirjoittajan valvonnassa ja se liittyy muuhun sähköiseen tietoon niin, että mahdolliset tiedon muutokset ovat havaittavissa. Kehittyneen sähköisen allekirjoituksen luotettavuuden taso on korkeampi kuin sähköisen allekirjoituksen. Manuaalisesti toimittaessa kehittynyt sähköinen allekirjoitus vastaisi henkilöllisyystodistuksen esittämistä tai omakätisesti allekirjoitettua ja kahden henkilön omakätisesti oikeaksi todistamaa asiakirjaa. Laissa sähköisistä allekirjoituksista määritellään myös turvallinen allekirjoituksen luomisväline. Luomisvälineelle asetettujen ehtojen mukaan on riittävän luotettavasti varmistuttava luomistietojen ainutkertaisuudesta ja luottamuksellisuudesta sekä siitä, ettei allekirjoituksen luomistietoja voida päätellä muista tiedoista. Lisäksi allekirjoitus on suojattava väärentämiseltä. Allekirjoittajan tulee voida suojata luomistiedot muiden käytöltä. Luomisväline ei saa muuttaa asiakirjan tietoja eikä estää tietojen esittämistä allekirjoittajalle itselleen. (SähkAL, 1, 5 §; Pajukoski 2004, 22, 43.)

Laatuvarmenteeseen perustuva sähköinen allekirjoitus edustaa sähköisen allekirjoituksen korkeinta tasoa. Siinä allekirjoittaja ja asiakirja todennetaan laatuvarmenteella, jota voi toistaiseksi Suomessa myöntää ainoastaan Väestörekisterikeskus. Manuaalisesti toimittaessa laatuvarmenteen käyttäminen vastaisi tilannetta, jossa julkinen notaari vahvistaa allekirjoituksen aitouden ja asiakirjan muuttumattomuuden. Viranomaisten päätöksistä ilmoitettaessa vaaditaan laatuvarmenteella varmistettua kehittynyttä sähköistä allekirjoitusta. (Pajukoski 2004, 22, 43-44.)

Lain sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä, tässä lyhenne SoTeSKL 159/2007, tarkoituksena on edistää asiakastietojen tietoturvallista käsittelyä. Laki astuu voimaan 1.7.2007. Sen asettamia velvoitteita on noudatettava viimeistään neljän vuoden kuluessa. Tätä opinnäytetyötä tehdessä lain käsittely oli osittain kesken, joten tietolähteenä on pääosin käytetty hallituksen lakiesitystä ja siihen liittyviä perusteluja. Lakiesityksestä käytetään tässä työssä merkintää HE 253/2006. Laki sisältää yleisluontoisia säännöksiä alan asiakastietojen sähköisen käsittelyn periaatteista. Tarkemmat teknistä toteuttamista koskevat ohjeet tullaan kirjaamaan lakiin liittyvään asetukseen tai myöhemmin uudistettavaan potilasasetukseen. Asetusten sisällöistä ei ole saatavilla tietoa tätä työtä kirjoitettaessa. Sähköisen asiakastietojen käsittelyn yleiset vaatimussäädökset velvoittavat kaikkia julkisia ja yksityisiä palveluntuottajia heidän järjestäessään

tai toteuttaessaan sosiaalihuoltoa tai terveydenhuoltoa. Sen sijaan potilasasiakirjojen tietorakenne- ja valtakunnallisiin palveluihin liittymisvelvoitteet koskevat toistaiseksi vain julkisia terveydenhuollon organisaatioita sekä niitä yksityisiä terveydenhuollon palveluntuottajia, joiden potilasasiakirjojen pitkäaikaissäilytys toteutetaan sähköisenä arkistointina. (HE 253/2006, 29, 50, 60; SoTeSKL 159/2007, 1-2, 24-25 §.)

Lakiesityksen perustelujen mukaan sosiaali- ja terveydenhuollon asiakastietojen sähköisen käsittelyn yleisiksi vaatimuksiksi kuuluvat velvoitteet turvata asiakastietojen saatavuus, käytettävyys, eheys sekä muuttumattomuus. Tiedon saatavuudella tarkoitetaan tiedon olemassaoloa asiakirjoissa. Käytettävyydellä tarkoitetaan sitä, että tieto käsittelymekanismeineen tulee aina tarvittaessa olla siihen oikeutettujen käyttäjien saatavilla. Eheydellä tarkoitetaan tietojen virheetöntä käsittelyä koko käsittelyprosessin ajan. Yleisiä vaatimuksia ovat myös asiakastiedon käytön ja luovutuksen seurantavelvoite sekä velvoite tunnistaa ja todentaa käsittelyn osapuolet luotettavasti. Asiakirjan muuttumattomuus ja kiistämättömyys on varmistettava kehittyneellä sähköisellä allekirjoituksella. Nämä yleiset vaatimukset ovat voimassa koko asiakastietojen säilytysajan. Sähköisestä asiakirjasta tulee olla olemassa vain yksi alkuperäis-tunnisteella merkitty asiakirja. Valtakunnallista arkistoa varten asiakirjat tulee yksilöidä yksiselitteisesti ISO-standardin (International Organization for Standardization) mukaisella OID-yksilöintitunnuksella (Object Identifiers). OID-yksilöintitunnus on kansainvälisesti vain yhteen objektiin liitettävä numeroarvo, joka yksilöi sen yksiselitteisesti ISO-yksilöintijärjestelmässä (JUHTA 2004). Asiakirjojen yksilöimisestä ja säilytysajoista säädetään tarkemmin lakiin liittyvässä asetuksessa. (HE 253/2006, 36, 51-52; SoTeSKL 159/2007, 4 §.)

Asiakastietojen käytön ja luovutuksen seurantavelvoite täyttyy, kun rekisterinpitäjä ylläpitää ja seuraa aktiivisesti käyttöoikeusrekisteriä, käyttäjäkohtaista lokitietoa sekä asiakirjatietojen luovutuslokia. Käyttölokiin kerätään tiedot käytetyistä asiakastiedoista, palvelujen antajasta, asiakastietojen käyttäjästä, tietojen käyttötarkoituksesta ja käyttöajankohdasta. Luovutuslokiin kerätään luovutuksiin liittyvät tiedot. Lokitietojen keräämisestä ja lokitietojen säilyttämisestä säädetään tarkemmin lakiin liittyvässä asetuksessa. (HE 253/2006, 52-53; SoTeSKL 159/2007, 5 §.)

Henkilötietojen käsittelyn osapuolten tunnistamis- ja todentamisvelvoite täyttyy, kun on voitu varmistua, että asioinnin osapuolet todella ovat niitä, joita ne ilmoittavat olevansa.

Sosiaali- ja terveydenhuollon sähköisessä asiakastietojen käsittelyssä asiakas, palveluiden antaja, muu mahdollinen osapuoli sekä tietotekniset laitteet tulee tunnistaa ja todentaa luotettavasti. (HE 253/2006, 54.) Tunnistamisen tai todentamisen tahallinen tai törkeästä huolimattomuudesta johtuva rikkomus on asiakastietojen käsittelyrikkomus, josta voidaan tuomita sakkoihin (SoTeSKL 159/2007, 23 §). Tunnistamiseksi kutsutaan menettelyä, jolla yksilöidään tietojärjestelmän käyttäjä. Tyypillisesti tunnistaminen toteutetaan tarkistamalla, onko käyttäjätunnus hyväksyttävien tunnusten joukossa. Tunnistaminen voidaan tehdä perinteisesti syöttämällä käyttäjätunnus tietojärjestelmään tai toimikortilla, jossa käyttäjätunnus on tallennettu magneettinauhaan tai mikrosiruun. Todentamisella varmistetaan käyttäjätunnuksen käyttäjän aitous ja oikeellisuus. Todentaminen toteutetaan vertaamalla tunnistetta vastaanottajalla käyttäjästä olevaan tietoon, muun luotettavan tahon tai varmentajan vahvistamaan tietoon. Tavanomaisin todentautumiskeino on tietää käyttäjätunnukseen liittyvä salasana tai PIN-koodi (Personal Identification Number). (Pajukoski 2004, 21-22; Tammisalo 2005, 110-111.) Käytännön tunnistamisen ja todentamisen teknisestä toteutuksesta esitetään säädettäväksi asetuksella (SoTeSKL 159/2007, 8 §).

Lain sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä mukaan luonnollisen henkilön, organisaation ja tietoteknisten laitteiden sähköisissä allekirjoituksissa tulee käyttää sähköisistä allekirjoituksista annetussa laissa määriteltyä kehittynyttä allekirjoitusta. Sitä on käytettävä asiakastietojen käsittelyssä, tiedonsiirrossa ja säilytyksessä. (SoTeSKL 159/2007, 9 §.)

Sähköisen viestinnän tietosuojalakia (516/2004), tässä SVTSL, sovelletaan yleisissä viestintäverkoissa tarjottaviin verkkopalveluihin, lisäarvopalveluihin sekä palveluiden käyttöä kuvaaviin tietopalveluihin. Yleisillä viestintäverkoilla tarkoitetaan verkkoja, joita tarjotaan etukäteen rajaamattomalle käyttäjäpiirille. Hyvinvointialan toiminnanohjauksen ja asiakashallinnan sovellus ei ole tarkoitettu rajaamattomalle käyttäjäpiirille, joten sähköisen viestinnän tietosuojalain säädöksiä ei käsitellä tässä yhteydessä. (SVTSL, 3 §; Helopuro, Perttula & Ristola 2004, 13-14.)

Tietoturvan suunnittelua varten on luotu erilaisia tietoturvastandardeja. Standardit eivät sinällään takaa turvallisuutta, mutta niitä noudattamalla voidaan tavoitella hyvää tietoturvatasoa. Yksi keskeisimmistä ja tunnetuimmista tietoturvasuunnittelua ohjaavista

standardeista on ISO 17799. Se on tietoturvan hyvän käytännön yleisstandardi, joka määrittelee menettelytapaohjeet tietoturvallisuuden suunnitteluun, ylläpitoon ja kehittämiseen. Standardi ei anna määräyksiä teknisistä ratkaisuista vaan toimii työvälineenä omien turvallisuuskäytäntöjen laadinnassa ja toisaalta niiden kattavuuden arvioinnissa. (Hakala ym. 2006, 46-48.) Kuviossa 5 on esitetty tietosuojan toteutumiseen liittyviä ISO 17799 -standardin kontrolleja sekä lisäkontrolleja sovelluskehitykselle ja -ohjelmoinnille.

Sovelluskehitys	
Tavoite: Varmistaa sovellusten ja niiden tietojen turvallisuus	
Kohde	**Kontrolli**
Muutosten hallinta	Edellyttää muodollista muutoksen hallinta- ja hyväksymismenettelyä.
Ohjelmistomuutokset	Ei suositella, rajoitetaan välttämättömiin muutoksiin, edellyttää tarkkuutta.
Tietovuodot	Mahdollisuudet tietojen vuotamiseen estetään.
Ulkoistettu sovelluskehitys	Ulkoistetun sovelluskehityksen toimintaa seurattava ja valvottava.
Lisäkontrollit	
Dokumentointi	Dokumentointiohjeet. Selkeä dokumenttihierarkia ja -rakenne. Määritellyt työvälineet. Henkilöstön koulutus. Selkeät vastuut.
Versionhallinta	Dokumentointijärjestelmään yhteydessä oleva versiointijärjestelmä. Versiointi erottelee eri vaiheessa olevat ohjelmistokoodit ja muutokset. Muodollinen hyväksymismenettely. Selkeät vastuut.
Käännösten hallinta	Muodollinen menettely käännösajojen suorittamiseksi. Selkeät vastuut.
Testaus	Sovelluskehitys ja testaus erotettu toisistaan. Vakioidut laite- ja käyttöjärjestelmäkokoonpanot. Suunnitelmalliset testausaineistot.
Ohjelmistotuki	Ohjeet asiakaspalautteen keräämiseen, ongelmien ja ratkaisujen kuvaamiseen ja tallentamiseen. Selkeät vastuut.
Sovellusohjelmointi	
Tavoite: Ehkäistä virheet, tietojen häviäminen, tietojen muuttaminen sekä tiedon väärinkäyttö	
Kohde	**Kontrolli**
Syötteet	Oikeellisuus ja täydellisyys tarkistettava ja varmistettava.
Sisäinen toiminta	Mekanismit, joilla havaitaan tietojen tahaton/ tahallinen muuttaminen.
Sanomaeheys	Sanomien autenttisuus- ja eheystarpeet määritetty ja toteutettu.
Tulostustiedot	Oikeellisuus ja käyttökelpoisuus varmistettava.
Lisäkontrollit	
Käyttöliittymä	Yksinkertaisuus, noudatetaan yleisiä graafisia suunnitteluperiaatteita. Korjaamisen tai hallitun keskeyttämisen mahdollistavat virheilmoitukset.
Syöttötietojen täydellisyys	Toiminnan kannalta pakollisten tietojen tarkistus ennen tallentamista tai käsittelyä. Ennen tarkistusta ohjauselementit pois käytöstä.
Näppäiltävä syöte	Merkki-, raja-arvo- ja tarkistusrutiinit käytössä syötteen oikeellisuustarkistuksissa. Korjaamiseen tai tietojen hylkäämiseen ohjaava virheilmoitus, jota ei voi ohittaa.

Kuvio 5. Eräitä ISO 17799 -standardin kontrolleja sekä lisäkontrolleja sovelluskehitykselle ja -ohjelmoinnille (mukailtu Hakala ym. 2006, 317-321)

Terveydenhuollon sähköisten järjestelmien kehitystyössä on kansainvälisesti käytetty ISO 27799 Health Informatics – Security Management on Health Using ISO/IEC 17799 -standardiluonnosta. Luonnos esittää vaatimukset arkaluontoisten tietojen käsittelyn luottamuksellisuudelle, tietojen muuttumattomuudelle ja saatavuudelle. Vaatimuksia on esitetty kaikille tietoturvallisuuden osa-alueille. Ohjelmisto- ja ohjelmistopalvelutuotannossa on huomioitava mm. seuraavia tietoturvavaatimuksia:

- Tietoturvariskien hallintaa varten on luotava kuvailevat kriteerit.
- Potilastietoja käsittelevälle omalle ja ulkoisten osapuolien henkilöstölle on laadittava salassapito- ja muut sopimusmenettelyt.
- Potilastietojen käsittelyssä käytettäviä tietojärjestelmiä, laitteistoa, ohjelmistoa tai tietovälinettä ei saa poistaa ilman lupaa.
- Käytöstä poistettavat tietojärjestelmät, laitteistot ja tietovälineet on tyhjennettävä potilastiedoista tai tuhottava fyysisesti luotettavalla tavalla.
- Potilastietojen käsittelyyn ja säilytykseen tarkoitettujen tietojärjestelmien kehitys- ja testausympäristöt on eriytettävä tuotannollisista ympäristöistä.
- On luotava ja dokumentoitava säännöt hyväksymiskriteereineen, joilla tietojärjestelmien tuotannollisia ympäristöjä otetaan käyttöön ja päivitetään uudempiin versioihin sekä määriteltävä ja dokumentoitava minimitestausmenettelyt ennen järjestelmien käyttöönottoa.
- Haittaohjelmien havaitsemista ja niiltä suojautumista varten on toteutettava asianmukaiset ja riittävät kontrollit sekä toteutettava riittävät koulutukset.
- Potilastiedoista on otettava asianmukaiset varmuuskopiot ja tallennettava ne siten, että tiedot säilyvät ja että ne ovat tarvittaessa otettavissa käyttöön.
- Käytönseuranta- ja lokitietoja on säilytettävä luotettavasti, hallittava tietoihin pääsyä sekä estettävä tietojen väärinkäyttö.
- Potilastietoja käsitteleville tietojärjestelmille on määriteltävä formaalit käyttäjien ja pääsynhallinnan periaatteet ja menetelmät.
- Käyttäjien todentamisen tason tulee vastata käyttäjälle myönnettävien valtuuksien tasoa.
- Potilastietojärjestelmässä käyttäjät on todennettava henkilökohtaisilla uniikeilla tunnisteilla, todentamisessa on suositeltavaa käyttää vahvaa todennusta.

