Tietoturvallinen kommunikaatioalusta
Luovutusten ja luovutuslokin hallinnan suositukset

Timo Itälä ja Pekka Ruotsalainen

Osaavien keskusten verkoston julkaisuja 6/2004

ISBN 951-33-1578-9

Stakesin monistamo, Helsinki

SISÄLLYSLUETTELO

ESIPUHE

Valtioneuvoston terveydenhuollon turvaamista koskevan periaatepäätöksen (11.4.2002) mukaisesti "valtakunnallinen sähköinen sairauskertomus" otetaan käyttöön vuoden 2007 loppuun mennessä. Sosiaali- ja terveysministeriö asetti vuoden 2003 alussa sähköisten potilasasiakirjojen käyttöönottoa ohjaavan työryhmän. Samalla käynnistettiin valtakunnalliset määrittelyhankkeet potilaskertomuksen ydintietojen ja yhteisten sanomien harmonisoimiseksi sekä tietoturvallisen tiedonvälityksen ohjeistuksen laatimiseksi. Yksi käynnistyneistä määrittelyhankkeista oli tietoturvallinen kommunikaatioalustaprojekti, josta sosiaali- ja terveysministeriö teki Stakesin kanssa sopimuksen. Sopimuksen mukaan Tietoteknologian osaamiskeskus (OSKE) tuottaa konkreettiset ohjeistukset/suositukset, jotka mahdollistavat potilasasiakirjojen ja -tiedon siirron tai käytön terveydenhuollon toimintayksiköiden välillä.

Koska tietoturvallinen kommunikaatioalusta -hanke on osa sähköisen potilaskertomuksen käyttöönottohanketta, tuottaa se ennen kaikkea ohjeistusta sähköisten potilastietojärjestelmien väliseen tiedon vaihtoon. Projekti tavoitteena on tuottaa hyvän käytännön määrittelyt seuraaviin kokonaisuuksiin:

- terveystietojen luovuttaminen
- sähköisen suostumuksen hyvät toimintatavat
- lokitietojen käyttö
- sähköisen allekirjoituksen hyvät toimintatavat
- sähköisen arkistoinnin hyvät periaatteet
- käytännön ohjeet terveydenhuollon PKI-infrastruktuurin toteuttamiselle
- potilaiden sekä terveydenhuollon ammattihenkilöiden ja palveluntuottajien nimeämisen hyvä käytäntö ISO-OID-koodiston mukaan

Suostumusta ja tietojen luovuttamista käsittävän työn alkuvaiheessa ilmeni, että sähköisen asiointiympäristön ongelmatiikan rinnalla on tarpeellista tarkastella tietosuojaa ja tietojen käyttöä erityisesti lainsäädännölliseltä kannalta. Lisäksi tulee ottaa huomioon nykyinen, tosiasiassa osittain manuaalinen toimintaympäristö ja sen rajoitteet.

Stakes on solminut sopimuksen luovutusten ja luovutuslokin hallinnan suositusten tuottamishankkeen asiantuntijatyöstä Conceptia Oy:n kanssa. Stakesin vastuuhenkilö hankkeessa on ollut tutkimusprofessori Pekka Ruotsalainen tietoteknologian osaamiskeskuksesta (OSKE). Hankkeen projektipäällikkönä on ollut Conceptia Oy:stä Timo Itälä.

Projekti tutustui 11 erilaiseen potilastietojärjestelmään haastattelemalla sekä järjestelmätoimittajien että tietojärjestelmien käyttäjäorganisaatioiden asiantuntijoita.

Sosiaali- ja terveysministeriö lähetti raportin laajalle lausuntokierrokselle. Lausuntoja antoivat JUHTA, Etelä-Karjalan sairaanhoitopiirin kuntayhtymä, Kela, Helsingin ja Uudenmaan sairaanhoitopiiri, Kymenlaakson sairaanhoitopiirin kuntayhtymä, Turun terveystoimi, Sisäasian ministeriö, Suomen potilasliitto ry., Suomen sairaanhoitajaliitto ry., Pohjois-Karjalan sairaanhoitopiiri/Antti Turunen ja Pekka Nevalainen, Mediconsult Oy, Doctorex Oy, Kanta-Hämeen shp/Taimo Turunen, Stakes/Marja Pajukoski, Tietosuojavaltuutetun toimisto, varatuomari Hannu Sorvari, Ensitieto Oy, Pirkanmaan sairaanhoitopiiri, Suomen Reumaliitto ry., Helsingin terveyskeskus, OYS/Timo Kouri, Keravan kaupungin sosiaali- ja terveysvirasto, Suomen Mielenterveysseura sekä kansallisen terveysprojektin sähköisen potilaskertomuksen ohjausryhmä.

Tämän raportin tarkastelun kohde on ollut tietojen (erityisesti terveydenhuollon asiakastietojen) luovutus toimintayksiköiden välillä. Raportista annetuista lausunnoista ilmeni, että projektin toivottiin tuottavan sen tehtäväksi antoa laaja-alaisempi ohjeistus mm. tietojen käsittelystä toimintayksikössä, potilastietojärjestelmien käyttäjänhallinnasta ja tietojen tallettamisesta potilaskertomuksiin. Käytettävissä olevat voimavarat eivät kuitenkaan mahdollistaneet laajentaa tarkastelua toimintayksikön sisällä tapahtuvaan tietojenkäsittelyyn. On kuitenkin syytä todeta, että toimintayksikössä tapahtuva käsittely ei ole tietojen luovutusta. Edelleen terveydenhuollon ammattihenkilöiden osalta toimintayksikkö päättää, ketkä heistä osallistuvat potilaan hoitoon, jolloin muut henkilöt ovat sivullisia. Toimintayksikössä työskentelevien käyttöoikeudet potilastietoihin on luonnollisesti rajattava tehtävän kannalta tarpeellisiin tietoihin.

Tietojen talletus ja tietojen noutaminen potilaskertomuksista ei ole myöskään kuulunut tämän raportin tehtäväksiantoon. Sama koskee alueellisten tietojärjestelmäkokonaisuuksien käyttäjän hallinnan ongelmatikkaa. Sekä alueelliselle käyttäjänhallinnalle että sähköiselle arkistolle laaditaan myöhemmissä projektissa hyvän toiminnan ohjeet.

Raportin tavoitteena on laatia niin pitkälle kuin mahdollista tekniikkariippumaton ohjeistus. Niinpä esimerkiksi tietojen luovutus on määritelty ja luovutusta koskeva ohjeistus on tehty riippumattomaksi siitä, toteutetaanko luovutus siirtämällä tietoja sanomamuodossa rekisterinpitäjien tietojärjestelmien välillä vai "katsellaanko" tietoja selaimella tms. ohjelmistolla toisen rekisterinpitäjän tietojärjestelmästä.

Saaduista lausunnoista ilmeni edelleen, että käytännön toimijoiden keskuudessa esiintyy erilaisia käsityksiä siitä, mikä on rekisterinpitäjä, mikä on alueellisen tietojärjestelmän luonne, mikä on hoitosuhde, miksi suostumusta yleensä tarvitaan ja miksi suostumus ei voisi olla yleinen. Tämän raportin liitteessä E on tiiviisti käsitelty näitä ja muita palautteissa esille nousseita periaatteellisia kysymyksiä.

Saatujen lausuntojen perusteella on ilmeistä, että tietojärjestelmien ja palvelujen ulkoistaminen muodostaa ongelmakokonaisuuden johon tarvitaan lisää ohjeistusta. Edelleen tarvitaan tarkentavaa ohjeistusta koskien ensihoidon tietojärjestelmiä ja niissä tapahtuvaa hoitotiedon käsittelyä. Tämän raportin laatimisen yhteydessä ei ole ollut mahdollisuutta tuottaa näitä ohjeita.