Standardiluonnoksessa mainitut suositukset tulevat todennäköisesti muuttumaan pakollisiksi tietoturvavaatimuksiksi sosiaali- ja terveydenhuollon sähköisissä järjestelmissä. (Tammisalo 2005, 14-16, 163.)

2.3 Tietosuoja sovelluksen suunnittelussa ja toteutuksessa

Ohjelmistotoimittajan liiketaloudellinen etu ja moraalinen velvollisuus on suunnitella sovellukset siten, että ne mahdollistavat asiakkaan tietosuojan toteutumisen koko asiakastiedon elinkaaren ajan. Tietosuojan toteutuminen ei saa olla kiinni käyttäjän toimista, vaan sovelluksen on ohjattava, jopa pakotettava, käyttäjää oikeanlaiseen toimintaan. (Tammisalo 2005, 70.) Täydelliseen tietosuojaan pakottavaa sovellusta ei ole mahdollista rakentaa, eikä se sellaisenaan olisi käyttäjän kannalta toimiva. Tietosuojan toteutuminen vaatii aina käyttäjältä henkilökohtaista ja ammatillista panostusta. Käyttäjä vastaa syöttämänsä tiedon lainmukaisuudesta ja oikeellisuudesta, sillä tiedon tulee vastata todellisuutta. Henkilötietolain mukaan tietosuojan toteutumisesta vastaa viime kädessä rekisterinpitäjä.

Tietosuojan toteutuminen on jatkuva prosessi, jonka onnistuminen edellyttää huolellista suunnittelua ja jatkuvaa analyysiä koko sovelluksen elinkaaren ajan. Vaikka takuuvarmaa tietosuojaa ja turvallisuutta ei ole olemassa, tavoitteena on luoda sovellukselle suojaus, joka eliminoi tiedonkäsittelyn aikana syntyneet sovelluksen sisäiset ja käyttäjän tahattomat virheet sekä tekee tahallisesta väärinkäytöstä vaikeaa. (Hakkerin käsikirja 2002, 718.)

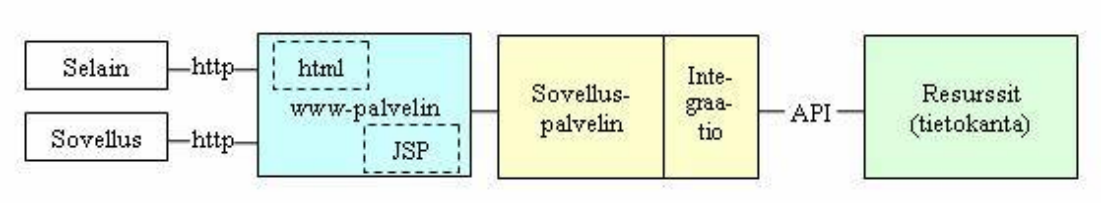
2.3.1 Arkkitehtuuri

Sovelluksen arkkitehtuuria suunniteltaessa on arvioitava kaikki kuviteltavissa olevat tietosuojariskit ja määritettävä sovellukselle tietoturvavaatimukset. Varsinkin Internet-verkossa käytettävän sovelluksen riskianalyysissä on lähdettävä ajatuksesta, että verkko on vihamielinen. (Hakkerin käsikirja 2002, 730-733.)

Hyvinvointialan toiminnalliset vaatimukset ovat monimuotoiset. Toiminnanohjaus ja asiakashallinta ovat palveluntuottajan ydintoimintoja, joissa syntyvien tietojen on oltava virheettömiä ja käytettävissä vuoden jokaisena päivänä kaikkina vuorokauden aikoina. Yhtäaikaisia sovelluksen käyttäjiä voi olla useita. Eri käyttäjät käsittelevät harvoin samaa tietoa, mutta tämä mahdollisuus on käytännössä olemassa. Hyvinvointialalla vasteaikojen ei tarvitse olla samaa luokkaa kuin terveydenhuoltoalalla tai muissa kriittisissä

järjestelmissä, joskin vasteajat vaikuttavat käyttäjän käsitykseen sovelluksen käytettävyydestä. Sovelluksessa käsiteltävät tiedot luetaan kuuluvaksi arkaluontoisiin tietoihin, joten tietosuojan tulee säilyä myös virhe- ja muissa poikkeustilanteissa. Tietoja saavat käsitellä vain niihin oikeutetut henkilöt työtehtäviensä puitteissa. Käyttöoikeuksia määriteltäessä tulee huomioida tehtävänmukaiset pääsyoikeudet. Lisäksi on huomioitava, että potilas- ja asiakastietojen kirjauksia sekä säilytysaikaa koskevat määräykset eroavat toisistaan (Pahlman 2005, 96-97, 120-121).

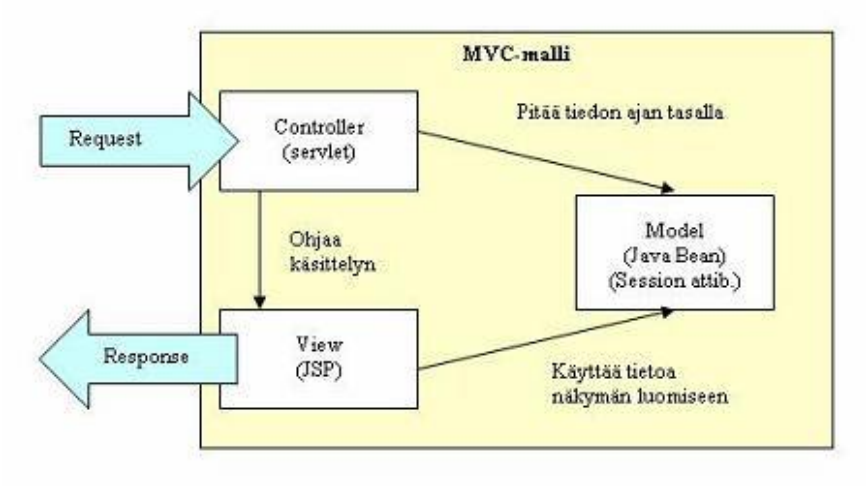
Nykyaikaisten sovellusten arkkitehtuuriksi on vakiintunut hajautettu arkkitehtuuri tietoturvallisuuden sekä skaalautuvuus-, saatavuus- ja luotettavuustarpeiden vuoksi. Hajautetussa arkkitehtuurissa asiakastaso (käyttöliittymä), sovelluslogiikka ja tietokanta (tiedon säilytys) on eritetty toisistaan riippumattomiksi moduleiksi. Hajautettuna arkkitehtuuri on helposti hallittavissa. Kuviossa 6 on esitetty n-tasoarkkitehtuuri, joka on hajautettuun arkkitehtuuriin perustuva sovellusratkaisu. Siinä sovellus on jaoteltu vielä pienempiin osiin, jossa jokaisella osiolla on oma roolinsa. (Ahonen & Hämeen-Anttila 2004, 5.)



Kuvio 6. Esimerkki sovelluksen n-tasoarkkitehtuurista (mukailtu Ahonen & Hämeen-Anttila 2004, 5)

Internetissä käytettävän hajautetun sovelluksen toteutuksessa voidaan käyttää esimerkiksi CGI (Common Gateway Interface), ASP (Active Server Pages) tai JSP (Java Server Pages) -tekniikoita. JSP-tekniikan etuna on, että sen avulla voidaan toteuttaa informaatiosisältöisiä ja dynaamisia www-sivuja laitteistoriippumattomasti. Tekniikassa kirjoitetaan staattisen HTML-osien (HyperText Markup Language) sekaan JSP-syntaksia. JSP on Java Servlet API:n (Application Programming Interface) laajennus. Servletit ovat alustastaan riippumattomia palvelinpään Java-moduleita. Palvelimen Java-versiosta käytetään nimeä J2EE (Java 2 Enterprise Edition). (Ahonen & Hämeen-Anttila 2004, 16-22, 96.)

JSP-tekniikkaa käytetään usein MVC-suunnittelumallin mukaisesti. Siinä erotetaan tieto (Model), näkymä tietoon (View) sekä tiedon käsittelijä ja tapahtumien ohjaaja (Controller) toisistaan. Mallin mukaan suunnitellun sovelluksen etuna on ylläpidon ja muutosten helppous varsinkin käyttöliittymän osalta. (Ahonen & Hämeen-Anttila 2004, 97-98.) Kuviossa 7 on esitetty MVC-suunnittelumallin eri komponenttien tehtävät ja toteutustavat.



Kuvio 7. MVC-suunnittelumallin komponentit, niiden tehtävät ja toteutustavat (Ahonen & Hämeen-Anttila 2004, 98)

Arkaluontoisen tiedon siirtoon on aina käytettävä suojattuja yhteyksiä. Salausprotokolla huolehtii, ettei viesti muutu yhteyden aikana ja että lähettäjä ja vastaanottaja ovat todella niitä, joita he sanovat olevansa. Tämän lisäksi salausprotokolla salakirjoittaa viestin sisällön. Internetissä käytettävän sovelluksen yleisin tietoturvaprotokolla on SSL (Secure Socket Layer). SSL toimii protokollapinon sovelluskerroksessa TCP-protokollan (Transmission Control Protocol) päällä läpinäkyvänä kerroksena. Istunnon avaamisessa osapuolet tunnistetaan, tarkistetaan varmenteet ja sovitaan käytettävästä istuntoavaimesta. Viestien salaamisessa käytetään sovittua salaisen avaimen menetelmää, eheys varmistetaan käyttämällä tiivistefunktiota. Mikäli suojatun yhteyden aikana tapahtuu jotakin poikkeavaa, SSL-protokolla lähettää tästä viestin toiselle osapuolelle. Tilanteesta riippuen virhe yritetään joko korjata tai yhteys katkaistaan. 128-bittinen salaustekniikka on turvallista, eikä sitä voida murtaa laskentatehokkaillakaan menetelmillä relevantissa ajassa. Salausprotokollan käyttö edellyttää varmenteen eli sertifikaatin hallussapitoa. Hakutilanteessa sertifikaatin hakijan on todistettava olemassaolonsa sekä oikeutensa

varmenteessa määritettyyn domain-nimeen. Varmenne myönnetään maksua vastaan määräajaksi. (Hakala ym. 2006, 390-392.)

2.3.2 Tietorakenteet ja käyttöliittymät

Henkilörekisteriin saa kerätä vain toiminnan kannalta oleellisia tietoja. Sovelluksen käyttöliittymät on suunniteltava niin, että kaikille tiedoille on työn organisoinnin kannalta tarkoituksenmukainen tallennuspaikka. Potilastietoja kerätään osittain eri tarkoitukseen kuin asiakastietoja. Koska molempia tietoja tarvitaan hyvinvointialan palvelujen toteutuksessa, ne kannattaa sijoittaa samaan henkilörekisteriin osarekistereiksi. Käyttöliittymissä on selkeästi erotuttava, mitkä tietokokonaisuudet ovat potilastietoja ja mitkä puolestaan sosiaalialan asiakastietoja. Asiakkaan yksilöintitiedot on oltava selkeästi näkyvillä kaikissa yksittäistä asiakasta koskevissa näkymissä.

Asiakas ja sovelluksen käyttäjät on yksilöitävä sovelluksen tietorakenteissa henkilötunnuksen lisäksi jollakin sovelluksen sisäisellä identifiointitunnuksella. Tämä mahdollistaa henkilöiden yksityisyydensuojan erilaisissa organisaation toimintaa kuvaavissa tilastoissa ja raporteissa. Terveydenhuollon sovelluksissa myös jokainen yksittäinen asiakirja on yksilöitävä valtakunnallista arkistoa varten ISO-standardin mukaisella OID-yksilöintitunnuksella. Hyvinvointialan palveluntuottajat toimivat kuitenkin sosiaalihuollon toimialueella, jolle kyseistä velvoitetta ei ole asetettu.

Potilaskirjauksista on selvittävä kirjauksen ajankohta, kirjaaja ja hänen ammatillinen asemansa. Lisäksi tietoon on liitettävä tiedon lähde tai alkuperä, jos tieto perustuu muuhun kuin työntekijän omiin tutkimuksiin, havaintoihin tai päätöksiin. Tietojen luovutuksista toisen rekisterinpitäjän haltuun sekä luovutuksiin liittyvistä suostumuksista on kirjattava ajankohta, paikka, luovutusperuste sekä luovuttaja ja hänen ammatillinen asemansa. Potilastietoja muutettaessa alkuperäisen tiedon on säilyttävä. Virheellisiä tietoja korjattaessa alkuperäinen tieto on siirrettävä taustarekisteriin ja sen yhteyteen on merkittävä tieto korjausajankohdasta, korjauksen perusteesta sekä tieto korjaajasta ja hänen ammatillisesta asemastaan. Potilaskirjauksiin liittyvien tietojen on toistuttava myös tulosteissa.

Potilastiedoista tehtävään lähetteeseen, hoidon loppulausuntoon tai yhteenvetoon, lausuntoon tai muihin näihin rinnastettaviin asiakirjoihin ja niiden tulosteisiin on liitettävä tekijänsä sähköinen tai omakätinen allekirjoitus. Sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetun lain mukaan sähköistä allekirjoitusta vaativissa asiakirjojen käsittelyssä, tiedon siirrossa ja säilytyksessä on käytettävä kehittynyttä allekirjoitusta. Laatuvarmennetta ei kuitenkaan edellytetä, vaikka potilasasetusta on joskus näin tulkittu. Kehittyneen sähköisen allekirjoituksen tarkemmasta teknisestä toteutustavasta ei vielä ole normitasoisia ohjeita olemassa. Sähköistä allekirjoitusta tehdessään tekijän tulee käyttää henkilökohtaista sähköistä varmennetta eli julkista ja salaista avainparia. Vaatimus tarkoittaa käytännössä, että sisäänkirjautumisessa on toteuduttava kehittyneen sähköisen allekirjoituksen vaatimukset.

Asiakkaalla on niin halutessaan tarkastusoikeus omiin tietoihinsa. Tarkastusoikeuden toteuttamista varten sovelluksessa on oltava toiminto, jonka avulla asiakasta koskevat tiedot saadaan käyttöön. Tietojen luovuttaja ei saa vaikuttaa siihen, mitä tietoja asiakkaasta poimitaan. Näkymään ja tulosteeseen on koottava yksiselitteisesti kaikki asiakasta koskevat sosiaali- ja terveydenhuollon tiedot.

Terveydenhuollon sovelluksissa potilaasta on toteutettava aikajärjestyksessä etenevä jatkuva potilaskertomus. Tämän lisäksi potilasasiakirjoilla edellytetään olevan standardin mukainen rakenne valtakunnallisen arkistointivelvoitteen vuoksi. Ylitarkastaja Marika Höökin (sähköpostiviesti 23.1.2007) mukaan sosiaalihuollon yksikön toiminnassa syntyvien potilastietojen osalta riittää, kun noudatetaan voimassa olevia terveydenhuollon tietojen säilytysaika-, salassapito- ja luovutussäännöksiä. Hyvinvointialan palveluntuottajat toimivat sosiaalihuollon toimialueella, joten valtakunnalliseen arkistointiin ja sen edellyttämään standardirakenteeseen ei toistaiseksi ole velvoitetta varautua. Tilanne saattaa muuttua siinä vaiheessa, kun sosiaalihuollossa otetaan käyttöön valtakunnallisesti yhtenevät käsitemäärittelyt.

Sosiaalihuollon asiakastietoja on säilytettävä henkilörekisterissä niin pitkään kuin asiakassuhde kestää. Terveydenhuollon tietojen säilytysaika riippuu tietotyypistä, mutta ajanvaraustietoja lukuun ottamatta säilytysajat ovat pidempiä kuin sosiaalihuollossa. Väliaikaiseksi tarkoitettuja muistiinpanoja ei tarvitse säilyttää. Kaikkeen muuhun tallennettavaan tietoon on tallennushetkellä liitettävä tieto säilytysajan oletetusta kestosta

hoitojakson päättymisen jälkeen. Tiedon liittäminen on toteuduttava automatisoidusti niin, ettei tapahtuma näy eikä haittaa käyttäjän muuta toimintaa käyttöliittymässä. Hoitojakson päätyttyä tiedot on poistettava aktiivista henkilörekisteristä taustatiedostoon. Tietojen lopullinen poistaminen tietorakenteista on oltava käyttäjästä riippuvaa ehdollista toimintaa, sillä normeissa mainitut säilytysajat ovat minimiaikoja. Lisäksi tietojen lopullinen poistaminen on oltava mahdollista vain rajatulle käyttäjäjoukolle.

2.3.3 Implementointi

Sovelluksen rakentamisessa on varauduttava ohjelmistovirheisiin, inhimillisiin käyttäjän virheisiin, tahalliseen häirintään sekä erilaisten tietojenkäsittely- ja tiedonsiirtolaitteiden aiheuttamiin teknisiin virheisiin. J2EE:n tietoturva pohjautuu Javan SecurityManager-luokkaan. Suoritettavan koodin oikeudet voidaan määritellä erillisellä tiedostolla koskematta sovelluksen ohjelmakoodiin. Toinen tapa oikeuksien määrittelyyn on lisätä ohjelmakoodiin erilaisia tarkistuksia. (Ahonen & Hämeen-Anttila 2004, 319-320.) Pääsynhallintaan liittyviä asioita käsitellään tarkemmin seuraavassa luvussa.

ISO 17799 -standardi edellyttää syötetietojen oikeellisuuden ja täydellisyyden tarkistamista. Syötetiedon tarkistaminen on välttämätöntä myös puskurin ylivuotojen ehkäisemiseksi. Puskuri on pala muistia, johon muuttujan arvo tallennetaan. Muistissa on usein eri puskureita vierekkäin. Puskurin ylivuoto tapahtuu, kun puskuri on liian pieni tallennettavaan dataan nähden. Tämä puskuriin mahtumaton data ylikirjoittaa vieressään olevat seuraavat muistipalat ja voi aikaansaada sovelluksessa odottamattomia toimintoja tai muuttaa alkuperäistä dataa virheelliseksi. Useat tarkoitukselliset tietoturvahyökkäykset pyrkivät hyödyntämään tätä ominaisuutta. (Hakkerin käsikirja 2002, 723-724.) Syötteestä on tarkistettava ainakin sen muoto ja sopivuus ennalta annettuihin raja-arvoihin nähden. Raja-arvojen tarkistukset voidaan toteuttaa sovelluslogiikassa listoina, vektoreina, matriiseina tai taulukoina. Joissakin tapauksissa syötteen tarkistamiseen voidaan käyttää tarkistemerkkiä, joka lasketaan sovelluksessa uudelleen. Jos syötteen tarkiste vastaa ohjelmallisesti laskettua tarkistetta, voidaan olettaa syötteen olevan virheetön. Tahattomasti aiheutettuja virhesyötteitä voidaan vähentää selkeillä ja ohjaavilla käyttöliittymäratkaisuilla sekä objekteihin liitetyillä pikaohjeilla. (Hakala ym. 2006, 322.)

Sovelluslogiikkaan on hyvä luoda mekanismit, joilla havaitaan tallennettavien ja siirrettävien tietojen muuttuminen tai häviäminen. Virheiden havaitsemiseksi tiedoista voidaan laskea varmistussummia tai korjausmahdollisuuden antava tarkiste. Eheystarkistukseen käytetään tiivisteitä. Useimmat havaitsemismenetelmät kykenevät havaitsemaan virheitä, mutta eivät pysty niitä automaattisesti korjaamaan. Korjauksia pystyvät tekemään matemaattisia algoritmeja käyttävät tarkisteet, mutta usein ne vaativat paljon prosessoritehoa. Niiden käyttö on kuitenkin perusteltua kriittisissä järjestelmissä. Ohjelmointikielen omia tiivistefunktioita käytetään esimerkiksi käyttäjätunnusten ja salasanojen salaamiseen. (Hakala ym. 2006, 325.)

Graff ja van Wyk listaavat implementoinnin suurimmiksi tietosuojariskeiksi syötteiden tarkistuksen laiminlyönnin lisäksi ympäristömuuttujat, alustamattomat ja samannimiset muuttujat, riittämättömästi tarkistetut tiedostoviittaukset sekä paluuarvojen huolimattoman käsittelyn. Erityistä huolellisuutta on noudatettava poikkeusten käsittelyssä sekä käyttäjien tunnistamis- ja todentamismenettelyissä. Hyvänä ohjelmointitapana mainitaan ohjelmakoodin ylläpidettävyyden tukemista riittävällä kommentoinnilla. Lähdekoodi on pidettävä suojattuna ja käyttämätön ohjelmakoodi tulee poistaa. He suosittelevat toteutettavaksi ohjelmakoodin katselmointitilaisuuksia, joissa ohjelmistovirheitä etsitään tarkistuslistojen avulla. Kriittisten sovellusten katselmoinneissa he suosittelevat käytettäväksi riippumatonta asiantuntijaa. (Kilpilinna 2004, 44-50.)

Sovelluksen tietojen eheyteen, käytettävyyteen ja luotettavuuteen vaikuttavat sovelluksen tietokanta, sen rakenteet sekä rajapintaan rakennetut mekanismit. Javassa tietokantoja käytetään JDBC-rajapinnan (Java Database Connectivity) luokkien sekä erillisten tietokanta-ajureiden avulla. SQL-kyselykielen (Structured Query Language) avulla voidaan operoida mitä tahansa relaatiotietokantaa lähes samalla tavalla. (Kosonen, Peltomäki & Silander 2005, 521.) MySQL on laajimmin käytetty avoimen lähdekoodin tietokanta. Sen etuina ovat nopeus, siirrettävyys eri käyttöjärjestelmien välillä sekä yhteensopivuus kaikkien ohjelmointikielten kanssa. Lisäksi sitä voi useimmiten käyttää kaupallisiin tarkoituksiin ilman lisenssiä. Tämä mahdollistaa alhaiset sovelluskehityskustannukset. (Meloni 2003, 11-13.)

Normalisoitu tietokanta on sinne tallennettujen tietojen eheyden edellytys. Eheyden ylläpidossa käytetään tietokantatasolla viite-eheysmäärityksiä, erilaisia syöttörajoitteita

ja tarkistusmekanismeja. Viite-eheydellä estetään viittaukset tietoihin, joita ei ole enää olemassa. Tietokannoissa, jotka eivät tue viite-eheyttä, on eheydestä huolehdittava ohjelmoitavilla eheysrutiineilla. Ohjelmakoodilla toteutettu viite-eheys monimutkaistaa sovelluslogiikkaa ja on siten alttiimpi piileville virheille. Tietokannan hallintajärjestelmä tarkistaa eheyksiä erilaisten tarkistus- ja virheilmoituspalveluiden sekä transaktioeli tapahtumalokien avulla. Kriittisissä sovelluksissa tietokannan hallintajärjestelmän on kyettävä huolehtimaan samanaikaisuuden ja toisaalta eriytyvyyden ongelmaa lukituksilla sekä eriytyvyystasojen avulla. (Kosonen ym. 2005, 525-526; Hakala ym. 2006, 338-344.) MySQL on tukenut viite-eheyttä vain joidenkin taulutyyppien osalta versiosta 3.23.44 alkaen. Versiossa 5.0 kaikki taulutyypit toteuttavat viite-eheyden. MySQL:n versio 5.0 toteuttaa myös transaktio-ominaisuuden. (MySQL AB 2007.)

Tietokannan tietojen luottamuksellisuuden toteutumiseen voidaan vaikuttaa käyttäjäroolien oikeuksien määrittelyillä. Niitä on jaettava tietokannoittain ja toiminnoittain. Tietokannan käyttöoikeuksia ja sovellusasetuksia on jaettava minimi-periaatteella eli myönnetään vain tarpeelliset oikeudet. (Hakala ym. 2006, 348-351.) Melonin (2003, 56) mukaan MySQL-tietokantaa ei tule koskaan ajaa juurikäyttäjänä.

2.3.4 Pääsynhallinta ja lokitiedot

Tietosuojan toteutuminen edellyttää sovelluksen pääsynhallinnalta todennuksen, valtuutuksen ja tilastoinnin toteutumista (Thomas 2005, 115). Todennuksella eli autentikoinnilla on käänteinen suhde luottamukseen. Jos käyttäjä nauttii luottamusta, yhteyden muodostamiseen ei vaadita tiukkaa autentikointia. Jos käyttäjä on heikosti tunnistettavissa, vaaditaan tiukempaa autentikointia. (Hakkerin käsikirja 2002, 126.) Valtuutus on käyttäjän käyttöoikeuksien määrittämistä. Tavallisesti käyttöoikeuksien määrittäminen perustuu valmiiksi määriteltyihin käyttäjärooleihin, joihin käyttäjät liitetään. Käyttäjäroolien tulisi sisältää pääsyoikeuksien lisäksi toiminnalliset ulottuvuudet. Tilastoinnin avulla rekisterinpitäjä kerää tietoa käyttäjästä ja hänen suorittamistaan toiminnoista, kun käyttäjä on sisäänkirjautuneena sovellukseen. (Thomas 2005, 115-117.)

Internetissä käytettävässä hyvinvointialan sovelluksessa vaaditaan erityisen vahvoja todentamismenettelyjä. Sovellusta tulee päästä käyttämään vain sellaiset henkilöt, jotka

rekisterinpitäjä on valtuuttanut ja joille on määritelty tehtävän mukaiset käyttöoikeudet. Jokaisella käyttäjällä on oltava oma henkilökohtainen tunniste. Tunnisteita luovutettaessa rekisterinpitäjän on varmistuttava, että käyttäjä on riittävästi koulutettu ja tietoinen tunnisteiden tietoturvallisesta käytöstä. Tunnisteita ei tule lähettää verkossa selkokielisenä. Sovelluksessa tunnisteiden käsittely on toteuduttava salatusti, eikä niitä saa tallentaa mihinkään väliaikaiseen muistiin tai tiedostoon. (Tammisalo 2005, 73-78.)

J2EE-sovellusten käyttäjätunnistusmekanismit perustuvat roolien käyttäjäoikeuksiin. Apache Tomcat -sovelluspalvelimen MemoryRealm- tai JDBCRealm-luokkien avulla voidaan hallita sovelluksen käyttäjätunnistusta, käyttäjien rooleja sekä salasanojen salausta. JAAS (Java Authentication and Authorization Service) on JDK:n (Java Developer Kit) pakettikokoelma, joka mahdollistaa koodikeskeisen käyttäjä- ja käyttäjäoikeustunnistuksen riippumatta sovelluksen muusta koodista. Käyttäjätunnistus ja tietoturvanhallinta voidaan toteuttaa J2EE:ssä myös itserakennetuilla komponenteilla.(Ahonen & Hämeen-Anttila 2004, 328-339.)

Autentikoinnin tietoturvallisuutta lisää, että sovellus hyväksyy salasanaksi vain ns. vahvan salasanan. Vahvan salasanan vähimmäispituus on kahdeksan merkkiä ja sen on sisällettävä ainakin kolmen eri merkistöryhmän merkkejä. Lisäksi salasana ei saa olla sama kuin viisi edellistä käytössä ollutta salasanaa ja sovelluksen on vaadittava salasanan vaihtamista säännöllisin väliajoin. Sovelluksen ei saa sallia liian montaa epäonnistunutta perättäistä sisäänkirjautusmisyritystä ilman, että se sulkee käyttäjätilin määräajaksi. Onnistuneessa kirjautumisessa on käyttäjälle näytettävä hänen edellinen onnistunut kirjautumisensa sekä mahdolliset epäonnistuneet kirjautumisyritykset. Salasanan vaihdon yhteydessä virhelyöntimahdollisuudet on minimoitava vaatimalla, että salasana on vahvennettava ennen tallentamista. (Hakkerin käsikirja 2002, 661-662; Tammisalo 2005, 77; Thomas 2005, 63-68.)

Vahvoiksi todentamismenetelmiksi voidaan laskea vaihtuvat salasanalistat, kuten haaste-vastalukulistat, tai kertakäyttöiset tunnisteet, toimikortit sekä biometriset tunnisteet. Toimikortti on luottokortin kokoinen muovikortti, joka sisältää suorittimen ja mikropiirejä. Toimikortille on tallennettu henkilön henkilövarmenne sekä sähköistä asiointia varten julkisen avaimen arkkitehtuurin mukainen julkinen ja salainen avainpari. Julkisen avaimen arkkitehtuurista käytetään nimitystä PKI (Public Key Infrastructure).

Toimikorttien käyttäminen vaatii aina laitteisiin liitettävän toimikorttilukijan. Biometrisia tunnisteita ovat esimerkiksi henkilön sormenjäljet tai kasvokuva. (Tammisalo 2005, 76, 104, 111, 114.) Vahvojen todentamismenetelmien käyttäminen vaatii sovellukselta käyttäjätunnus–salasana-paria vaativampia tekniikoita. Ne eivät useinkaan tue kertakirjautumisen periaatetta. Käyttäjän toimintaa hankaloittavat useat eri kirjautumiset vaarantavat tietoturvaa, sillä käyttäjien on todettu helposti pyrkivän ohittamaan koko henkilökohtaisen sisäänkirjautumisen. (Thomas 2005, 114.) Myös Ylipartasen (2004, 68) mukaan on olennaista, ettei liian raskaalla suojauksella estetä tietojen käsittelyä.

Nykyisin voimassa olevassa normistossa käyttäjätunnistus ja -todentaminen edellytetään toteutettavan riittävän luotettavasti. Teknisiä toteutusmääräyksiä riittävän luotettavasta tasosta ei ole kirjattu. Pienissä ja keskisuurissa yksiköissä ammattilaisen tehtävänmukainen tunnistaminen on toteutettu jo käyttäjätunnusten luovuttamisen yhteydessä. Jos sovelluksesta siirretään asiakastietoja toiseen tietojärjestelmään sähköisesti, tulee potilasasetuksen mukaisia lähetteitä, hoidon loppulausuntoja ja yhteenvetoja sekä niihin verrattavia asiakirjoja varten sovelluksessa olla kehittyneen sähköisen allekirjoituksen mukainen varmennemenettely. Menettely on yleisimmin toteutettu henkilökohtaisella toimikortilla.

Sosiaali- ja terveydenhuollon asiakastietojen sähköistä käsittelyä koskevan lain mukaan myös käsittelyssä käytettävät tietotekniset laitteet tulee tunnistaa luotettavasti. Tätä opinnäytetyötä tehtäessä ei ollut käytettävissä lainkohdan tulkintaa, jonka perusteella olisi voitu selvittää tarkoitetaanko tunnistamisella laitteiston IP-numeroa (Internet Protocol) vai OID-yksilöintitunnusta. Tunnistamisen tekniset toteutusvaatimukset tultaneen kirjaamaan lakiin liittyvään asetukseen. Asetuksen määräysten perusteella on ratkaistava, voidaanko arkaluonteisia tietoja sisältäviä tietojärjestelmiä toteuttaa siten, että ne olisivat käytettävissä julkisissa verkoissa paikasta riippumattomasti.