Raportissa on tehty sekä periaatteellisia että toiminnallisia ehdotuksia. Ehdotusta, joka mahdollistaisi potilaan oikeuden luovutuslokin tarkistamiseen kannatettiin monissa lausunnoissa. Raportissa korostetaan, että tarvitaan pikaisesti valtakunnalliset luokitukset mm. rekisterinpitäjästä, tietojen käyttötarkoituksesta, asiayhteydestä, tietojen sensitiivisyydestä ja erityissuojaustarpeesta. Yksi tärkeä periaatteellinen ehdotus on se, että merkinnät luovutettavien tietojen rekisterinpitäjästä, tietojen käyttötarkoituksesta ja erityissuojaustarpeesta tulee sisältyä luovutettaviin tietoihin. Keskeisiä ehdotuksia ovat myös luovutuspyynnön, luovutussanoman ja luovutuslokin tietosisällöt. Potilastietojärjestelmän käyttöoikeuden luovuttaminen toisessa toimintayksikössä työskentelevälle henkilölle edellyttää sen mahdollistavan lainsäädännön olemassa oloa. Siksi *käyttöoikeuden jakamista toisiin toimintayksikköihin ei voi pitää asianmukaisena toimintana*.

Siirtyminen manuaalisesta sähköiseen ympäristöön edellyttää henkilökunnan koulutusta. Tarvitaan kattava koulutus ja perehdyttämispanostus paikallisella, alueellisella ja valtakunnallisella tasolla sekä henkilökunnan sähköisen potilaskertomuksen että tietoturvallisen tiedonvälityksen suositusten käyttöönoton tukemiseksi.

Tehdyn selvityksen mukaan (liite A) toimintayksiköiden välinen tiedon luovutus on käytännössä vielä melko vähäistä. Tietojärjestelmissä esiintyy myös tietosuojaan liittyviä ongelmia. Osa näistä saattaa johtua siitä, ettei ohjelmistoja ole alun perin osattu suunnitella henkilölain lähtökohdista

Potilaskertomusten digitalisoitumisen ja tietoturvallisen tiedonvaihdon teknisten mahdollisuuksien syntymisen myötä on odotettavissa, että tietojen luovuttaminen tulee merkittävästi lisääntymään. Juuri nyt elämme siis eräänlaista "puoliautomaattista siirtymävaihetta". Tämän raportin ehdotusten käyttöönotto tulisikin aikatauluttaa siten, että suositukset ovat täysimääräisesti voimassa silloin, kun *tietojärjestelmät* kykenevät hoitamaan tietoliikenteen, luovutusten edellytysten tarkistamisen, luovutuksesta informoinnin ja potilaskertomukseen tehtävien merkintöjen tekemisen ilman erillistä manuaalista työtä.

Tässä raportissa on (suostumusraportista poiketen) käytetty termiä potilas merkitsemään sekä potilasta että terveydenhuollon asiakasta. Raportti keskittyy terveydenhuollon toimintayksiköiden väliseen tiedon luovuttamiseen, mutta esitetyt yleiset periaatteet muodostavat hyvän lähtökohdan tuleville sosiaalihuoltoa sekä terveydenhuollon ja sosiaalihuollon välistä tietojen luovutusta koskevalle ohjeistukselle.

Tietoturvalliseen tiedonvälitykseen liittyen on OSKE ja Osaavien keskusten verkosto tuottanut aikaisemmin seuraavat dokumentit ja selvitykset:

- Elektronisen potilaskertomuksen sisältömääritykset, K. Hartikainen, A. Kokkola ja R. Larjomaa, OSVE 4/2000
- Selvitys asiakas- ja potilasasiakirjojen sähköisestä säilytyksestä ja kiistämättömyydestä, A. Ensio ja P. Ruotsalainen, OSVE 1/2001
- Ehdotus sosiaali- ja terveydenhuollon sähköisen asioinnin arkkitehtuuriksi - terveydenhuollon PKI-arkkitehtuuri, OSVE 4/2002.
- Sähköisen asiakas- ja potilasasiakirjojen säilytyksen ja kiistämättömyyden hyvä käytäntö, A. Ensio ja P. Ruotsalainen, OSVE 1/2003. Tämä dokumentti sisältää ehdotukset ammattilaisten, potilaiden, palveluntuottajien ja terveydenhuollon sähköisten dokumenttien yksikäsitteiseksi nimeämiseksi.
- Selvitystyö sosiaali- ja terveysministeriölle "Lääkärin tunnistus sähköisen reseptin kokeilussa - vaihtoehtoisia tapoja koskeva selvitys", P. Ruotsalainen, Helsinki 28.3.2003.
- Eduskunnan vuoden 2003 lopulla hyväksymä lainmuutos sosiaali- ja terveydenhuollon saumattoman palveluketjun ja sosiaaliturvakortin kokeilusta annetusta laista.
- Tietoturvallinen kommunikaatioalusta: Suositukset sähköisen suostumuksen periaatteiksi, T. Mikola, H. Sorvari ja P. Ruotsalainen, Osaavien keskusten verkosto 3/2004.

Kiitän kaikkia tämän suosituksen valmisteluun sen eri vaiheissa osallistuneita henkilöitä ja organisaatioita heidän antamastaan panoksesta ja arvokkaista neuvoista.

Pekka Ruotsalainen
Tietoturvallinen kommunikaatioalusta -projektin vastuuhenkilö
Tutkimusprofessori

1. Valtakunnallinen terveyshanke

Valtioneuvoston terveydenhuollon turvaamista koskeva periaatepäätös valtakunnallisesta terveyshankkeesta annettiin 11.4.2002. Hankkeen tavoitteena on, että väestö saa tarvitsemansa laadukkaan hoidon maan eri osissa. Periaatepäätökseen on kirjattu mm. seuraavat toimenpidealueet:

- toimiva perusterveydenhuolto ja ennaltaehkäisevä työ
- hoitoon pääsyn turvaaminen
- henkilöstön saatavuuden ja osaamisen turvaaminen
- toimintojen ja rakenteiden uudistaminen
- terveydenhuollon rahoituksen vahvistaminen

Toimintojen ja rakenteiden uudistamisen yhtenä kohteena on valtakunnallisen sähköisen sairaskertomuksen käyttöönotto ja terveydenhuollon tietojärjestelmien yhteensopivuuden turvaaminen. Edellä mainitun periaatepäätöksen mukaisesti "valtakunnallinen sähköinen sairauskertomus" otetaan käyttöön vuoden 2007 loppuun mennessä samalla kun toimintojen sekä rakenteiden uudistushankkeet on saatettu loppuun vuoteen 2007 mennessä.

1.1 Osahanke 4.1.3, valtakunnallisen sähköisen sairauskertomuksen käyttöönotto

Sosiaali- ja terveysministeriö asetti 29.1.2003 sähköisten potilasasiakirjojen toteuttamista ohjaavan työryhmän. Samalla käynnistettiin sähköisen sairauskertomuksen käyttöönottoa tukevat valtakunnalliset määrittelyhankkeet mm. potilaskertomuksen ydintietojen, avointen rajapintojen sekä tietoturvallisen tiedonvälityksen ohjeistuksen laatimiseksi.

Osahankkeen tavoitteena on tukea hyvän ja laadukkaan hoidon ja yli organisaatiorajojen tapahtuvan saumattoman hoidon ja palvelun järjestämistä. Katsotaan, että jos terveydenhuollon ammattihenkilöllä on käytössään kokonaiskuva asiakkaan/potilaan aikaisemmasta hoito- ja sairaushistoriasta, voidaan tuottaa nykyistä laadukkaampaa hoitoa. Tavoitteena on siis ”saumatonta hoitoa tukeva saumaton tiedonkulku”.

Sähköisen sairauskertomuksen käyttöönottoprojektin konkreettiseksi tavoitteeksi on asetettu sähköisten potilaskertomusjärjestelmien valtakunnan laajuinen käyttöönotto vuoteen 2007 mennessä, tietojärjestelmien yhteistoiminnallisuus ja terveydenhuollon kansallinen tietoturvallinen tiedonvälitysympäristö[1].