Rekisterinpitäjän velvollisuus on valvoa rekisteritietojen käyttöä, joten sovellukseen on luotava seurannan toteuttamista varten käyttäjäloki. Käyttäjälokitietojen on keräännyttävä audit trail -periaatteen mukaisesti aukottomana kirjausketjuna. Käyttäjälokia voidaan käyttää myös tilastotarkoituksiin tietoliikenteen kapasiteetin seurannassa, kustannusten allokoimisessa eri toimipisteiden kesken tai teknisten ongelmien selvittämiseen. Käyttäjälokia ei kuitenkaan tule käyttää työntekijöiden työ- tai palvelussuhteen ehtojen

noudattamisen tarkastamiseen. Lokia saavat käyttää vain ne henkilöt, joiden työtehtäviin rekisterinpitäjä on määritellyt rekisteritietojen käytön valvonnan. Loki muodostaa oman muusta rekisteristä erillisen henkilörekisterin, joten sovelluksen käyttäjälokin toteuttamisessa on huomioitava samoja asioita, mitä edellä on esitetty. (Tietosuojavaltuutetun toimisto 2003, 2-5.)

2.3.5 Ohjelmistotuotanto

Asiakkaan tietosuojan toteutuminen sovelluksen toiminnassa edellyttää ohjelmistotuotannolta kaikkia niitä määrittelyn, suunnittelun, toteutuksen, dokumentoinnin ja testauksen käytäntöjä, joita katsotaan yleensä kuuluvan hyvälaatuiseen ohjelmistotuotantoon. Näitä käytäntöjä on kuvattu ISO 17799 -standardissa sekä ISO 27799 -standardiluonnoksessa, joita on käsitelty luvussa 2.2.4. Standardien johtoajatuksena on, että ohjelmistotuotannon eri vaiheissa toiminnan tulee olla suunniteltua ja toteutua johdonmukaisesti kaikissa tilanteissa samalla tavalla riippumatta kuka työntekijöistä työvaiheen suorittaa. Näin toimimalla voidaan vähentää inhimillisistä virheistä johtuvia tietosuojapuutteita. Suunnitelmallisuuteen kuuluu aina tehtäviin valtuuttaminen ja prosessin dokumentointi. Dokumenttien tulee olla yksityiskohtaisia menettelytapaohjeita. Ohjelmistotuotannossa erityisesti muutoksenhallinnan tulee olla suunnitelmallista ja hyväksymismenettelyjä noudattavaa. Standardien mukaisessa toiminnassa jokainen toteutunut työvaihe tulee olla jälkikäteen todennettavissa.

Tammisalon (2005, 16) mukaan eräät ISO 27799 -standardiluonnoksessa mainituista tietoturvavaatimuksista ovat tulossa pakollisiksi sosiaali- ja terveydenhuollon sähköisten sovellusten ohjelmistotuotantoon. Tämä toteutettaneen sovellusten sertifiointiedellytyksenä. Laissa sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä ei sertifiointia vielä edellytetä. Sertifioinnin saavuttaminen vaatii yleensä usean vuoden järjestelmällisen parantamistyön, joten siihen varautumisen kannattanee kuitenkin aloittaa riittävän ajoissa.

2.4 Tietosuoja SaaS-ohjelmistopalvelutuotannossa

SaaS-ohjelmistopalveluna toimitettavan sähköisen järjestelmän sovellus- ja tietokanta-arkkitehtuuri voidaan toteuttaa monella eri tavalla. Pääsääntöisesti ohjelmistopalvelut on toteutettu niin, että palvelun asiakasorganisaatiot käyttävät yhteistä sovelluslogiikkaa mutta tietokanta-arkkitehtuuri on joko eriytetty tai jaettu. Eriytetyssä arkkitehtuurissa kullakin asiakasorganisaatiolla on oma, eriytetty tietokantakokonaisuutensa, kun taas jaetussa arkkitehtuurissa sovellus käyttää yhteistä tietokantaa ja asiakkaiden tietokokonaisuudet erotetaan toisistaan asiakasidentifioinnin avulla. Myös näiden välimuotoja voidaan käyttää SaaS-ohjelmistopalvelusovelluksen arkkitehtuurina. Pääosin arkkitehtuurivalinnat vaikuttavat sovelluksen toteutus- ja ylläpitovaiheiden työmääriin ja sitä kautta kokonaiskustannuksiin. Arkaluonteisia tietoja sisältävien ohjelmistopalvelusovellusten tietokantaratkaisuna on tietoturvasyistä käytettävä ainoastaan eriytettyä arkkitehtuuriratkaisua. (Chong & Carraro 2006; Chong, Carraro & Wolter 2006.)

SaaS-ohjelmistopalvelua tuottaessaan toimittaja toimii toimeksiantosopimuksensa mukaan teknisenä rekisterinpitäjänä. Henkilötietolaki velvoittaa teknistä rekisterinpitäjää huolellisuuteen ja rekisteritietojen suojaamiseen. Tietoturva-asiat kuuluvat ohjelmistotoimittajan palvelujen yleisiin laatuvaatimuksiin. Telelainsäädännössä määritellään viestin kuljetuspalveluiden tietoturvasta tarkasti. Nämä määräykset sitovat tietoliikennepalvelujen tarjoajia. Palvelinpalveluiden osalta, joihin SaaS-ohjelmistopalveluiden katsotaan kuuluvan, tietoturva-asiat ovat kevyemmin säädeltyjä. Niissä sovelletaan lähinnä henkilötietolakia. Rekisterinpitäjän ja palveluntuottajan tulee sopia tietoturvasta ainakin henkilötietoja koskevilta osin. Palveluntuottajan on ennen palvelutoiminnan aloittamista annettava rekisterinpitäjälle asianmukainen selvitys ja sitoumus henkilötietojen suojaamistoimista. (HetiL 5, 32 §; Lampola ym. 2003, 45-47.)

Rekisterinpitäjän on ilmoitettava tietosuojavaltuutetun toimistolle sähköisesti toteutetun rekisterinpidon teknisen toteutuksen ulkoistamisesta. Ohjelmistopalveluntuottajan puolestaan on ilmoitettava palvelutoiminnan aloittamisesta. Rekisterinpitäjällä on velvollisuus laatia ja pitää julkisesti nähtävillä rekisteriseloste, jossa selvitetään mm. henkilötietojen käsittelyn tarkoitus, säännönmukaiset tietolähteet ja tietojen luovutukset. Ohjelmistopalveluun kuuluvana toimittajan on toimitettava asiakkaalleen rekisteriselosteen ja -ilmoituksen laatimista varten kuvaukset sovelluksen sisältämistä tietoryhmistä sekä

sovelluksen tietoturvasuojauksen periaatteista. (HetiL 10, 36 §; Ylipartanen 2004, 83, 119.) Hyvänä kauppatapana on pidettävä, että toimittaja toimii asiantuntijan roolissa ohjaamalla asiakasta hyvään rekisterinpitoon.

Teknisenä rekisterinpitäjänä SaaS-ohjelmistopalveluntuottajan on huolehdittava kaikista niistä palvelimen ylläpitoon liittyvistä toimista, joita tietosuojan ja tietoturvallisuuden toteutuminen edellyttää. Tästä tietoturvallisuuskentästä ei tässä opinnäytetyössä tarkastella hallinnolliseen tietoturvallisuuteen, henkilöstöturvallisuuteen, fyysiseen turvallisuuteen eikä laitteistoturvallisuuteen liittyviä asioita.

Paavilaisen mukaan sähköisten järjestelmien käyttöturvallisuuteen kuuluu turvallisten käyttöperiaatteiden ja jatkuvuuden turvaaminen. Turvallisella käyttöperiaatteella hän tarkoittaa sovelluksen asianmukaista asentamista sekä sen huolellista ja jatkuvaa ylläpitoa siten, että asennus- ja ylläpitotoimet on määritelty, vastuutettu sekä kirjallisesti ohjeistettu. Sovelluksen toimintakykyä sekä kuormitusta on seurattava tarkoituksenmukaisilla työkaluilla ja mittareilla. Mittaustuloksia on seurattava ja niitä on hyödynnettävä asiakkaille tarkoitetun tietoturvaselvityksen laadinnassa. Käyttöturvallisuuteen kuuluva sovelluksen jatkuvuus on turvattava asianmukaisella toipumissuunnitelmalla, dokumentoinnilla, pääsynvalvonnalla, lokitiedoilla sekä näiden suojauksella. Vikatilanteita varten sovelluksesta ja sen sisältämistä tiedoista on otettava varmistukset, joiden avulla järjestelmä voidaan palauttaa vikaa edeltävään tilaan mahdollisen vikatilanteen sattuessa. Toimivassa varmistuskäytännössä otetaan täydellinen varmuuskopio koko järjestelmäkokonaisuudesta ja sen datasisällöistä viikoittain. Tämän lisäksi muuttuneet datasisällöt varmistetaan päivittäin. Varmuuskopioversioita tulee olla vähintään kaksi eri kappaletta, joten ainakin vuoroviikoin varmistukset tulee tallentaa eri medioille. Pitkäaikaissäilytystä varten tietyt täydelliset varmistusmediat on säilytettävä säädetyn vähimmäisajan. Kaikkien varmistustoimien, palautukset mukaan lukien, on oltava testattuja, dokumentoituja ja varmistusten osalta mahdollisimman pitkälle automatisoituja. Varmistustoimien onnistumista on seurattava säännöllisesti. (Paavilainen 1998, 213, 221-223; Tammisalo 2005, 59-60, 66-67; Hakala ym. 2006, 141-145.)

Tietojen säilytyksessä on huomioitava, että pitkänkin säilytysajan jälkeen tietojen on oltava reaalisesti palautettavissa. Tietosisältöjen lisäksi käytetyistä sovelluksista, tietokannoista, selaimista ja muista järjestelmään liittyvistä ohjelmistoista on oltava

purkutilanteessa käytettävissä asianmukaisesti toimivat versiot. Varmuuskopiot ja tietovälineet on suojattava vähintään samantasoisesti kuin varsinaiset rekisteritiedot. Samoin on varauduttava tekniikan muuttumiseen ja siitä johtuvaan säilytettävän tiedon siirtämiseen uuden järjestelmän ymmärtämään muotoon (Tammisalo 2005, 66-67; Hakala ym. 2006, 143-144).

2.5 Tutkimuksia tietosuojasta ja ohjelmistopalvelutuotannosta

Oikeuspoliittisen tutkimuslaitoksen tutkimushankkeessa on tutkittu henkilötietolain vaikutuksia eri aloilla. Muttilaisen tutkimuksessa tarkasteltiin tietosuojaa kansalaisten näkökulmasta 1990- ja 2000-lukujen vaihteessa. Tutkimusaineisto koostui osin vuosikymmenen vaihteessa tehdyistä kyselytutkimuksista sekä viranomaistilastoista, osin vuoden 2004 aikana toteutetuista 15–74 -vuotiaille kohdennetuista puhelinhaastatteluista. Tuloksien mukaan lähes puolet suomalaisista oli melko huolestunut tai erittäin huolestunut henkilötietojensa käsittelystä. Koko Euroopan yhteisön alueella vastaava osuus on n. 60 %. Joka kolmas suomalainen koki joutuneensa luovuttamaan itsestään liikaa tietoja erilaisiin yritysten ja viranomaisten rekistereihin. Omissa rekisteritiedoissaan virheitä oli havainnut joka kahdeksas. Tietosuojavaltuutetun toimistoon vireille laitettujen asioiden määrä oli kymmenen vuoden aikana kaksinkertaistunut. Vaikka asioiden vireille pano on helpottunut sähköpostin lisääntyneen käytön myötä, tämä silti kertoo, että tietosuojaan liittyvät ongelmat koskettavat laajasti erilaisia julkisen ja yksityisen sektorin toimintoja. (Muttilainen 2006, 1-2, 24, 74-75.)

Reposen (2006, 9, 69-72) tutkimuksen mukaan arkaluontoisten potilastietojen luottamuksellisuus toteutuu henkilöstön arvioimana melko hyvin Pohjois-Karjalan keskussairaalassa. Tutkimus käsitteli pääasiallisesti sairaalaorganisaation tietoturvallisuutta ja tietosuojalainsäädäntöä toteuttavaa toimintaa niiltä osin kuin tietoturvallisuus ja sen osa-alueet henkilöstöä käytännön työssä koskettavat. Potilastietojen luottamuksellisuuden, eheyden ja saatavuuden toteutumista tarkasteltiin henkilöstön tietoturva-asioiden tiedon tason, tietoturvallisen asenteen sekä käyttäytymisen näkökulmasta. Tietojärjestelmän tietosuojaominaisuuksia ei tarkasteltu. Tuloksissa todettiin tietoturvallisen asenteen olevan myönteinen, mutta vastuualueiden epämääräisyys, selkeä tiedon ja ohjeistuksen puute vaikeuttavat tietoturvan toteutumista käytännön työssä. Usein tietojärjestelmien

käytettävyysongelmat pakottavat käyttäjät etsimään nopeasti vaihtuvissa tilanteissa kiertoteitä, jotka romuttavat tietoturvaratkaisujen käyttötarkoitukset. Tutkimus toteutettiin vuoden 2005 alussa. Vastaukset edustivat 13 %:a koko henkilöstön määrästä.

Hassol tutkijaryhmineen toteutti vuonna 2003 USA:ssa Pennsylvaniassa projektin, jossa tarkasteltiin asiakkaiden tyytyväisyyttä käyttää www-yhteyttä terveyden ja sairauteen liittyvien asioidensa hoidossa. Geisinger Health System on laajan alueen terveydenhuollon organisaatio, jolla on 52 klinikkaa sekä 2 sairaalaa 31 piirikunnan alueella. Organisaatiolla on käytössään sähköinen potilastietojärjestelmä, Electronic Health Care Record EHR, johon on myös asiakkailla pääsy MyChart-liittymän avulla. Sovelluksen avulla käyttäjä voi mm. kommunikoida sähköisesti terveydenhuollon toimijoiden kanssa, tehdä ajanvarauksia sekä tarkastella rajatusti omia terveys- ja sairaustietojaan. Sovelluksen käyttö on erittäin suosittua organisaation asiakkaiden keskuudessa. Tutkimustulosten mukaan sovelluksen käyttö oli teknisesti helppoa, kommunikointi ammattilaisten kanssa oli helppoa ja ymmärrettävää sekä asiakkaat kokivat saaneensa riittävästi informaatiota ongelmatilanteisiinsa kaikissa ikäryhmissä. Koulutustaso vaikutti tuloksiin niin, että ylemmän koulutustason asiakkaat olivat tyytyväisempiä kuin vähemmän koulutetut. Tutkimuksessa tarkasteltiin myös tietosuojaan liittyviä asioita. Vastausten mukaan vain vähemmistö, 30 %, oli hieman huolissaan tietojensa luottamuksellisuudesta. Selkeä enemmistö oli vain vähän tai ei lainkaan huolestunut tietosuojastaan. Enemmän koulutetut olivat selvästi luottavaisempia tietosuojaansa kuin alemman tason koulutuksen saaneet. Sovellukseen kirjauduttiin henkilökohtaisella käyttäjätunnuksella ja salasanalla. Sovelluksen tietoliikenne oli salattua 128-bittisellä salauksella. (Hassol ym. 2004.)

SaaS-palveluna tarjottavien sovellusten määrä on nousussa aikaisempiin vuosiin verrattuna. Tämä on havaittavissa Kontion, Lassilan ja Maulan yhdeksättä kertaa toteutetussa ohjelmistoyrityskartoituksesta, jossa tarkasteltiin suomalaista ohjelmistotuoteliiketoimintaa. Tutkimuksen mukaan yrityksistä 53 % tarjosi vuoden 2005 aikana SaaS-mallin mukaista ohjelmistopalvelua. Vastaava luku oli vuotta aikaisemmin vain 35 %. Kansainvälisessä ohjelmistotuoteliiketoiminnassa SaaS-malli on jo pitkään ollut suosittua. Suomessa tätä liiketoimintaa harjoittavat pääosin suuret ohjelmistotalot. Tutkimuksen mukaan ohjelmistoalan yritykset ovat alkaneet kiinnittää huomiota yhä enemmän sovellusten monistettavuuteen ja tuotteistukseen. (Kontio ym. 2006.)