Sähköisen sairauskertomuksen käyttöönottoprojekti jakautuu kolmeen osahankkeeseen. Niiden toteuttamisesta vastaavat Suomen Kuntaliitto (potilaskertomuksen ydintiedot, jatkohoidon suunnitelma, sähköiset lomakkeet ja metadata), Stakes (tietoturvallinen kommunikaatioalusta) ja Suomen HL7 yhdistys (avoimet rajapinnat).

[1] Kansallisen terveydenhuoltoprojektin hanke 4.1.3, Valtakunnallisen sähköisen sairauskertomuksen käyttöönotto, Hankesuunnitelma 17.12.2002

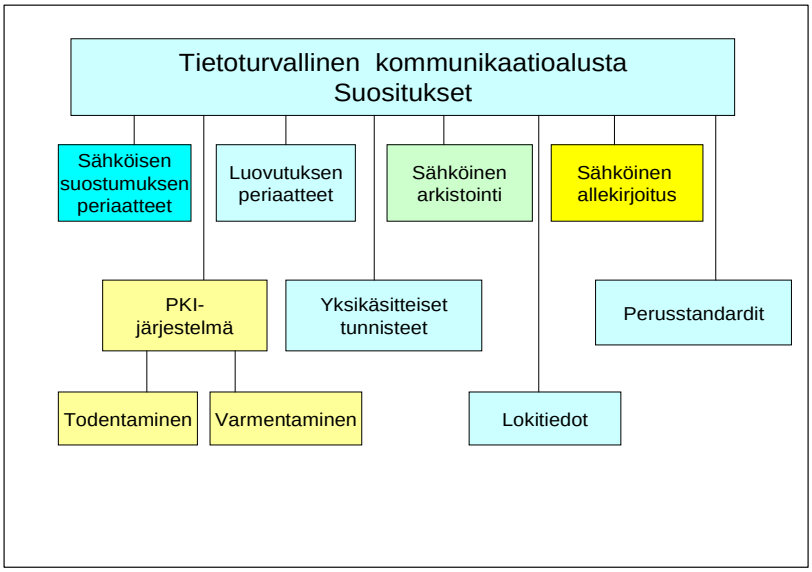
1.2 Tietoturvallinen tiedonvälitysympäristö osahanke

Lähtökohtana on, että hoitotiedon luovutuksen tulee tapahtua siten, että lainmukainen yksityisyyden suoja ja sen edellyttämä tietojen suojaaminen toteutuvat lainsäädännön edellyttämällä tavalla.

Suomalaisessa terveydenhuollon palvelujärjestelmässä terveydenhuollon toimintayksiköt ovat hoitotietojen rekisterinpitäjiä (liite D). Rekisterinpitäjien välillä voidaan luovuttaa salassa pidettävää tietoa joko potilaan suostumuksella tai ilman suostumusta lainsäädännön määrittämin perustein. Potilaan suostumuksella voidaan luovuttaa hänen ongelmansa hoitamisen kannalta tarpeelliset hoitotiedot toiselle rekisterinpitäjälle hoitoon osallistuvien ammattihenkilöiden käyttöön.

Tietoturvallinen kommunikaatioalusta -hanke tuottaa suosituksia tietoturvalliselle tiedonvälitykselle. Hanke koostuu useista osaprojekteista, jotka on esitetty kuvassa 1. Kukin osaprojekti tuottaa suosituksia. Laadittavia suosituksia voidaan hyödyntää niin organisaatioiden välisessä tiedonvaihdossa kuin toteutettaessa terveydenhuollon alueellisia tai seutukunnallisia sähköisiä palveluja. Kommunikaatioalustahankkeessa tuotetaan mm. seuraavat suositukset:

- PKI-arkkitehtuurin käyttöönotto toimintayksikkötasolla
- Potilaiden, ammattihenkilöiden ja palveluntuottajien nimeämisen hyvä käytäntö
- Sähköisen suostumuksen periaatteet
- Luovutusten ja luovutuslokin hallinnan suositukset
- Sähköisen allekirjoituksen hyvät toimintatavat
- Sähköisen arkistoinnin hyvät periaatteet



Kuva 1 Tietoturvallisen kommunikaatioalusta -hankkeen osat

On ilmeistä, että suositukset yksinään eivät riitä turvaamaan tietojärjestelmien yhteistoimintaa. Suositusten lisäksi tietojärjestelmien käytännön yhteistoiminnallisuus tulee edellyttämään myös nykyisten potilastietojärjestelmien yhtenäistämistä.

1.3 Luovutuksen periaatteet - osaprojekti

Suostumusten ja luovutusten hallintaa on kehitetty maassamme tähän mennessä pääsääntöisesti toimintaympäristöön, jossa tietojen vaihto rekisterinpitäjien välillä tapahtuu joko manuaalisesti tai kopioimalla sähköisesti tietoja rekisterinpitäjien asiakasrekistereiden kesken. Tämän projektin yhteydessä tehdyn selvityksen (liite A) perusteella on ilmeistä, että nykyisiä potilastietojärjestelmiä tulee päivittää, jotta ne täyttäisivät lainsäädännön vaatimukset sähköisesti tapahtuvan hoitotietojen luovutuksen ja suostumusten hallinnan osalta.

Luovutuksen periaatteiden määrittely on yksi tietoturvallinen kommunikaatioalusta -hankkeen osaprojekteista. Sen tavoitteena on synnyttää yhtenäiset periaatteet tietojen luovuttamiselle terveydenhuollon rekisterinpitäjien välillä erityisesti digitaalisessa potilaskertomusjärjestelmäympäristössä. Projektissa tehdyn kartoituksen (liite A) perustella ilmeni, että tarvitaan myös kooste yksityisyyden suojaa ja tietoturvaa koskevasta lainsäädännöstä sekä niistä periaatteista, joihin hyvän käytännön mukainen tietojenkäsittely perustuu.

Ohjeistuksen tavoitteena on sekä ohjeistaa rekisterinpitäjien tietojärjestelmien väliset tietojen luovutuksen pelisäännöt että tukea alueellista/seutukunnallista yhteistoimintaa asiakaskohtaisten hoitotietojen käsittelyssä voimassaoleva lainsäädäntö huomioonottaen.

1.4 Toimintayksikössä tapahtuva tietojenkäsittely

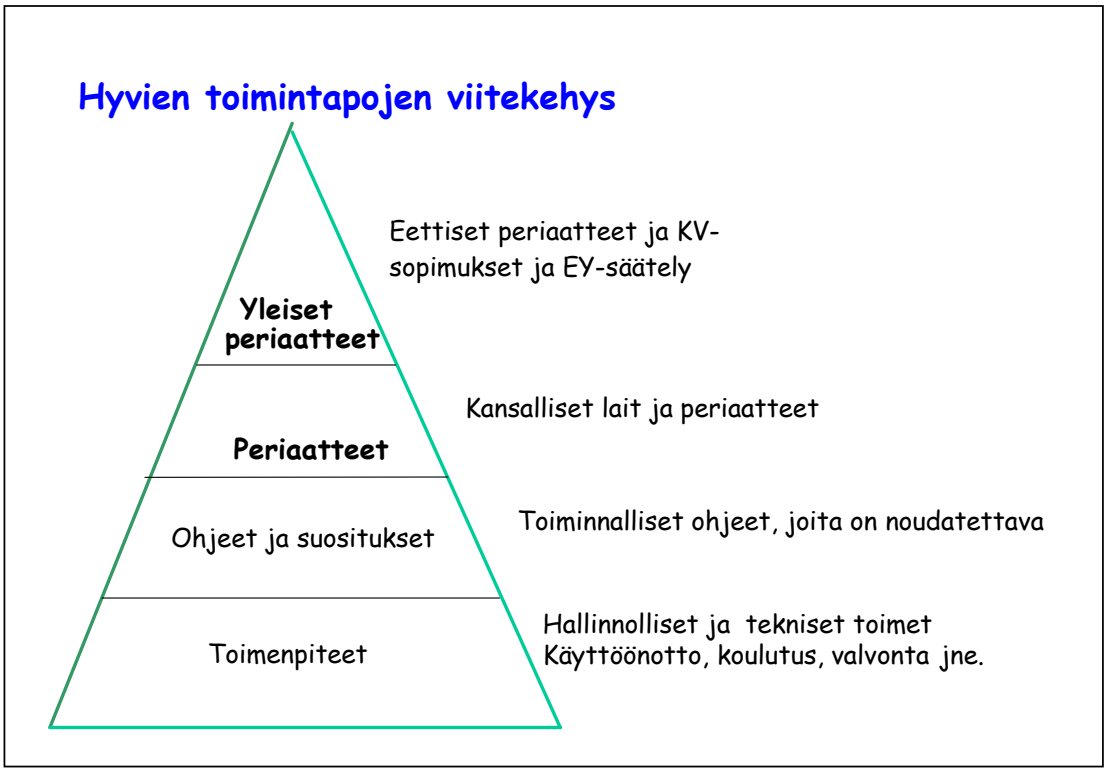
Tämän raportin *tarkastelun kohteena ei ole toimintayksikössä* tapahtuva tietojenkäsittely. Toimintayksikössä tapahtuva käsittely ei ole tietojen luovutusta. Toimintayksikössä tapahtuvan tietojenkäsittelyn osalta on huomattavat, että