SaaS- tai ASP-mallin mukaisia ohjelmistohankkeita on tutkittu enimmäkseen liiketoiminnallisesta tai sopimusoikeudellisesta näkökulmasta. Nordström ja Sääksjärvi (2004, 6-13) tarkastelivat erään ASP-sovellusvuokraustoiminnassa epäonnistuneen yrityksen toimintaa verkostoitumisen liiketoiminnallisesta näkökulmasta. Tarkasteltava yritys oli vuoden 2000 aikana solminut sopimuksen itseään huomattavasti suuremman telealan yrityksen kanssa. Yritysten aikomuksena oli ryhtyä harjoittamaan ASP-mallin mukaista sovellusvuokrausta toiminnanohjaukseen ja projektinhallintaan tarkoitetuilla sovelluksilla. Liiketoimintaa ei päästy aloittamaan ja lopulta teleyritys vetäytyi hankkeesta. Strategista verkostomallianalyysia käyttäen tutkijat löysivät useita syitä hankkeen epäonnistumiselle. Ennen kaikkea yritykset eivät yhteistoimintasopimuksestaan huolimatta saavuttaneet todellisia synergiaetuja. Viestintä ei kulkenut, tietotaitoa ei haluttu tai osattu vaihtaa. Kumpikin osapuoli koki, ettei saanut riittävästi vastinetta panokselleen. Toiseksi ohjelmistoyrityksellä oli huomattavaa teknologista osaamista, mutta massatuotannon toteuttamisessa vaadittavia usean eri teknologian yhdistämisprojekteista ei ollut riittävästi kokemuksia. Kolmantena syynä tutkijat näkivät, että tuotekehityksessä unohdettiin asiakkaat ja heidän tarpeensa.

3 PROJEKTIN LÄHTÖKOHDAT, TAVOITE JA TEHTÄVÄT

3.1 Projektin lähtökohdat

Vuosikymmenen vaihteessa on tapahtunut palvelurakenteen muutos laitoshoidosta asumispalveluihin. Hyvinvointialan palveluntuottajien määrä on lisääntymässä. Tätä kasvua ovat olleet mahdollistamassa viime vuosina käyttöönotetut uudet rahoitusmallit. Uusi toimintamuoto on esimerkiksi palvelusetelikäytäntö, jossa asiakas voi valita palveluntuottajansa itsenäisesti ja maksaa osan palveluistaan kunnan myöntämillä palveluseteleillä. (Kauppinen & Niskanen 2005, 5, 26, 34.) Hyvinvointialan palvelutuotanto vaatii suuria investointeja. Toimialan kustannuksen syntyvät valtaosin henkilökustannuksista. Liiketoiminnan on oltava tuottavaa myös hoiva-alan yrityksissä, joten yritysten on hiottava toimintaprosessinsa toimiviksi. Hoiva-alan ammattilaiset haluavat

kuitenkin antaa asiakkailleen parasta mahdollista hoitoa. Codebird Oy tarjoaa TUHA-ohjelmistopalvelulla hyvinvointialan palveluntuottajille mahdollisuuden keskittyä tekemään työtä, jota he parhaiten osaavat. Ohjelmistopalvelua käyttämällä palveluntuottajan ei tarvitse resursoida tietotekniseen osaamiseen tai laitteisiin.

Codebird Oy on aiemminkin toiminut sosiaali- ja terveydenhuollon tietojärjestelmätuotannon parissa. Yrityksellä on toimialan osaamista, mutta koska TUHA on tuotteena uusi ja hyvinvointialan tietosuojavaatimukset korkeat, Codebird Oy halusi varmistua sovelluksensa tietosuojan toteutumisesta. Näistä lähtökohdista esitettiin tämän työn tekijälle toive toteuttaa opinnäytetyönä TUHA-sovelluksen ja sen ohjelmistotuotannon tietosuojaa tarkasteleva arviointi. Seuraavissa luvuissa tarkastellaan lähemmin Codebird Oy:tä yrityksenä sekä TUHA:a sovelluksena ja ohjelmistopalvelutuotteena.

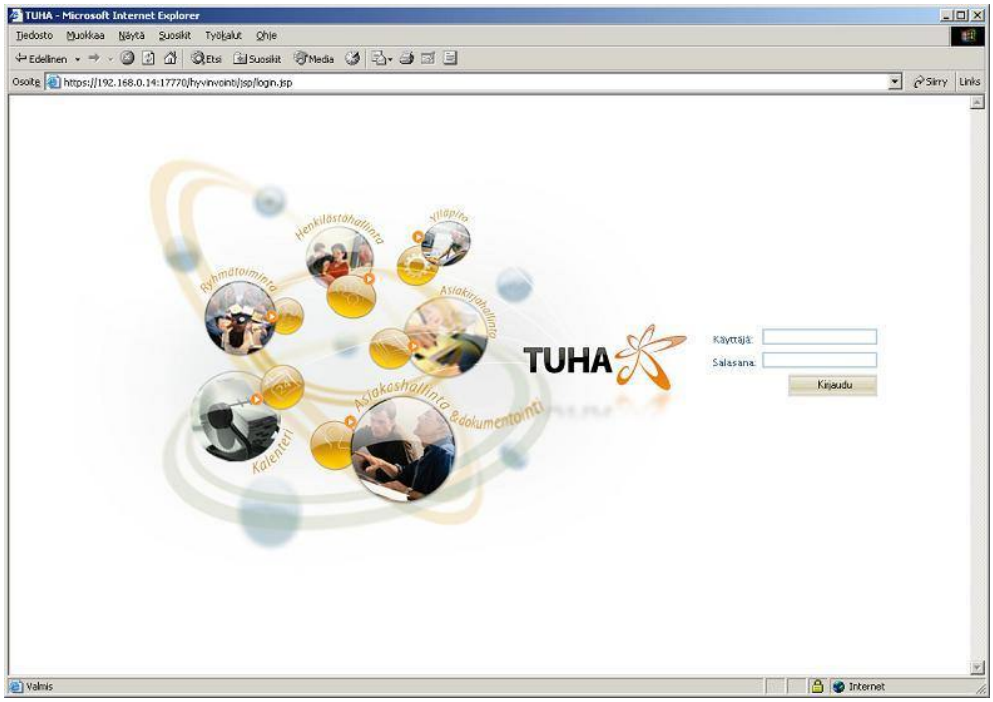
3.1.1 Yritystiedot

Codebird Oy on vuonna 2002 perustettu ohjelmistoalan yritys, jonka tuotteet auttavat asiakkaitaan tehostamaan ja kehittämään omia toimintojaan. Yrityksen osaaminen keskittyy mobiiliteknologiaan, paikannusratkaisuihin sekä www-pohjaisiin ratkaisuihin. Yritys palvelee asiakkaita mm. logistiikan, projektin- ja resurssienhallinnan sekä hoivatyön alueilla. Yrityksen omistavat toimiva johto, Grenovia Oy ja VeraVenture Oy. Codebird Oy:llä on päätoimipiste Porissa. Sivutoimipiste sijaitsee Tampereella. Yrityksen palveluksessa on tällä hetkellä seitsemän henkilöä. (Codebird Oy 2006.)

TUHA-sovellusta ja -ohjelmistopalvelua tuottavaan työryhmään kuuluu neljä henkilöä. Näistä päätoimisesti tämän tuotteen parissa työskentelee yksi henkilö. Työryhmän osaaminen on monialaista. Siihen kuuluu perinteisen ohjelmistokehitys- ja liiketoimintaosaamisen lisäksi verkko- ja tietoliikennetekniikan osaamista. Lisäksi työryhmällä on järjestelmätukiosaamista, atk-koulutustaitoja, markkinoinnin ja asiakashallinnan osaamista sekä sähköisen kirjaamisen ja rekisterinpidon asiantuntijaosaamista.

3.1.2 TUHA-sovellus

TUHA on pienen tai keskisuuren yksityisen ja kolmannen sektorin hyvinvointialan asumis- tai avopalveluja tarjoavan yksikön toiminnanohjauksen sekä asiakashallinnan tarpeisiin kehitetty sähköinen järjestelmä. TUHA nimenä tulee sanoista tuetun asumisen hallintajärjestelmä. Sovelluksen avulla yritys voi hoitaa kaikkea ajanhallintaan, asiakastietojen ja työyhteisön päivittäiseen kirjaukseen, asiakaslaskutukseen sekä toiminnassa tarvittavien asiakirjojen hallintaan liittyviä tehtäviä. Järjestelmässä on myös työväline työvuorojen suunnitteluun sekä palkanmaksun perusteiksi toteutuneiden työtuntien laskentaan. Sovellukseen kirjaudutaan käyttäjäkohtaisella käyttäjätunnuksella ja salasanalla sisäänkirjautumisnäkymästä (Kuva 1). Käyttäjällä on pääsyoikeus vain niihin sovelluksen osioihin, joita hän työtehtävänsä hoitamiseksi tarvitsee.

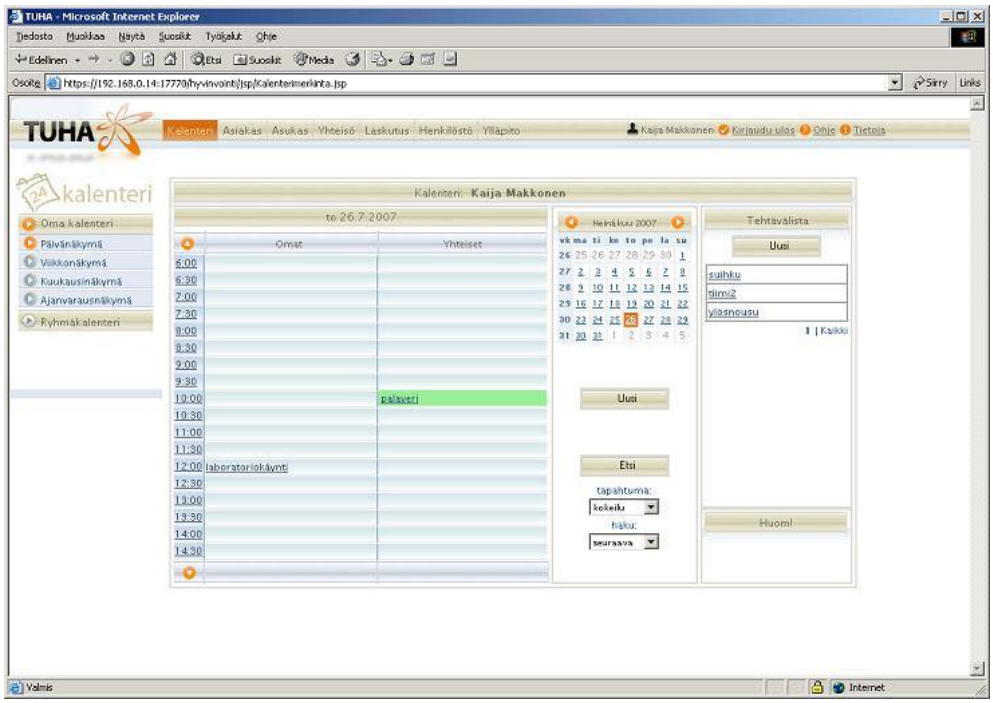


Kuva 1. TUHA-sovelluksen sisäänkirjautumisnäkymä

Jokainen sovelluksen näkymä on toteutettu siten, että päävalikko on näytön yläreunassa vaakasuorana rivinä. Päävalikko on käytettävissä kaikissa tilanteissa. Osiokohtaiset valikot sijaitsevat näkymien vasemmassa reunassa. Käyttäjä pystyy koko istunnon ajan hahmottamaan sijaintinsa järjestelmässä valikkojen visuaalisten värikoodien avulla. Asiakkaan yksilöintitiedot sijaitsevat aina otsikkorivillä. Visuaaliset ja toiminnalliset yhdenmukaisuudet toistuvat toimintanäppäinten ja näkymien toimintalogiikassa.

Kokematonta käyttäjää ohjaavat objektikohtaiset pikaohjeet. Tämän lisäksi jokaisesta käyttöliittymänäkymästä on avattavissa päävalikolla sijaitsevasta ohjelinkistä näkymäkohtainen toimintaohje.

Ajanhallintaosiossa käyttäjällä on käytettävissään oma henkilökohtainen kalenteri sekä näkymä työyhteisön yhteiseen kalenteriin. Kalenterimerkintä voidaan merkitä näkymään myös yksittäisen asiakkaan tai asukkaan kalenteriin. Kalentereista ovat valittavissa tarpeen mukaan päivä-, viikko- tai kuukausinäkymät. Kuvassa 2 on esimerkki päiväkalenterinäkymästä. Käyttäjälle suunnitellut työvuorot erottuvat kalenterinäkymissä taustaltaan erivärisinä. Ryhmäkalenterinäkymässä työyhteisön jäsenille voidaan etsiä yhteistä palaveriaikaa sekä merkitä se kaikille yhdellä tallennuksella. Näiden toimintojen lisäksi ajanhallintaosiossa voidaan tehdä keltaisten muistilappujen kaltaisia tehtävämerkintöjä. Tehtävämerkintä näkyy kaikille työyhteisön jäsenille. Tehtävämerkintä poistuu näkymästä, kun joku käyttäjistä merkitsee sen toteutuneeksi.



Kuva 2. TUHA-sovelluksen päiväkalenterinäkymä

Avo- ja asumispalveluiden käyttöön tarkoitetuissa osioissa ovat asiakkaiden ja asukkaiden yksilölliset henkilö- ja laskutustiedot, terveyden- ja sairaanhoitoon liittyvät tarpeelliset taustatiedot, diagnoosit, lääkitykset sekä laboratoriotutkimustulokset. Lisäksi niissä voidaan kirjata erilaisia hoito-, tavoite- ja kuntoutussuunnitelmia, päivittäisiä kirjauksia,

yhteenvetoja sekä täyttää hoitoilmoituslomake. Päivittäisiä kirjauksia voidaan tehdä myös kootusti päiväraporttinäkymästä. Yhteisöosiossa voidaan kirjata erilaisten hoidollisten ryhmien tai kokousten muistiinpanoja.

Henkilöstöosiossa ovat käyttäjien omat näkymät henkilötietoihin sekä työvuoro- ja lomasuunnitelmiin. Tähän kuuluvat myös ylläpitäjän käyttäjätunnuksilla käytettävät työvuorojen suunnittelunäkymät sekä toteutuneiden työvuorojen tuntiyhteenvedot. Jokaisen asiakkaan, asukkaan, työntekijän ja työyhteisön tietokokonaisuuksiin kuuluvat lisäksi asiakirjat. Asiakirjat ovat järjestelmän ulkopuolisia sähköisesti tallennettuja tiedostoja, joita voidaan liittää osaksi TUHA-sovellusta. Laskutusosiossa voidaan muodostaa ja tulostaa laskuja asiakkaan käyntihistorian, asukkaan asumistietojen tai maksajakohtaisen koonnin perusteella. Ylläpito-osiossa ovat käyttäjähallinta ja järjestelmäloki. Tämän lisäksi siellä määritellään järjestelmään yrityskohtaiset järjestelmäasetukset.

TUHA-sovelluksen versio 1.0.0 on julkaistu vuoden 2007 helmikuussa. Sovellusta käytetään Internet-verkon välityksellä miltä tahansa käyttäjän tietokoneelta, jossa on selain ja laajakaistayhteys. Tietoliikenne kulkee julkisessa verkossa HTTP(S)-liikenteenä (HyperText Transfer Protocol Secure). Tietokantana on MySQL-tietokanta. Sovellus on toteutettu JSP-tekniikalla MVC-mallin mukaisesti.