- Toimintayksikössä työskentelevien käyttöoikeudet potilastietoihin on rajattava tehtävän kannalta tarpeellisiin tietoihin (STM asetus potilasasiakirjojen laatimisesta, 19.1.2001/99 4 § ensimmäinen momentti).
- Terveydenhuollon ammattihenkilöiden osalta toimintayksikkö päättää, ketkä heistä osallistuvat potilaan hoitoon, jolloin muut henkilöt ovat sivullisia. Potilaan suostumusta tietojen käyttöön toimintayksikön sisällä ei siis hoitoon osallistuvilta edellytetä.

Jotkut toimintayksiköt ovat ottaneet käyttöön yksikön sisäisiä henkilötietolain mukaisia potilastietojen käyttöä rajaavia erityissuojauksia (esimerkiksi sen suhteen, ketkä henkilöt saavat käyttöönsä potilaan psykiatriset hoitotiedot). Osana hyvää asiakaspalvelua voidaan myös kunnioittaa potilaan toivomusta rajata niitä ammattihenkilöitä, jotka osallistuvat hänelle toimintayksikössä annettavaan hoitoon. Tällöin tietojen käsittelyoikeus seuraa hoitosuostumuksen rajoja.

2. Tietojen luovuttamisen yleisperiaatteet

Tietojen luovuttaminen tapahtuu eettisessä, juridisessa, toiminnallisessa, hallinnollisessa ja teknisessä toimintaympäristössä (kuva 2). Nämä kaikki tulee ottaa huomioon laadittaessa suosituksia asiakastietojen luovuttamisesta ja lokitietojen käytöstä.



Kuva 2 Hyvien toimintatapojen viitekehys. (Lähde P. Ruotsalainen, Attachment 8 kirjassa Interreg PACS. Final Report, Research Affairs, University of Helsinki, 2003).

Tämän raportin jäsentelyssä noudatetaan kuvan 2 mallia. Raportissa käsitellään ensin luovutukseen liittyviä yleisiä periaatteita ja sen jälkeen tarkastellaan terveydenhuolto-spesifisiä periaatteita. Lopuksi laaditaan toiminnalliset ohjeet ja annetaan teknisiä toimenpidesuosituksia.

2.1 Lainsäädännöstä johtuvat yleiset vaatimukset tietojenkäsittelylle

Toimintayksiköiden välisellä tietojen luovuttamisella tarkoitetaan henkilötiedon vaihtoa (esim. siirtämistä tai katselua) kahden tai useamman eri rekisterinpitäjän välillä (liite D). *Koska vastuu tietojen luovutuksen lainmukaisuudesta on luovuttavalla rekisterinpitäjällä on tämän raportin suosituksissa painotettu tietoja luovuttavan toimintayksikön näkökulmaa*. Luovutus on myös pyritty määrittelemään tekniikkariippumattomasti. *Luovuttamista on siis sekä tietojen siirto toisen rekisterinpitäjän tietojärjestelmään että tietojen katselu teknisellä yhteydellä* (esimerkiksi www-selaimella) toisen rekisterinpitä-

jän tietojärjestelmästä. Sillä, tallettaako luovutuksen saaja toisen rekisterinpitäjän tietojärjestelmä luovutetut tiedot myöhempää käsittelyä varten tai onko kyseessä pelkkä tietojen katselu, ei ole merkitystä.

Henkilötietolaissa (HeTiL, liite C) säädetään mm. siitä, millä yleisillä edellytyksillä ja periaatteilla henkilötietoja voidaan käsitellä (kuten esimerkiksi kerätä, tallettaa, käyttää, luovuttaa, säilyttää ja hävittää). Henkilötietolaissa lähtökohtaisesti kielletään arkaluonteisten henkilötietojen käsittely yleisellä tasolla sekä säädetään käsittelyn sallivat poikkeukset, jotka koskevat mm. terveydenhuollon, vakuutustoiminnan ja sosiaalihuollon tietojen käsittelyä. Näiden sektoreiden tietojen käsittely perustuu lähtökohtaisesti henkilötietolakiin, mutta näitä alueita koskevalla erityislainsäädännöllä voidaan antaa sekä henkilötietolakia tarkentavia että menettelyjen osalta ohjaavia määräyksiä.

Henkilötietolain periaatteista voidaan katsoa johtuvan seuraavat tämän raportin kannalta oleelliset vaatimukset:

- Etukäteissuunnittelun vaatimus
- Huolellisuus ja suojaamisvelvoite
- Virheettömyys-, eheys- ja luotettavuusvaatimus
- Käyttötarkoitussidonnaisuus
- Tarpeellisuusvaatimus
- Yhteysvaatimus
- Informointivelvoite
- Seurantavelvoite
- Tarkastusoikeus
- Korjaamisoikeus

Tietojärjestelmien toteutuksessa tarpeellisuus- ja huolellisuusvaatimukset sekä suojaamisvelvoitteet ja salassapitovaatimukset voidaan huomioida vain, jos potilasasiakirjojen laatimistapa ja tietorakenteet ovat kaikilta osin suunniteltu ja toteutettu analysoitujen tietotarpeiden pohjalta.

2.2 Terveydenhuollon tietojen käsittelyä ohjaavat lait ja asetukset

Terveydenhuollon tietojen käsittelyä ohjaavia lakeja ovat yleislakien (mm. henkilötietolaki) lisäksi terveydenhuollon erityislait ja säädökset. Potilastietojen käsittelyä ja luovutusta koskevat lait ja asetukset ovat voimassa riippumatta siitä, luovutetaanko tietoja paperilla vai sähköisessä muodossa. Sähköiseen asiointiin ja allekirjoitukseen on lisäksi säädetty omat lakinsa, joissa otetaan huomioon sähköisen toimintaympäristön asettamat erityisvaatimukset.

Säännöksiin liittyy niiden hierarkia. Henkilötietolain yleisvelvoitteet ja muut kohdassa 2.1 mainitut yleiset vaatimukset tulevat terveydenhuollossa sovellettavaksi kaikissa tapauksissa ja kaikkeen henkilötietojen käsittelyyn. Terveydenhuollon lainsäädännössä ei ole niitä korvaavia säännöksiä. Asetustasoinen säätely (esim. potilasasiakirja-asetus 99/2001) ei syrjäytä henkilötietolakia eikä sen edellä mainittuja yleisperiaatteita ja vaatimuksia. Esimerkiksi potilasasiakirja-asetuksessa olevat säädökset voivat olla ja osin ovat henkilötietolakia täydentäviä ja henkilötietolain säännöksiä ohjaavia menettelyjen osalta, mutta ne eivät syrjäytä henkilötietolain säännöksiä. Yleisesti voidaan sanoa, ettei henkilötietolain kanssa ristiriidassa olevia säännöksiä tule soveltaa (Tietosuojavaltuutetun toimiston lausunto).

Yhteenveto tämän raportin kannalta keskeisistä ohjaavista laista, asetuksista ja ohjeista on esitetty liitteessä C. Osaavien keskusten verkoston raportissa 3/2004 (Tietoturvallinen kommunikaatioalusta: Suositukset sähköisen suostumuksen periaatteiksi) on käsitelty yksityiskohtaisemmin ohjaavaa lainsäädäntöä.

2.2.1 Etukäteissuunnittelun vaatimus

Henkilötietojen käsittelyssä ja erityisesti otettaessa käyttöön automaattisen tietojenkäsittelyn ja tiedonsiirron järjestelmiä on syytä ottaa huomioon sekä henkilötietolaissa että -viranomaisten osalta - myös viranomaisten toiminnan julkisuudesta annetussa laissa säädetty etukäteissuunnittelun vaatimus sekä yleisesti hyvän tietojenkäsittelyn ja hyvän tiedonhallinnan aikaansaaminen (katso liite F).

Henkilötietolain 5 ja 6 §:t edellyttävät, paitsi henkilötietojen käsittelyn tarkoituksen etukäteen tapahtuvaa määrittelyä ja tiedon eri käsittelyvaiheiden suunnittelua, erityisesti säännönmukaisten tietolähteiden (käytännössä myös tietosisällön) sekä säännönmukaisten tietojen luovutuksen määrittelyä ja niihin liittyvien tietotarpeiden analysointia (ks. liite 1 ja liite 2). Tässä määrittelytyössä ja määrittelyn käytännön toteutuksessa sekä myös muutoin tehtävien hoidossa ja potilastietojen käsittelyssä tulee ottaa huomioon myös muut tämän raportin kohdassa 2.1 mainitut yleisvelvoitteet (katso myös www.tietosuoja.fi).

2.2.2 Huolellisuus- ja suojausvelvoite

Henkilötietojen käsittelyn huolellisuusvelvoite perustuu henkilötietolain 5 §:ään ja suojaamisvelvoite henkilötietolain 32 §:ään. Potilaslaissa ei ole erillisiä potilastietoihin liittyviä huolellisuus- ja suojaamisvelvoitetta, mutta em. periaatteet ilmenevät muun muassa potilaslain 13 §:ssä.

Potilasasiakirjoissa olevat tiedot ovat arkaluonteisia ja salassa pidettäviä. Potilassuhteen luottamuksellisuus ja potilaan yksityisyyden suoja edellyttävät huolellisuutta potilasasiakirjojen käsittelyssä (mm. laatimisessa, säilyttämisessä, käyttämisessä sekä luovuttamisessa). Tiedon luovuttajan on varmistuttava erityisesti siitä, että luovutettava tieto ei joudu sivullisten käsiin.

2.2.3 Virheettömyys-, eheys- ja luotettavuusvaatimus

Hyvän hoidon, potilaan turvallisuuden ja henkilökunnan oikeusturvan takaamiseksi potilasasiakirjatietojen tulee olla oikeita, virheettömiä, ymmärrettäviä ja laajuudeltaan riittäviä. Tiedon luovuttajalla on vastuu luovutettavien tietojen virheettömyydestä (kts. HetiL 32 §). Luovutuksen saajan tulee varmistua luovutettujen tietojen alkuperästä ja muuttumattomuudesta.

Virheettömyys-, eheys- ja luotettavuusvaatimus merkitsevät mm. seuraavaa:

- Tietojen vaihtoon käytetään vain huolella kirjattuja ja vahvistettuja potilastietoja.
- Siirrettävät tiedot vahvistetaan laatijan allekirjoituksella ja toimitetaan yhtenä kokonaisuutena. Allekirjoituksen avulla voidaan varmistua tietojen alkuperästä ja muuttumattomuudesta.
- Tietojen ymmärrettävyyteen tulee panostaa mm. käyttämällä yhteisiä termejä, koodeja ja luokituksia. Tieto käytetyistä analyysimenetelmistä ja viitearvoista tulee liittää osaksi toimitettavia tietoja.

2.2.4 Käyttötarkoitussidonnaisuus

Käyttötarkoitussidonnaisuus tarkoittaa henkilötietolain mukaan, että tietoja käytetään tai luovutetaan vain samaan käyttötarkoitukseen, kuin tiedot on alunperin kerätty. Terveydenhuollossa hoitotietoja voidaan luovuttaa erityislakien perusteella myös esim. valvontaviranomaiselle. Potilaan suostumuksella tietoja voidaan luovuttaa esimerkiksi etuuksien hakemista varten toiselle viranomaiselle tai organisaatiolle (mm. Kela ja vakuutusyhtiöt). Myös sosiaalihuollon viranomaisilla on lainsäädännössä säädetty oikeus saada tietoja terveydenhuollon viranomaisilta.

Käyttötarkoitussidonnaisuuden vastaista on tietojen hoitoon liittymätön katselu.

2.2.5 Tarpeellisuusvaatimus

Potilasasiakirjoissa olevien merkintöjen on oltava potilaan hoidon kannalta tarpeellisia. Luovutuksen pyytäjän tulee pyytää vain tehtäviensä hoidon ja käyttötilanteen kannalta tarpeellisia tietoja (esim. kaikkia perustason päivittäisiä merkintöjä potilaasta ei ole tarkoitettu luovutettaviksi).

Tiedon luovuttajalla on oikeus tietää tietojen käyttötarkoitus, jonka perusteella hän rajaa luovutettavat tiedot niin, että ne ovat tarpeellisia esitettyyn käyttötarkoitukseen.

2.2.6 Yhteysvelvoite

Yhteysvelvoite merkitsee, että luovutuksen saajalla on oltava hoitosuhde tai muu asiallinen yhteys (esim. lakiin perustuva oikeus saada tiedot) potilaaseen.

2.2.7 Potilaan informointi ja velvollisuus hankkia potilaan suostumus

Henkilötietolain 24 § edellyttää potilaan informointia. Potilasta tulee informoida etukäteen luovutuksen merkityksestä niin, että hän tietää suostumuksen vapaaehtoisuuden, sekä tuntee riittävässä määrin luovutettavat tiedot, luovutuksen saajan, luovutettavien tietojen käyttötarkoituksen sekä suostumuksensa merkityksen.

Tiedon luovuttaja voi luovuttaa tietoja potilasasiakirjoista vain potilaan antamalla suostumuksella tai nimenomaisen lainsäännöksen perusteella.

2.2.8 Luovutusten seurantavelvoite

Potilasasiakirja-asetuksen mukaan (PotA 21 §) tietojen luovuttamisesta tulee tehdä merkintä potilasasiakirjoihin. Sekä tietojen luovuttajan että luovutuksen saajan on tehtävä merkinnät potilasasiakirjoihin tietojen luovutuksesta (ts. mitä tietoja, milloin, kenelle, kuka luovutti) ja luovutuksen perusteesta.

2.2.9 Potilaan tarkastusoikeusvaatimus

Potilaalla on oikeus tarkastaa, mitä tietoja hänestä on merkitty potilasasiakirjoihin. Tarkistusoikeuden käytön yhteydessä tulee informoida säännönmukaisista tietolähteistä ja tietojen luovutuksista. Henkilötietolain mukainen tarkastusoikeus ei koske luovutuksen lokitietoja.

Laissa sosiaali- ja terveydenhuollon saumattoman palveluketjun kokeilusta (811/2000 ja sen jatkolaki 1225/2003) säädetään, että potilaalla on oikeus saada tietää, kuka on käyttänyt tai kenelle on luovutettu häntä koskevia viitetietoja sekä mikä on ollut käytön tai luovutuksen peruste.