3.1.3 TUHA-ohjelmistopalvelu

TUHA:a markkinoidaan SaaS-ohjelmistopalveluna. Palvelusopimuksen allekirjoituksen jälkeen Codebird Oy perustaa palvelimilleen asiakasyritykselle tietokannan, jonka jälkeen asiakasyritys pääsee aloittamaan käyttöönottoprojektin. Järjestelmän käyttöönottoprojekti on aina asiakasyrityksen oma projekti, jota Codebird Oy tukee. Tukeen kuuluu kirjallisen materiaalin lisäksi käyttöönoton ohjaus ja neuvonta. Käyttöönottoprojektitukeen kuuluvat TUHA-sovelluksen käyttäjäkoulutukset. Koulutukset toteutetaan asiakasyrityksen toiveiden mukaan joko ylläpitäjille suunnattuna ylläpitäjäkoulutuksena tai vaihtoehtoisesti peruskäyttäjäkoulutuksena koko henkilöstölle. Molempiin koulutuksiin kuuluvat aina olennaisena osana tietoturva-asiat. Käyttöönottoprojektissa yritys luo itse omat yrityskohtaiset asetukset, luo työntekijöilleen käyttäjätunnukset sekä vie asiakkaidensa pohjatiedot järjestelmään.

Ohjelmistopalvelun käytöstä asiakasta veloitetaan perustamiskustannusten lisäksi sopimuksen mukaisella käyttäjämäärään sidotulla hinnalla kuukausittain. Tätä suoritusta vastaan asiakas saa käyttäjälisenssit TUHA-sovelluksen käyttämiseen. Yhtäaikaisten käyttäjien tai tietoliikenteen määrää ei muuten rajoiteta. Tietosisällön tallennuskapasiteetti on perussopimuksella 300 megatavua. Palveluun kuuluvat yrityskohtaisen tietokannan varmuustallennukset sekä uudet sovelluspäivitykset ilman lisäkustannuksia. Asiakkaalla ei ole vastuuta palvelinkapasiteetin riittävyydestä tai laitteistojen vikaantumisista. Asiakkaan vastuulla on huolehtia omasta laajakaistayhteydestään sekä omien atk-päätteidensä virusturvasta ja palomuuriohjelmistosta.

3.2 Tavoite ja tehtävät

Projektin tavoitteena oli laajentaa ja syventää Codebird Oy:n tietosuojaan liittyvää tietämystä. Tietämys on tiedon tulkintaa, asiantuntijuutta tietyllä osa-alueella. Toinen tavoite oli tarkastella tietosuojan toteutumisen tasoa TUHA-sovelluksessa sekä sen jakelukanavana käytetyssä ohjelmistopalvelutuotannossa. Tarkastelussa haluttiin erityisesti keskittyä sovelluksiin kirjattujen asiakkaiden tietosuojaan ja sen toteutumiseen. Projektin tuloksia hyödynnetään paitsi TUHA-ohjelmistopalvelun jatkokehityksessä myös muissa yrityksen hyvinvointialaan liittyvien sovellusten kehitystyössä.

Projektin täsmennetyt tehtävät olivat seuraavat:

1) Codebird Oy:n tietosuojaan liittyvän tietämyksen laajentaminen ja syventäminen
   - Mitkä normit sääntelevät yksityisille ja kolmannen sektorin hyvinvointialan palveluntuottajille suunnatun Internet-verkossa käytettävän sovelluksen asiakastietojen tietosuojaa?
   - Mikä on näiden normien sisältö ja merkitys sovelluksen suunnittelulle ja toteutukselle?
   - Mikä on näiden normien merkitys SaaS-ohjelmistopalvelussa ohjelmistotoimittajan näkökulmasta?
   - Mihin muutoksiin Codebird Oy:n tulee varautua tulevaisuudessa liittyen edellä mainittuihin asioihin?

2) Yksityisille ja kolmannen sektorin hyvinvointialan palveluntuottajille suunnatun Internet-verkossa käytettävän sovelluksen asiakastietojen tietosuojavaatimusten toteutuminen TUHA:ssa ja sen ohjelmistopalvelutuotannossa
   - Miten tietosuojavaatimukset toteutuvat TUHA-sovelluksessa (versio 1.0.0)?
   - Miten tietosuojavaatimukset toteutuvat TUHA-ohjelmistopalvelussa?
   - Miten TUHA-sovellusta ja -ohjelmistopalvelua voitaisiin kehittää näiden tietosuojavaatimusten valossa, että ohjelmistotuotannon eettiset sekä yrityksen liiketaloudelliset vaatimukset olisivat tasapainossa?

Projektin tehtäviin ei kuulunut tarkastella asiakastietojen luovutuksiin liittyviä tietosuojaseikkoja, sillä projektin aikataulu- ja työmääräresurssit olivat ennalta rajatut. Samalla perusteella tarkastelun ulkopuolelle jätettiin kokonaistietoturvakentän hallinnollinen, henkilöstöön liittyvä, fyysinen sekä laitteistoulottuvuudet. Edelleen projektitehtävän kehitysehdotusten osalta tavoitteena ei ollut ratkaisujen toteuttaminen, vaan lähinnä puutteellisesti toteutuvien tietosuojavaatimusten määrittäminen sekä toteuttamiskelpoisten kehittämisideoiden esittäminen.

4 PROJEKTIMENETELMÄT

4.1 Menetelmät ja niiden luotettavuus

Ensimmäisen projektitehtävän osalta menetelmänä oli tiedon keruu Internetissä olevista tietopankeista ja muista alan verkkodokumenteista, kirjallisuudesta sekä erityisasiantuntijoilta. Tieto kerättiin, kirjattiin ja sen merkitys arvioitiin projektitehtävien kannalta. Tämän jälkeen kerättyä tietoa sovellettiin projektitehtävien mukaisiin ohjelmistotoiminnan osa-alueisiin.

Toisen projektitehtävän osalta menetelmänä oli tapaustutkimuksena toteutettava laadullinen ja kehittävä arviointi. Tapaustutkimus eli case study antaa yksityiskohtaista ja intensiivistä tietoa yhdestä yksittäisestä tapauksesta tai joskus myös rajatusta joukosta

toisiinsa suhteessa olevia tapauksia. Tavoitteena on yleensä ilmiön kuvailu. Tapaustutkimuksessa aineisto voidaan kerätä mm. havainnoimalla ja dokumentteja tutkimalla. (Hirsjärvi, Remes, & Sajavaara 2000, 123.) Tässä opinnäytetyössä tapaustutkimus toteutettiin laadullisen eli kvalitatiivisen tutkimusotteen tapaan. Laadullisille tutkimuksille on luonteenomaista pehmeys, subjektiivisuus sekä tutkijan ja tutkittavan aineiston läheisyys. Kvalitatiivisen tutkimuksen tutkimusstrategia on tyypillisesti strukturoimaton, suunnitelmia muutetaan olosuhteiden mukaan. Sen vahvuutena on syvyys ja yksityiskohtaisuus, joskin heikkoutena voidaan nähdä tulosten yleistämisen ongelmallisuus. (Hirsjärvi ym. 2000, 123-125, 155.) Kehittävän eli formatiivisen arvioinnin tavoitteena on toiminnan kehittäminen ja muokkaaminen (Robson 2000, 80). Tähän opinnäytetyöhön kehittävä tutkimusote sopii hyvin, sillä Codebird Oy:n liiketoiminnan lähtökohtana on kehittää laadukkaita tuotteita ja palveluja asiakkaiden tarpeisiin.

Arviointi eli evaluaatio on jonkin kohteen arvon tai merkityksen määrittämistä. Kohdetta verrataan suhteessa tiettyihin arviointiperusteisiin ja tästä näkökulmasta tutkimuksen tekijä esittää arvioivan päätelmän. Stakesin Sosiaalipalvelujen evaluaatioryhmä FinSoc määrittelee, että arviointitutkimuksessa arvioidaan systemaattisesti jotakin kohdetta käyttäen yhteiskunta- ja käyttäytymistieteiden tutkimusmetodeja. Arvioinnin pyrkimyksenä on objektiivinen ja luotettava kuvaus, jonka lähtökohtana on määritelty arvoperusta. Arviointitutkimuksessa on kyse vertailusta tosiasioiden ja ideaalin välillä. Keskeistä on arviointikriteereiden ja mittareiden muodostaminen, mittaaminen sekä tietoon perustuva arvio. Ulkopuolisen on kyettävä seuraamaan ja arvioimaan myös intuitioon ja assosiaatioon perustuvia päätelmiä. (FinSoc 2001, 5-6, 23-24.) Robsonin mukaan arvioinnissa on kyse arvon määrittämisestä. Tutkimuksessa puolestaan on kyse kuvaamisesta, selittämisestä ja ymmärtämisestä. Arviointi voi olla tutkimusta, jos sillä on harkittu tutkimusasetelma ja aineisto kerätään, analysoidaan sekä tulkitaan systemaattisesti. (Robson 2000, 25.)

Tässä opinnäytetyössä arvioinnin lähtökohtana olivat voimassa olevat normit, niiden pohjalta annetut toimialan asiantuntijoiden ohjeet sekä käytettävissä olevat lakiesitykset perusteluineen. Arviointi perustui työn toteuttajan omiin henkilökohtaisiin havaintoihin ja kokemuksellisiin tuloksiin. Täsmällisen toistettavuuden edellyttämää systemaattista mittaristoa ei laadittu, sillä projektitehtävän tulokset oli tarkoitettu vain yrityksen oman toiminnan kehittämiseen ilman tieteellistä näyttöä.

Projektia toteutettaessa arvioija työskenteli Codebird Oy:n palveluksessa TUHA-ohjelmistopalvelun tuotevastaavana. Tämä vaikuttaa projektimenetelmän luotettavuuteen eli reliabiliteettiin kahden suuntaisesti. Luotettavuutta lisää se, että arvioija tunsi TUHA-sovelluksen ja -ohjelmistopalvelutuotannon kokonaisuutena erittäin hyvin. Tämä mahdollisti kokonaisvaltaisen, kattavan ja tosiseikkoihin perustuvan mielikuvan luomisen tietosuojan toteutumisesta. Luotettavuutta lisää tulosten jääminen ainoastaan yrityksen sisäiseen käyttöön, koska arvioijalla ei tässä tapauksessa ole pyrkimystä tulosten vääristämiseen markkinointia varten. Toisaalta arvioija on osallistunut tuotekokonaisuuden määrittelyyn, suunnitteluun ja toteutukseen. Se voi vääristää arviointituloksia varsinkin jälkimmäisen projektitehtävän osalta, koska suunnittelijalla on aina positiivinen käsitys sovelluksestaan. Tämän voi kuitenkin nähdä myös niin, että tuotevastaava pyrkii saamaan mahdollisimman objektiivisen ja realistisen kuvan tuotteestaan sekä sen kehittämismahdollisuuksista.

Projektimenetelmien validiteettiin vaikuttaa arviointimittariston puuttuminen. Mittariston rakentaminen tämän luonteisessa projektissa ei ole tarkoituksenmukaista ja toisaalta valmiin mittarin käyttäminen ei sovellu projektitehtävään. Tehtävään sopivan strukturoidun mittarin löytäminen on ongelmallista ja yleensä sellaisen käyttäminen tekee arvioinnin jäykäksi. Toisaalta mittariston puuttuminen lisää inhimillisen virheen riskiä.

4.2 Projektin toteutus

Projekti toteutettiin projektitehtävien mukaisesti kahtena erillisenä osiona. Ensimmäisessä osiossa toteutettiin tietosuojaan liittyvän tiedon keruu. Tiedon keruu aloitettiin marraskuussa 2006. Kaikki tieto oli kerätty helmikuussa 2007. Tiedon keruuseen ja sen ohjelmistotuotannon käytäntöihin liittyvään soveltamiseen käytettiin lähes puolet projektin kokonaistyömäärästä.

Tietolähteenä käytettiin pääosin Finlex-säädöstietopankkia, tietosuojavaltuutetun toimiston sekä Stakesin verkkosivustoja ja tietosuojaan liittyviä painettuja teoksia. Aihealueesta lähetettiin sähköpostitse kaksi kysymystä tietosuojavaltuutetun toimistolle, joista toiseen saatiin vastaus. Tiedon keruussa haluttiin tarkoituksellisesti käyttää normiston lisäksi alan asiantuntijoiden lausuntoja ja heidän kirjoittamiaan teoksia, koska

katsottiin, ettei opinnäytetyön tekijällä ole riittävästi asiantuntijuutta tulkita normistoa. Tiedon keruun yhteydessä pohdittiin normiston asettamien vaatimusten merkitystä hyvinvointialan sovelluksen toiminnallisuuteen ja toteutusratkaisuihin sekä ohjelmisto- ja ohjelmistopalvelutuotantoon. Tiedon keruun kaikki tuotokset haluttiin kirjata tausta-aineistoksi, vaikka se merkitsi eräin kohdin saman tiedon toistamista useaan kertaan. Tällä haluttiin turvata tausta-aineiston jatkohyödyntäminen tämän opinnäytetyön ulkopuolelle rajatuissa aihepiireissä.

Projektin toisessa osiossa toteutettiin TUHA-sovelluksen sekä sen jakelukanavana käytetyn ohjelmistopalvelun case-arviointi tietosuojan toteutumisen näkökulmasta. Arvioinnin perusteella laadittiin vielä kehitysehdotukset sekä sovelluksen että ohjelmistopalvelun tietosuojan parantamiseksi. Kehitysehdotusten laadinnassa pyrittiin huomioimaan myös liiketaloudellinen näkökulma. Arviointi ja kehitysehdotusten laadinta toteutettiin alkuperäisestä projektisuunnitelmasta poiketen osittain yhtäaikaisesti tiedon keruun kanssa. Vaihe aloitettiin tammikuussa 2007 ja se saatiin päätökseen saman vuoden maaliskuussa. Arviointityöhön ja kehitysehdotusten laadintaan käytettiin noin kolmasosa projektin kokonaistyömäärästä.

Arviointityön toteuttamiseksi tarkasteltiin TUHA-sovelluksen vaatimusmäärittelyjä, spesifikaatioita, ohjelmakoodia, tietokantaa sekä itse sovellusta ja sen käyttöohjeita. Sovelluksessa on kaikkiaan 86 näkymää ja 31 tulostenäkymää. Sovelluskokonaisuus muodostuu 228 tiedostosta ja 33 tietokantataulusta. Kaikkea ohjelmakoodia ei käyty läpi, vaan tarkasteltiin lähinnä sen periaatteellisia ratkaisuja. Näiden lisäksi tarkasteltiin ohjelmistokehitysprosessia ja sen eri osa-alueita. Ohjelmistopalvelun arviointia varten tarkasteltiin varsinaisen palveluprosessin lisäksi sen dokumentaatiota, verkko-, tietoliikenne- ja varmistuskäytäntöjä, koulutusmateriaaleja sekä asiakassopimuksia.

5 TUOTOKSET

Ensimmäisen projektitavoitteen mukaiset tuotokset ovat kirjattuna tämän opinnäytetyön tausta-aineistoksi. Toisen projektitavoitteen mukainen arviointiosuus (Liite1) ja sen pohjalta esitetyt kehitysehdotukset (Liite 2) esitetään Satakunnan ammattikorkeakoulun vuoden 2006 opinnäytetyöohjeen julkisuussäännösten mukaisesti niiden luottamuksellisuuden vuoksi tämän opinnäytetyön liitteinä. Liitteet luovutetaan vain opinnäytetyön tilaajalle Codebird Oy:lle.