2.3 Luovutuksen hallinta

Tietoja luovuttavan rekisterinpitäjän vastuulla on varmistua edellä esitettyjen vaatimusten ja velvoitteiden toteutumisesta potilastietoja luovutettaessa. Terveydenhuollon toimintayksikön terveydenhuollosta vastaavan johtajan tulee antaa kirjalliset ohjeet potilasasiakirjoihin sisältyvien tietojen käsittelystä ja menettelytavoista (PotA 3 §).

Sähköisessä toimintaympäristössä em. vaatimusten ja velvoitteiden toteutusta varten tulee toimintayksikössä olla luovutusten hallintajärjestelmä. Hallintajärjestelmän tulee perustua huolelliseen etukäteissuunnitteluun, jolla varmistetaan tietojen lainmukainen käsittely ja osapuolten tietojärjestelmäarkkitehtuurien yhteistoiminta.

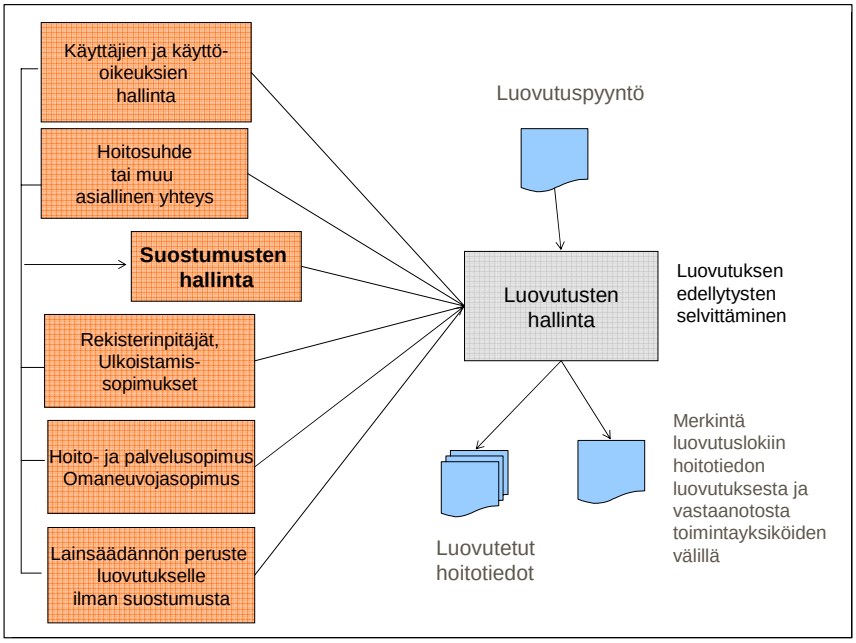
Luovutuksen hallinnan vaatimukset on tarkoituksenmukaista toteuttaa sekä organisaatio- että potilaskohtaisella tasolla:

1. Organisaatiotasolla on synnytettävä luovutusten osapuolten välille luottamussuhde. Mikäli sitä ei ennestään ole olemassa on se synnytettävä dynaamisesti. Luottamuksen synnyttämisessä voidaan käyttää joko luotettavaa kolmatta osapuolta tai luottamus perustuu osapuolten keskinäisiin neuvotteluihin ja tietoturvapoliitikkoihin. Tietojen käsittely suunnitellaan ja otetaan käyttöön luottamuksen synnyttämisen toteuttavat toiminnalliset ja tekniset ja ratkaisut.

   Luottamuksen peruslähtökohta on, että osapuolet tuntevat toistensa tietoturvapolitiikan ja voivat luottaa siihen, että kumpikin osapuoli käsittelee potilastietoja velvoitteiden ja vaatimusten mukaisesti ja että tiedonsiirto tapahtuu turvallisesti.

2. Potilaskohtaisella tasolla tietojen luovuttajan tulee varmistua sekä yhteys-, tarpeellisuus-, käyttötarkoitus- ja informointivaatimusten toteutumisesta että suostumuksen olemassaolosta (mikäli se tarvitaan) ennen kyseisen potilaan tietojen luovuttamista. Tätä varten luovutuksen pyytäjän on pystyttävä osoittamaan lainmukainen luovutusperuste ja esitettävä riittävät ja luotettavat perusteet luovutuksen edellytysten voimassaolosta.

Luovutuksen ja suostumuksen hallintaa tulee kehittää kokonaisuutena. Etukäteen tapahtuva suunnittelu ja tietovirtojen analysointi on tehtävä luovutusten ja suostumusten hallinnan toteuttamista suunniteltaessa. Kuva 3 esittää tässä kokonaisuudessa huomioon otettavia seikkoja.



Kuva 3 Luovutuksen ja suostumuksen hallinnan kokonaisuus (Lähde: Suostumusraportti)

2.4 Tietojen luovutustavat

Tietojen luovutus tapahtuu seuraavilla perustavoilla:

- *Luovutuspyynnön perusteella tapahtuva luovutus*
- *Luovuttajan aloitteesta ilman tiedon vastaanottajan pyyntöä tapahtuva luovutus*

Monimutkaisemmat luovutustilanteet ovat näiden kahden perustavan yhdistelmiä.

Luovutuksen perusteena voi olla potilaan antama kirjallinen, suullinen tai asiayhteydestä muutoin ilmenevä suostumus, hänen kanssaan tehty sopimus tai laissa mainittu sellainen peruste, joka ei vaadi potilaan antamaa suostumusta.

Esimerkkejä suostumuksen perusteella tapahtuvasta luovutuksesta ovat:

- lähetteen käsittelyn yhteydessä tarvittavien lisätietojen lähettäminen
- hoitopalautteen lähettäminen
- sähköisen reseptin lähettäminen apteekkiin
- potilaasta kerättyjen hoitotietojen käsittely (esim. katsominen selaimella) viitetietojen tai muun vastaavan tietoteknisen ratkaisun avulla toisen toimintayksikön tietojärjestelmästä
- potilaan palveluketjusuunnitelman toteutus viitetietoja käyttävän aluetietojärjestelmän palvelujen avulla

Esimerkkejä tilanteesta, jossa luovutus ei vaadi suostumusta:

- Ostopalvelu merkitsee toimeksiantosuhdetta. Ostopalvelutietojen tuottamiseen tarvittavan tiedon luovuttaminen sekä ostopalveluiden tuloksena syntyvien tietojen luovuttaminen tilaajalle ei vaadi yleensä potilaan suostumusta. On kuitenkin syytä

huomata, että ostopalvelujen asema riippuu siitä kenen lukuun palvelu tehdään. Ostopalvelua voidaankin tarkastella yhtenä rekisterinpidon erityistilanteena
- Kiireelliseen ensihoitoon liittyvät tietojen luovutustilanteet, joissa on kyseessä potilaan hengenvaara (ns. pakkotilanteet).
- Potilaslain 13 §:ssä säädetyt muut perusteet

Suostumusta ja suostumuksen hyviä käytäntöjä on käsitelty yksityiskohtaisemmin raportissa Tietoturvallinen kommunikaatioalusta: Suositukset sähköisen suostumuksen periaatteiksi, Osaavien keskusten verkosto 3/2004.

3. Luovutukseen liittyvät käsitteet ja asiakirjat

Terveydenhuollossa käytetään vakiintunutta henkilötietolain mukaista termiä '**tietojen luovutus**' silloin, kun puhutaan hoitotietojen luovutuksesta kahden tai useamman rekisterinpitäjän välillä. Toimintayksikössä tapahtuva **tietojen käyttö** ei ole luovutusta (ks. 1.4.1).

Käytännössä voi samaan hallinnolliseen toimintayksikköön kuulua useita eri rekisterinpitäjiä (esim. terveyskeskus voi toimia samalla kertaa sekä julkisen terveydenhuollon toimintayksikkönä että työterveyshuollon toimintayksikkönä). Samalla toimintayksiköllä voi myös olla eri käyttötarkoituksiin muodostettuja henkilörekistereitä. Eri rekisterit on pidettävä erillään ja niiden välinen tiedon vaihto on luovutusta.

Luovutusprosessiin liittyviä keskeisiä käsitteitä ovat luovutuksen pyytäjä, tietojen luovuttaja ja vastaanottaja, luovutuspyyntö, luovutuksen peruste, tietojen käyttötarkoitus ja luovutettavat tiedot.

Tämän raportin käsittelemissä tilanteissa, luovutuspyyntö ja luovutus tapahtuu joko kahden rekisterinpitäjän välillä tai rekisterinpitäjän ja sellaisen organisaation kesken, jolla on laista johtuva oikeus tietojen saantiin. Tietojen luovutuksen perusteena voi olla potilaan antama suostumus tai muu laissa määritelty peruste. Potilaan nimenomaisella suostumuksella voidaan tietoja luovuttaa myös hänen nimeämälleen muulle organisaatiolle (rekisterinpitäjälle) tai henkilölle ottaen huomioon henkilötietolain käyttötarkoitussidonnaisuus.

3.1 Luovutuspyyntö ja luovutus

Luovutuksen käsitteet ja tietosisältö noudattavat aiemmin mainitun suostumusraportin määrityksiä. Käsitteiden määrittelyssä on painotettu sähköistä toimintaympäristöä.

Luovutuspyyntö on

- sähköisessä toimintaympäristössä dokumentti mahdollisine liitteineen (esim. suostumus), joka toimitetaan sille rekisterinpitäjälle, jolta tietoja pyydetään luovutettavaksi.

Luovutuspyynnön ja luovutuksen yksilöivä tunniste

- Luovutuspyyntö ja luovutettavat asiakirjat on tarpeen yksilöidä yksikäsitteisesti niin, että ne voidaan myöhemmin tunnistaa ja niihin voidaan tarvittaessa viitata. Luovutuspyyntö ja luovutusasiakirja yksilöidään tietojärjestelmissä OID-tunnuksen (liite D) avulla, jonka tietojärjestelmän tulee antaa automaattisesti.

Luovutuksen pyytäjä on

- Terveydenhuollon ammattihenkilö tai itsenäinen ammatinharjoittaja, jolla on työtehtäviensä johdosta oikeus pyytää tietojen luovutusta. Luovutuksen pyytäjällä tulee olla hoitosuhde tai muu asiallinen yhteys potilaaseen. Luovutuksen pyytäjä tunnistetaan nimellä ja henkilötunnuksella. Luovutuspyyntöön on lisäksi syytä merkitä hänen työtehtävänsä kyseisessä organisaatiossa.

- Luovutuksen pyytäjä voi olla myös viranomainen, muu organisaatio tai henkilö, jolla on lainmukainen oikeus hoitotietojen saamiseen. Organisaation tulee määritellä ne vastuuhenkilöt, joilla on oikeus pyytää luovutusta organisaation puolesta.

Potilas/Asiakas on

- Henkilö, jonka hoitotietojen luovuttamisesta on kysymys.

Hoitotiedon luovuttaja on

- Terveydenhuollon toimintayksikkö tai itsenäinen ammatinharjoittaja, joka on luovutettavaksi pyydettyjen hoitotietojen rekisterinpitäjä.

Luovutuksen saaja/Luovutuksen vastaanottaja on

- Terveydenhuollon toimintayksikkö tai itsenäinen ammatinharjoittaja, jolle potilaan hoitotietoja luovutetaan. Luovutuksen vastaanottaja on tavallisesti se toimintayksikkö, joka hoitaa potilaan ongelmaa ja jossa työskentelevä ammattihenkilö tietoja pyytää. Koska hoidosta vastaava toimintayksikkö päättää, ketkä sen henkilökunnasta osallistuvat hoidon antamiseen (ja ketkä ovat sivullisia) ei luovutuksen saajan sisällä tapahtuvaa tiedonkäsittelyä koskevia rajauksia voi tässä yhteydessä tehdä. Toimintayksikön sisällä tietojen käytön rajaukset tapahtuvat yksikön oman käyttäjänhallinnan avulla.
- Hoitopalautteen lähettämisen yhteydessä erikoissairaanhoidon ammattihenkilö pyytää potilaalta suostumuksen hoitopalautteen lähettämiseen potilaan lähetteen laatineeseen toimintayksikköön, joka on siis luovutuksen saaja (poikkeukset kts. PotL 13.3).
- Luovutuksen vastaanottaja voi ilman potilaan suostumusta olla myös viranomainen, organisaatio tai henkilö, jolla on lainmukainen oikeus hoitotietojen saamiseen. Tällöin luovutuksen saamisoikeuden rajaukset liittyvät luovutuksen saajan lainmukaiseen asemaan taikka tehtävään.

Luovutettavat hoitotiedot ovat

- Ne jäljempänä selvitetyin tavoin rajatut hoitotiedot, joita luovuttaja luovuttaa luovutuspyynnön ja mahdollisen suostumuksen, sopimuksen tai laista johtuvan muun syyn perusteella.
- Luovutettavia tietoja on mahdollista rajata käyttötarkoituksen mukaisesti. Rajauksen tekijöitä voivat olla mm. potilas ja joissain tapauksissa myös tiedon luovuttaja. Potilaskertomuksen tietorakenteiden tulee tukea rajauksia.
- Luovutuspyynnössä on mahdollista tarkentaa/rajata luovuttajaa koskevia tietoja, esimerkiksi toimintayksikön tietty toimipaikka tai tietty potilasrekisteri. Rekisteri tulee aina yksilöidä (esim. työterveyshuollon rekisteri tai "tavallinen" potilasrekisteri).
- Yksittäistä irrallista tietoa ei tulisi pyytää eikä luovuttaa. Tällaisen tiedon luovuttaminen voi olla lain vastaista, koska se voi loukata vaatimusta tiedon eheydestä ja asiakirjojen muuttamiskieltoa. Tarvittaessa voidaan luovuttaa asiakirjan osa (esimerkiksi vakuutusyhtiölle). Tällöin luovutuksesta on käytävä selville, että kyseessä ei ole kokonainen asiakirja

Luovutettaville hoitotiedoille on tarpeellista kehittään luokitus, mikä helpottaa sekä potilaan informointia että luovutettavien hoitotietojen valintaa (kuten myös potilaan mahdollisesti tekemiä rajauksia).

Asiayhteys

- Asiayhteys on se hoito-/palvelukokonaisuus, jonka piirissä potilas on. Se on myös rajausperuste tietojen luovuttamisessa. Hoitokokonaisuus on esimerkiksi vuodeosastohoitojakso tai päivystyskäynti. Jotta asiayhteyttä voitaisiin käsitellä tietojärjestelmissä, on sitä varten tarpeen laatia luokittelu. Asiayhteyttä on käsitelty tarkemmin suostumusraportissa. Laadittavan luokituksen lähtökohtana voidaan käyttää suostumusraportissa olevaa alustavaa luetteloa asiayhteyksistä.

Tietojen käyttötarkoitus

- Käyttötarkoitus, johon tietoa voidaan henkilölain ja potilaslain mukaan käyttää. On huomattava, että eri rekisterit on perustettu alun perin eri käyttötarkoituksiin. Suostumusraportissa on käsitelty käyttötarkoitusta yksityiskohtaisemmin.

Luovutuksen peruste

- Luovutuksen perustuessa potilaan antamaan suostumukseen on tämä kirjallinen, suullinen tai asiayhteydestä ilmenevä suostumus luovutuksen peruste. Sähköisessä luovutusprosessissa luovutuspyynnössä viitataan potilaan antamaan suostumukseen (ts. suostumusasiakirjaan) sen yksilöintitunnuksella. Mikäli suostumus on suullinen tai asiayhteydestä ilmenevä, tulee se ilmetä luovutuspyynnöstä ja olla luovutuksen pyytäjän varmentama.
- Luovutuksen perustuessa potilaan kanssa tehtyyn kokeilulain mukaiseen sopimukseen viitataan luovutuspyynnössä sopimusasiakirjaan (esimerkiksi kokeilulaissa määritelty omaneuvojasopimus) sen yksilöintitunnuksella.
- Luovutuksen perustuessa suostumuksen sijasta laissa määrättyihin muihin tilanteisiin tulee lainkohta (peruste) yksilöidä.
- Luovutuksen perustuessa pelkästään toimintayksiköiden väliseen osto- tai toimeksiantosopimukseen viitataan luovutuspyynnössä kyseiseen sopimusasiakirjaan sen yksilöintitunnuksella. Nämä asiakirjat tulee arkistoida asianmukaisesti
- Tietojärjestelmiä varten on tarkoituksenmukaista tehdä luovutuksen perusteista luokittelu.