Tausta-aineiston tietosuojaa käsittelevät lait ja asetukset ovat tämän hetken voimassa olevaa suomalaista lainsäädäntöä. Ne velvoittavat kaikkia toimialan ohjelmistotoimittajia. Lakien ja asetusten lisäksi haluttiin käsitellä tietosuojan toteutumiseen liittyviä standardeja. Ohjelmistotoimittajia ei ole toistaiseksi velvoitettu standardien noudattamiseen, mutta niiden noudattamista voidaan pitää ohjelmistotuotannon hyvänä käytäntönä. Sosiaali- ja terveydenhuollon tietojärjestelmätuotannossa käytettäviksi suositeltavia standardiluetteloita on koottu sosiaali- ja terveysministeriön sekä Stakesin julkaisuissa. Tarkasteltaviksi standardeiksi valikoitui yksi ohjelmistotuotannon tietoturvallisuutta käsittelevä yleisstandardi sekä yksi erityisesti sosiaali- ja terveydenhuollon näkökulmasta tietosuojaa ja tietoturvaa käsittelevä standardiluonnos. Näihin valintoihin päädyttiin, koska nämä standardit ovat yleisiä kansainvälisessä käytössä ja ne sopivat sekä asiasisällöiltään että tarkkuudeltaan tämän opinnäytetyön tarkoituksiin. Lisäksi näiden standardien sisällöistä oli saatavilla riittävästi tietoa.

Projektin myötä tekijän tietosuojaan liittyvä osaaminen on laajentunut ja syventynyt. Tekijän aikaisemmat tiedot tietosuojasta liittyivät terveydenhuollon ammatilliseen osaamiseen. Näiltä osin tekijän aikaisempaa osaamista syvennettiin. Tietämys laajeni koskemaan myös sosiaalihuollon toimialaa. Uutta tietoa omaksuttiin tarkastelemalla tietosuojaa ohjelmistotoimittajan näkökulmasta. Tekijän ohjelmistotuotanto-osaaminen syveni, koska tässä opinnäytetyössä pohdittiin tietosuojan merkitystä ohjelmistotuotantoprosessin eri vaiheissa. Keskeistä on ymmärtää, mitkä seikat ovat ohjelmistotoimittajan vastuulla ja mitkä kuuluvat asiakasorganisaation ratkaistaviksi. Projekti myös havainnollisti muuttuvien normistojen seuraamisen merkityksen ohjelmistotuotannossa.

6 TULOKSET

6.1 Tavoitteiden saavuttaminen

Projektille asetetut tavoitteet onnistuttiin saavuttamaan pääosin kokonaan. Hyvinvointialan yksityisten palveluntuottajien toiminnanohjaus- ja asiakashallintajärjestelmään kirjattujen asiakkaiden tietosuojan toteutumista ohjaava normisto sekä sen keskeiset seikat kerättiin ja kirjattiin. Teoriatietoa syvennettiin analysoimalla normiston vaikutusta Internetissä käytettävän sovelluksen suunnitteluun ja toteutukseen sekä SaaS-ohjelmistopalvelutuotantoon. Lisäksi kerättiin tietoa normistossa tapahtuvista tulevista muutoksista. Hankitun tietämyksen avulla arvioitiin TUHA-sovelluksen ja TUHA-ohjelmistopalvelun tietosuojan toteutumista. Projektin päätteeksi arviointitulosten pohjalta esitettiin sovellukselle ja ohjelmistopalvelulle eettisesti ja liiketaloudellisessa mielessä kannattavia kehitysehdotuksia. Tietosuojaan liittyvää tietoa kerättiin, analysoitiin ja arvioitiin ohjelmistotoimittajan näkökulmasta tietoliikenneturvallisuuden, tietoaineistoturvallisuuden, ohjelmistoturvallisuuden sekä käyttöturvallisuuden osa-alueilta. Projektin tuotoksena syntyi joitakin uusia käytänteitä sekä uusia, aikaisemmista tuotteista poikkeavia ratkaisuja. Tiedon keruu normistosta oli riittävän yksityiskohtaista, joten tuloksia voidaan hyödyntää myös yrityksen muissa projekteissa. Kehitysehdotuksia voidaan käyttää eräänä näkökulmana suunniteltaessa yrityksen liiketoimintaa TUHA-sovelluksen ja sen ohjelmistopalvelun osalta.

Projektin aikana esitettiin tietosuojavaltuutetun toimistolle sähköpostitse kaksi kysymystä. Kysymyksillä haluttiin saada asiantuntijan vahvistus eräisiin ohjelmistosuunnittelua koskeviin tulkinnanvaraisiin kysymyksiin. Kysymyksistä ensimmäinen käsitteli jatkuvan sairauskertomus -ominaisuuden olemassaoloa sosiaalihuollon tietojärjestelmässä. Tähän saatiin tietosuojavaltuutetun toimiston ylitarkastajalta vastaus, ettei ominaisuus ole välttämätön, jos muut terveydenhuollon tietojen käsittelyyn, luovuttamiseen ja säilyttämiseen liittyvät seikat on huomioitu. Toisessa kysymyksessä haettiin vahvistusta käsitykselle, jonka mukaan Internet-verkossa käytettävän hyvinvointialan sovelluksen käyttäjätunnistukseen ja -todennukseen riittää käyttäjätunnus–salasana-pari, kun käyttäjän henkilöllisyys on todennettu käyttäjätunnuksia luovutettaessa ja salasana on

muodostettu vahvan salasanan periaatteita noudattaen. Samassa yhteydessä toivottiin tulkintaa, onko asiakastietojen käsittelyyn käytetyt laitteistot tunnistettava myös tässä yhteydessä. Näihin kysymyksiin ei saatu vastausta projektiaikana. Internetissä käytyjä tai ohjelmistotoimittajien välisiä keskusteluja ei katsottu riittävän luotettaviksi ja objektiivisiksi tietolähteiksi. Projektitavoitteen ei voida katsoa täysin toteutuneen näiltä osin.

6.2 Menetelmän rajoitukset

Projektissa käytetyssä menetelmässä rajattiin tarkastelun ulkopuolelle suuria sovelluksen kokonaisturvallisuuteen vaikuttavia osa-alueita. Tarkastelun ulkopuolelle jäivät kokonaan asiakasorganisaation hallinnollinen sekä henkilöstöön liittyvä turvallisuus, fyysinen turvallisuus ja laitteistoturvallisuus. Tietoliikenneturvallisuutta tarkasteltiin vain rajatusti. Rajauksia jouduttiin tekemään projektiin käytettävissä olevan ajan sekä työmäärän vuoksi. Käytännössä sovelluksen tietoturvan eri osa-alueet vaikuttavat kiinteästi toinen toisiinsa, joten niiden eriyttäminen on keinotekoista. Tarkastelun rajaaminen pelkästään ohjelmistotoimittajan näkökulmaan rajoittaa jonkin verran tarkastelutuloksia. Arvioinnissa huomioitiin kuitenkin ohjelmistopalveluntuottajan hyvien kauppatapojen mukainen vastuu ohjata asiakasta rekisterinpitoon kuuluvissa asioissa. Tämän vuoksi tässä opinnäytetyössä on eräiltä kohdin tarkasteltu myös muita kuin perinteisiä ohjelmistotoimittajan vastuita.

Normiston edellyttämän tietosuojavaatimusten toteutumisen arviointiin ei kehitetty varsinaista mittaristoa, vaan arviointi suoritettiin subjektiivisena analyysinä taustaaineistossa käsiteltyjen aihepiirien osalta. Tätä menetelmää käytettäessä lukija ei voi arvioida analyysin objektiivisuutta luotettavasti. Tietojen keruun ja analyysin osalta pyrittiin käyttämään vain Codebird Oy:stä riippumattomia luotettuja lähteitä, kuten asiantuntijoiden kirjoittamia lähteitä tai suoraa sähköpostitse toimitettua tiedonantoa.

6.3 Tietosuojaan liittyviä huomioita

Normistoa tarkasteltaessa huomattiin, että eräitä tietosuojan toteutumiseen kriittisesti vaikuttavia periaatteita on määritelty normistossa hyvin väljästi. Esimerkiksi avoimessa

verkkoympäristössä toimivan sovelluksen käyttäjätodennuksen minimivaatimuksena on riittävän luotettava toimintatapa. Todennuksen teknisiä ratkaisutapoja ei ole määritelty tämän tarkemmin. Normiston väljyys antaa ohjelmistokehittäjille vapauksia toteuttaa tuoteominaisuudet oman parhaan näkemyksensä mukaisesti. Ongelmalliseen tilanteeseen joutuvat kuitenkin sovelluksen käytöstä rekisterinpitäjinä vastaavat tahot. Onko heillä aina riittävää asiantuntemusta arvioida eri tuotteiden käyttäjätodennuksen tietosuojatasoja? Arviointi onnistunee, kun sen toteutuksessa on mukana tietojenkäsittelyalan koulutuksen saaneita henkilöitä. Suurten organisaatioiden tietohallintaosastoilla työskentelee yleensä alan ammattilaisia. Yksityiset ja kolmannen sektorin hyvinvointialan palveluyritykset ovat yleensä pieniä tai keskisuuria organisaatioita, joilla ei ole välttämättä varaa palkata erityisasiantuntemusta. Heidän on arvioitava eri tietojärjestelmätuotteita parhaan taitonsa mukaan tai luotettava muiden tekemiin arviointeihin.

Edellä esitetyssä tilanteessa voi rekisterinpitäjä edellyttää sosiaali- ja terveydenhuollon sähköiseltä tietojärjestelmätuotteelta sertifiointia. Sovellussertifikaatin myöntää riippumaton taho, jolla on asiantuntemusta arvioida tuotteen tietosuojan toteutumisen ja tietoturvallisuuden tasoa. Tuotteen sertifiointi vaatii pitkäjänteistä kehitystyötä ja se nostaa usein tuotteen hintaa. Tällä hetkellä suomalaisia hyvinvointialalle suunnattuja sovelluksia on niin vähän, ettei ohjelmistotoimittajilla ole juurikaan ollut tarvetta sertifioida tuotteitaan. Yleisesti keskusteluissa on esitetty, että julkisen vallan tulisi säädellä sosiaali- ja terveydenhuollon sovellusmarkkinoita edellyttämällä tuotteilta sertifiointia.

Rekisteröityjen tietosuoja tulisi olla eräs keskeisimmistä sähköisten järjestelmien laatuvaatimuksista. Tietosuojan tietoinen tai huolimattomuudesta johtuva rikkominen on rangaistava teko. Henkilötietolaissa määritellään henkilörekisteririkkomus ja laissa sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä määritellään asiakastietojen käsittelyrikkomus. Tietosuojan rikkominen aiheuttaa asiakassuhteessa aina luottamuksen menetyksen. Jos osapuolten välillä ei ole aitoa luottamusta, koko toiminta menettää tarkoituksensa. Tietosuoja ei ole koskaan asia, josta on tai ei ole huolehdittu. Se rakentuu useista pienistä toisistaan riippuvaisista yksityiskohdista, joiden toteutumista tulee valvoa jatkuvasti ja jonka ratkaisut ovat riippuvaisia ympäröivästä todellisuudesta. Vaikka Codebird Oy on TUHA-sovellusta rakentaessaan tietoisesti tavoitellut rekisteröidyn tietosuojaa toteuttavaa ratkaisua, opinnäytetyöllä osoitettiin, että kehittämistyötä on edelleen jatkettava.

Ohjelmistotoimittajan tavoitteena sovelluksen ja siihen liittyvän palvelukokonaisuuden rakentamisessa on yrityksen luonteen mukaisesti voiton tuottaminen. Ohjelmistokehityksen on toimittava lakien määrittelemissä rajoissa, mutta voiton tuottamiseksi sitä keskeisimmin ohjaa markkinoinnin ja myynnin määrittelemät suuntaviivat. Tuotteen on oltava kilpailukykyinen. Muussa tapauksessa tuotteella ei ole markkinoita, eikä tuote tuota toivottua voittoa. Jos asiakaskunta odottaa tuotteelta tietosuojan toteuttavia ominaisuuksia, on todennäköistä, että ohjelmistotoimittaja pyrkii rakentamaan tuotteensa odotukset täyttäviksi. Lakien ja markkinaodotusten lisäksi sovellusten tietosuojaominaisuuksiin vaikuttavat ohjelmistoyrityksen resurssit. Taloudelliset resurssit ja erityisesti sovelluskehittäjien osaamistaso joko mahdollistaa tietosuojaa toteuttavat ominaisuudet tai päinvastaisessa tilanteessa estää niiden toteutumisen. Sovelluskehityksessä käytettyjen toimintaprosessien ja käytäntöjen laadukkuus sekä jatkuva kehittäminen ovat osaltaan sovelluksen ja siihen liittyvän palvelukokonaisuuden tietosuojan mahdollistajia.

6.4 Tulosten hyödyntäminen ja jatkohaasteet

Projektin aikana syntyneitä tuotoksia on hyödynnetty yhtä aikaa projektin toteutumisen aikana. Tuotoksia on hyödynnetty sekä TUHA-sovelluksen ohjelmistotuotannossa että ohjelmistopalvelun kehitysprosessissa. Eräitä projektin alkuvaiheessa esiin nousseita tietosuojaan vaikuttavia asioita on jo toteutettu muuttamalla TUHA-sovelluksen toiminnallisuutta ennen version 1.0.0 valmistumista. Myös ohjelmistopalvelutoimintaa on kehitetty projektin aikana kerättyjen tietojen perusteella. Näistä esimerkkeinä ovat mm. potilastietojen yhteyteen tallentuvat tiedot kirjaamisajankohdasta, kirjaajasta sekä kirjaajan ammatillisesta tehtävästä, ohjelmistotoimittajan ilmoitus tietosuojavaltuutetun toimistolle ulkoistetun teknisen rekisterinpidon palvelutuotannon aloittamisesta sekä koko ohjelmistopalveluprosessin asiakasyhteistyön sisällön kehittäminen. Valtaosa kehitysehdotuksissa käsitellyistä asioista on jo huomioitu sovelluksen 2.0.0 versiosuunnitelmissa. Suunnitelmat ehdotusten käytännön toteuttamisesta on jo aloitettu. Uuden version valmistuminen ajoittuu tämän vuoden syksyyn.

Eräitä tietosuojan toteutumisen kannalta vähemmän kriittisiä yksityiskohtia jää mahdollisesti toteutettavaksi myöhemmissä TUHA-sovelluksen kehitysversioissa. Eettisenä ratkaisuna ajankohtien siirtäminen ei ole kestävää ajattelua, mutta näihin ratkaisuihin on

päädytty liiketaloudellisista syistä. Projektissa avoimeksi jääneisiin kysymyksiin tulee aktiivisesti etsiä vastauksia asiantuntijatahoilta ja seurata myöhemmin voimaantulevien asetusten sisältöjä. Codebird Oy:n sovelluskehitysprosessin parantamiseksi esitettyjen kehitysehdotusten toteuttaminen vaatii aikaa, sillä totuttujen toimintatapojen muuttamisen on oltava suunnitelmallista.

Jatkossa TUHA-sovelluksen ja -ohjelmistopalvelun tietosuojaa tulisi tarkastella ainakin fyysisen turvallisuuden sekä laitteistoturvallisuuden osa-alueilta. Käytännössä arviointi voitaisiin toteuttaa esimerkiksi laatimalla sovelluksen ja ohjelmistopalvelun tietoturva-analyysi. Analyysin tuloksia voitaisiin hyödyntää TUHA-ohjelmistopalvelun asiakkaille tehtävän tietoturvaselvityksen laadinnassa. Tietosuojaa olisi mielenkiintoista tarkastella myös rekisterinpitäjän näkökulmasta. Tässä tarkastelussa painottuisivat erityisesti hallinnollinen turvallisuus sekä henkilöstöturvallisuus.

6.5 Työskentelyn arviointi

Projekti toteutettiin suunnitellussa aikataulussa. Projektisuunnitelman mukaiset työmäärät ylittyivät hieman. Projektin toteuttaminen vaati kurinalaista työtä, sillä työ tehtiin pääosin päivätyön ohella iltaisin ja viikonloppuisin. Palkallisena päivätyönä projektia tehtiin projektisuunnitelman mukaisesti kahtena viikon mittaisena jaksona tammikuussa ja helmikuussa 2007. Työn eri vaiheita toteutettiin käytännössä rinnakkain, vaikka projektisuunnitelmaan oli laadittu erilliset ajanjaksot jokaiselle työvaiheelle. Suurimmaksi riskiksi arvioitu aikatauluriski ei toteutunut.

Projektin vaikeimpana asiana koettiin normistossa esitettyjen asioiden soveltamista ohjelmistokehitykseen. Koska tekijän aiemmat kokemukset ohjelmistokehityksestä olivat vähäiset, jouduttiin soveltamistyötä varten opiskelemaan tietosuojan lisäksi monia alan perusteoksia. Tekijän oman oppimisprosessin kannalta tämä oli hyvä asia, sillä osaaminen laajeni monella eri saralla. Tietosuoja-arviointityötä helpotti tekijän aiempi terveydenhuollon toimialueen vahva osaaminen ja sen käsitteiden hallitseminen. Tekijällä oli lisäksi aiempaa kokemusta projektityyppisestä työskentelystä. Tämä helpotti projektin hallintaan liittyvää työskentelyä.

LÄHDELUETTELO

Ahonen, T. & Hämeen-Anttila, T. 2004. JSP-ohjelmointi. Jyväskylä. Docendo Finland Oy.

Chong. F. & Carraro, G. 2006. Architecture Strategies for Catching the Long Tail [verkkodokumentti]. Microsoft Corporation. [Viitattu 17.2.2007]. Saatavissa: http://msdn2.microsoft.com/en-us/library/aa479069.aspx

Chong, F., Carraro, G. & Wolter, R. 2006. Multi-Tenant Data Architecture [verkkodokumentti]. Microsoft Corporation. [Viitattu 17.2.2007]. Saatavissa: http://msdn2.microsoft.com/en-us/library/aa479086.aspx

Codebird Oy:n sivut [verkkodokumentti]. [Viitattu 18.1.2007]. Saatavissa: http://www.codebird.com/

FinSoc 2001. Arviointi sosiaalipalveluissa. Katsaus arvioinnin peruskysymyksiin [verkkodokumentti]. Sosiaali- ja terveysalan tutkimus- ja kehittämiskeskus. FinSoc Työpapereita 3/2001. [Viitattu 18.1.2006]. Saatavissa: http://groups.stakes.fi/NR/rdonlyres /A826D5F7-40D4-4A20-8E3E-02194FD5AAC9/0/Ty%C3%B6papereita32001.pdf

Hakala, M., Vainio, M. & Vuorinen, O. 2006. Tietoturvallisuuden käsikirja. Jyväskylä. Docendo Finland Oy.

Hakkerin käsikirja. 2002. Edita Publishing Oy. IT Press.

Hassol, A., Walker, J., Kidder, D., Rokita, K., Young, D., Pierdon, S., Deitz, D., Kuck, S. & Ortiz, E. 2004. Patient experiences and attitudes about access to a patient electronic health care record and linked web messaging. Journal of the American Medical Informatics Association [verkkolehti]. Volume 11, Issue 6, pages 505-513. [Viitattu 28.12.2006]. Saatavissa: https://lillukka.samk.fi/login
(> Elsevier sciencedirect > keywords: Electronic health care & author: Hassol > Full Text + Links). Palvelu vaatii Lillukka-käyttäjätunnuksen.

HE 253/2006 = HE 253/2006 vp. Hallituksen esitys eduskunnalle sosiaali- ja terveydenhuollon asiakastietojen sähköistä käsittelyä koskevaksi lainsäädännöksi.

Heiliö, P-L. & Ylipartanen, A. 2006a. Tietosuoja osana palvelujen laatua. Teoksessa Narikka, J. (toim.) Sosiaali- ja terveyspalvelujen lainsäädäntö käytännössä. Helsinki. Tietosanoma Oy, 628-632.

Heiliö, P-L. & Ylipartanen, A. 2006b. Tietosuojaa ohjaavat säännökset. Teoksessa Narikka, J. (toim.) Sosiaali- ja terveyspalvelujen lainsäädäntö käytännössä. Helsinki. Tietosanoma Oy, 633-654.

Heiliö, P-L. & Ylipartanen, A. 2006c. Asiakasrekistereihin sisältyvien tietojen salassapito ja suojaaminen. Teoksessa Narikka, J. (toim.) Sosiaali- ja terveyspalvelujen lainsäädäntö käytännössä. Helsinki. Tietosanoma Oy, 655-664.

Helopuro, S., Perttula, J. & Ristola, J. 2004. Sähköisen viestinnän tietosuoja. Helsinki. Talentum.

HetiL = L 22.4.1999/523. Henkilötietolaki.

Hirsjärvi, S., Remes, P. & Sajavaara, P. 2000. Tutki ja kirjoita. Helsinki. Tammi.

Höök, M. 2007. Tietosuojavaltuutetun toimisto vastaa [yksityinen sähköpostiviesti]. Vastaanottaja: Anita Kemppinen. Lähetetty 23.1.2007 klo 15:01 (GMT +0200).

JUHTA 2004. JHS 159 suositus [verkkodokumentti]. Julkisen hallinnon tietohallinnon neuvottelukunta. [Viitattu 28.1.2007]. Saatavissa: http://www.jhs-suositukset.fi/intermin/hankkeet/jhs/home.nsf/pages/61856314E6BD1256C225713A005D53BC

Kauppinen, S & Niskanen, T. 2005. Yksityinen palvelutuotanto sosiaali- ja terveydenhuollossa. Sosiaali- ja terveydenhuollon tutkimus- ja kehittämiskeskus. Raportteja 288. Helsinki. Stakes.

Kilpilinna, J. 2004. Tietoturvallisuuden erityiskysymykset ohjelmiston implementointivaiheessa. Teoksessa Paavilainen, J. (toim.) Tietoturvallinen ohjelmointi [verkkodokumentti]. Tampereen yliopisto. Tietojenkäsittelytieteiden laitos. Sarja B-2004-5, 43-50. [Viitattu 28.10.2006]. Saatavissa: http://www.cs.uta.fi/reports/bsarja/B-2004-5.pdf

Kleemola, M. 1999. Tietosuoja tietotekniikan käytössä. Teoksessa Saranto, K. & Korpela, M. (toim.) Tietotekniikka ja tiedonhallinta sosiaali- ja terveydenhuollossa. Helsinki. WSOY, 159-174.

Kleemola, M. & Tervo-Pellikka, R. 1998. Tietosuoja. Vaatimukset verkottuvassa tietojärjestelmässä. Espoo. Suomen Atk-kustannus Oy.

Kontio, J., Lassila, A. & Maula, M. 2006. Ohjelmistoyrityskartoitus 2006, Suomalainen ohjelmistotuoteliiketoiminta 2005 [verkkodokumentti]. Helsinki. Teknillinen korkeakoulu. Ohjelmistoliiketoiminnan laboratorio, Yritysstrategian ja kansainvälisen liiketoiminnan laboratorio. [Viitattu 17.10.2006]. Saatavissa: http://www.sbl.tkk.fi/oskari/Press_Oskari2006_220806_final.pdf

Kosonen, P., Peltomäki, J. & Silander, S. 2005. Java 2 Ohjelmoinnin peruskirja. Jyväskylä. Docendo Finland Oy.

Lampola, M., Lemström, T., Löfberg, C., Kulmala, T., Einovaara, P., Sampo, A. & Koskinen, P. 2003. ASP käsikirja. ASP-toiminnan arvoverkko ja juridiset mallit. Tampereen teknillinen yliopisto. Tuotantotalouden osasto. Tutkimusraportti 5 / 2003. Tampere. Tampereen teknillinen yliopisto.

Larjovuori, R-L. 2004. Ennakointitutkimus hyvinvointipalveluiden tulevaisuudesta Pirkanmaalla [verkkodokumentti]. Pirkanmaan TE-keskuksen julkaisuja 8. Tampereen yliopisto. Liiketaloudellinen tutkimus- ja koulutuskeskus. [Viitattu 27.12.2006]. Saatavissa: http://www.piramk.fi/hyke/Materiaalit/hyvinvointi.pdf

Meloni, J. 2003. MySQL Trainer Kit. Edita Publishing Oy. IT Press.

Muttilainen, V. 2006. Suomalaiset ja henkilötietojen suoja [verkkodokumentti]. OPTL:n julkaisuja 218. Oikeuspoliittinen tutkimuslaitos. Helsinki. [Viitattu 28.12.2006]. Saatavissa: http://www.optula.om.fi/35424.htm

MySQL AB. 2007. MySQL 3Development Roadmap [verkkodokumentti]. [Viitattu 16.2.2007]. Saatavissa: http://dev.mysql.com/doc/refman/5.1/en/roadmap.html

Narikka, J. 2006. Asiakastietojen käsittelyn avoimuus ja rekisteröidyn oikeudet. Teoksessa Narikka, J. (toim.) Sosiaali- ja terveyspalvelujen lainsäädäntö käytännössä. Helsinki. Tietosanoma Oy, 696-671.

Nordström, H. & Sääksjärvi, M. 2004. Application Service Provisioning as a Strategic Network – Evaluation of a Failed ASP Project [verkkodokumentti]. Helsinki School of Economics. Department of Management. In Fourth IFIP Conference on e-Commerce, e-Business, and e-Government (I3E). Toulouse. France. [Viitattu 17.10.2006]. Saatavissa: http://project.hkkk.fi/vertigo/paperit/asp_as_a_strategic_network.pdf

Ohtonen, J. (toim.) 2002. Satakunnan Makropilotti: tulosten arviointia [verkkodokumentti]. FinOHTAn raportti 21/2002. [Viitattu 28.10.2006]. Saatavissa: http://finohta.stakes.fi/NR/rdonlyres/E81C4727-11B1-437D-AFD6-79D8A7BDC9DF/0/r021f.pdf

Paavilainen, J. 1998. Tietoturva. Espoo. Suomen Atk-kustannus Oy.

Pahlman, I. (toim.) 2005. Asiakirjajulkisuus ja tietosuoja sosiaali- ja terveydenhuollossa. Helsinki. Edita Publishing Oy.

Pajukoski, M. 2004. Sähköinen asiointi sosiaali- ja terveydenhuollossa. Lainsäädännön rajat ja mahdollisuudet. Sosiaali- ja terveysalan tutkimus- ja kehittämiskeskus. Raportteja 283. Helsinki. Stakes.

PotA = A 1.3.2001/99. Sosiaali- ja terveysministeriön asetus potilasasiakirjojen laatimisesta sekä niiden ja muun hoitoon liittyvän materiaalin säilyttämisestä.

PotL = L 17.8.1992/785. Laki potilaan asemasta ja oikeuksista.

Reponen, K. 2006. Terveydenhuollon organisaation tietoturvallisuus henkilöstön arvioimana [verkkodokumentti]. Sosiaali- ja terveydenhuollon tietohallinto. Kuopion yliopisto. Terveyshallinnon ja -talouden laitos. Terveyshallintotieteen Pro gradu -tutkielma. [Viitattu 28.10.2006]. Saatavissa: http://www.uku.fi/tht/opinnaytteet/kreponengradu.pdf

Rintala, E-L. 2005. Hyvinvointi- ja teknologiayrittäjien yhteistyö käynnistyi. Prizz.Uutiset 3/2005, 6.

Robson, C. 2000. Käytännön arvioinnin perusteet. Opas evaluaation tekijöille ja tilaajille. Helsinki. Tammi.

SHAL = L 22.9.2000/812. Laki sosiaalihuollon asiakkaan asemasta ja oikeuksista.

Sosiaali- ja terveysalan tietoyhteiskuntayksikkö 2006. Sosiaali- ja terveydenhuollon toimialaluokitus 2002. Kansallinen koodistopalvelu [verkkotietokanta]. Sosiaali- ja terveysalan tutkimus- ja kehittämiskeskus. [Viitattu 27.12.2006]. Saatavissa: http://sty.stakes.fi/FI/koodistopalvelu/koodisto.htm (> Tuotantokoodistopalvelin > 1.2.246.537.6.27 > Koodit)

Sosiaali- ja terveysministeriö 2005. Tietoteknologian käytön edistäminen sosiaalihuollossa -hankesuunitelma [verkkodokumentti]. Sosiaali- ja terveysministeriön monisteita 2005:1. [Viitattu 1.1.2007]. Saatavissa: http://www.stm.fi/Resource.phx/publishing /store/2005/01/cd1106564669942/passthru.pdf

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

SVTSL = L 16.6.2004/516. Sähköisen viestinnän tietosuojalaki.

SähkAL = L 24.1.2003/14. Laki sähköisistä allekirjoituksista.

Sääksjärvi, M., Nordström, H., Santonen, T. & Lassila, A. 2004. Ohjelmistopalvelua verkosta (Software as a Service) [verkkodokumentti]. TEKESin VERTIGO-tutkimus: Working Paper 1/2004. HKKK. Tietojärjestelmätiede. [Viitattu 8.10.2006]. Saatavissa: http://project.hkkk.fi/vertigo/paperit/SAASRAP-FIN1.pdf

Tammisalo, T. 2005. Sosiaali- ja terveydenhuollon tietojärjestelmien tietoturvan ja tietosuojan hallinnan periaatteet ja hyvät käytännöt [verkkodokumentti]. Sosiaali- ja terveysalan tutkimus- ja kehittämiskeskus. Raportteja 5/2005. [Viitattu 28.10.2006]. Saatavissa: http://www.stakes.fi/verkkojulkaisut/raportit/Ra5-2005.pdf

Terrar, D. 2006. Saas – the insider's guide [verkkodokumentti]. Business Two Zero. [Viitattu 29.1.2006]. Saatavissa: http://biztwozero.com/btz/saas-the-insiders-guide/

Thomas, T. 2005. Verkkojen tietoturva, perusteet. Edita Publishing Oy. IT Press.

Tietosuojavaltuutetun toimisto 2001. Henkilötietolain merkitys kunnallisessa sosiaalihuollossa [verkkodokumentti]. Asiaa tietosuojasta -sarja 1/2000, päivitetty 2001. [Viitattu 28.10.2006]. Saatavissa: http://www.tietosuoja.fi/uploads/ezg64pfwohs1.rtf

Tietosuojavaltuutetun toimisto 2003. Käyttäjälokin tietojen käsittely henkilötietolain mukaan [verkkodokumentti]. Asiaa tietosuojasta -sarja 1/2003. [Viitattu 28.10.2006]. Saatavissa: http://www.tietosuoja.fi/uploads/6ty78bp189atp.rtf

Winblad, I., Reponen, J., Hämäläinen, P. & Kangas, M. 2006. Informaatio- ja kommunikaatioteknologian käyttö Suomen terveydenhuollossa vuonna 2005 [verkkodokumentti]. Sosiaali- ja terveysalan tutkimus- ja kehittämiskeskus. Raportteja 7/2006. [Viitattu 28.10.2006]. Saatavissa:
http://www.stakes.fi/verkkojulkaisut/raportit/R7-2006-VERKKO.pdf

Ylipartanen, A. 2004. Tietosuoja terveydenhuollossa. Potilaan asema ja oikeudet henkilötietojen käsittelyssä. Helsinki. Tietosanoma Oy.

LIITELUETTELO

Liitteet 1. ja 2. sisältävät luottamuksellisia tietoja, joten ne luovutetaan Satakunnan ammattikorkeakoulun vuoden 2006 opinnäytetyöohjeen julkisuussäännösten mukaisesti vain opinnäytetyön tilaajalle Codebird Oy:lle.