Luovutuspyynnön/luovutuksen ajankohta

- Aika/aikaleima, jolloin luovutuspyyntö ja luovutus on tehty.

Luovutuspyynnön allekirjoitus

Luovutuspyyntö koostuu metatiedoista (ns. luovutuspyynnön kuvailutiedot) ja mahdollisista liitteistä (esim. suostumusdokumentti). Allekirjoituksella varmistetaan luovutuspyynnön aitous, alkuperä, muuttumattomuus ja oikeudellinen sitovuus. Sähköisesti tehdyssä luovutuspyynnössä tulee käyttää sähköistä allekirjoitusta.

- Allekirjoitus on sen henkilön tekemä, jolle toimintayksikkö on valtuuttanut tekemään luovutuspyyntöjä (tavallisesti terveydenhuollon ammattihenkilö).
- Luovutuspyynnön muuttumattomuus voidaan varmistaa myös kokeilulaissa mainitulla organisaatioallekirjoituksella. Tietoteknisesti voidaan luovutuspyyntö liitteineen tallettaa sähköiseen kirjekuoreen, joka ”suljetaan” em. organisaatioallekirjoituksella (ks. kokeilulaki 2003/1225, liite C).

Luovutuksen allekirjoitus

Allekirjoituksella varmistetaan luovutettavien tietojen aitous, alkuperä ja muuttumattomuus sekä oikeudellinen sitovuus. Allekirjoitus varmistaa tietojen siirtymisen muuttumattomina luovuttajalta luovutuksen saajalle. Varsinaisen hoitotiedon alkuperän varmistamiseksi tarvitaan tiedon merkitsijän allekirjoitus, joka voi sisältyä luovutettavaan tietosisältöön.

Sähköisessä toimintaympäristössä tietojen luovutuksella tarkoitetaan (asiakirja) kokonaisuutta, joka koostuu luovutettavista tiedoista ja luovutuksen kuvailutiedoista (ms. metatiedoista).

- Allekirjoitus on terveydenhuollon ammattihenkilön tekemä. Allekirjoittaja voi olla myös muukin kuin terveydenhuollon ammattilainen, jos toimintayksikkö (tai organisaatio) on valtuuttanut hänelle tämän tehtävän.
- Sähköisesti tapahtuvassa luovutuksessa tulee käyttää sähköistä allekirjoitusta. Luovutettavien tietojen ja kuvailutietojen muuttumattomuus voidaan varmistaa myös kokeilulain mukaisella organisaatioallekirjoituksella. Tietoteknisesti voidaan luovutussanoma liitteineen tallettaa sähköiseen kirjekuoreen, joka ”suljetaan” organisaatioallekirjoituksella (kts. kokeilulaki 2003/1225, liite C).

3.2 Suostumus

Luovutuksen perusteena on aina ensisijaisesti potilaan antama suostumus. Sen on kirjallisessa muodossaan suostumusasiakirja, johon on liitetty yksilöintitunnus. Suostumuksen täsmällinen sisältö sekä suostumuksen pyytäminen on kuvattu suostumusraportissa (OSVE 2/2004).

Sähköisessä toimintaympäristössä luovutuspyyntö ja suostumus muodostavat kokonaisuuden ja siksi jäljempänä määritellyissä luovutuspyynnön kuvailutiedoissa tulee olla viittaus (viite/linkki) kyseiseen luovutukseen liittyvään suostumukseen.

Kokeilulaissa mainittuun omaneuvojasopimukseen sisältyy asiakaan antama kirjallinen suostumus, jonka perusteella omaneuvojalla on oikeus saada tehtävänsä suorittamiseksi koskevia tietoja. Lain mukaan "Kun asiakas on valinnut omaneuvojan, laaditaan omaneuvojapalvelun toteuttamisesta kirjallinen sopimus, jonka asiakas ja omaneuvoja allekirjoittavat".

3.3 Potilasasiakirjoihin tehtävät merkinnät luovutuksesta, Lokitiedot

Luovutuspyynnöstä ja luovutuksesta tehdään merkinnät potilasasiakirjoihin (kts. PotA 10 § ja PotA 21 §). Potilasasiakirjoissa tulee olla luovuttamista koskevat potilaan suostumukset. Tietojen vastaanottajan tulee viedä vastaanottamansa tiedot potilasasiakirjoihinsa (PotA 10 §). Tietojen alkuperä on tällöin myös merkittävä.

Tässä raportissa suositellaan, että sähköisessä luovutuksessa tieto luovutuksesta merkitään aina luovutuslokiin. Tarvittavat merkinnät on kuvattu jäljempänä tässä raportissa. Luovutettua dataa ei ole syytä viedä lokitietoihin.

3.4 Toimintayksikkö ja toimipaikka

3.4.1 Toimintayksikkö eli rekisterinpitäjä

Rekisterinpitäjä vastaa potilastietojen tallettamista sekä luovuttamista koskevien vaatimusten ja velvoitteiden täyttymisestä. Henkilötietolain ja potilaslain mukaan potilastietoja hallinnoiva toimintayksikkö on rekisterinpitäjä. Terveydenhuollon toimintayksiköt on määritelty potilaslaissa (PotL 2 §). Sen mukaan mm.

- terveyskeskus
- erikoissairaanhoitolaissa tarkoitettu sairaala tai siitä erillään oleva sairaanhoidon toimintayksikkö
- sairaanhoitopiirin kuntayhtymän päättämä hoitovastuussa oleva kokonaisuus
- yksityinen terveydenhuollon palveluja tuottava yksikkö
- työterveyslaitos sen tuottamien terveyden- ja sairaanhoidon palvelujen osalta
- valtion mielisairaala
- puolustusvoimain sairaanhoitolaitos
- vankilamielisairaala

ovat terveydenhuollon toimintayksiköitä.

Käytäntöön on vakiintunut toimintayksiköiden nimiksi potilaslain määrittelyistä hieman poikkeavia nimiä kuten

- yksityinen terveydenhuollon ammatinharjoittaja lääkäriasemalla tai erillisellä vastaanotolla
- lääkäriasema
- kansanterveystyön kuntayhtymän toimintayksikkö
- työterveyshuollon toimintayksikkö
- erikoissairaanhoidon kuntayhtymän toimintayksikkö (jossa voi sen päätöksellä olla yksi tai useampia toimintayksiköitä)
- terveyskeskus

3.4.2 Toimintayksikön toimipaikat

Toimintayksikköön kuuluu käytännössä useampia toimipaikkoja. Toimintayksikön ja sen toimipaikkojen välillä esiintyy mm. seuraavia rakenteita:

- Lääkäriasemalla voi olla toimipaikkoja usealla paikkakunnalla.
- Yksityinen ammatinharjoittaja voi toimia usealla paikkakunnalla eri toimipaikoissa.
- Kansanterveystyön kuntayhtymän toimintayksiöllä voi olla useita terveysasemia ja sairaaloita.
- Työterveyshuollon toimintayksiköllä voi olla toimipaikkoja usealla eri paikkakunnalla.
- Erikoissairaanhoidon kuntayhtymän toimintayksiköllä voi olla useita toimipaikkoja. Sillä voi olla myös diagnostisen tiedon tuottamiseen ja näytteiden ottamiseen tarkoitettuja toimipaikkoja.
- Erityishuoltopiirin kuntayhtymän toimintayksiköllä voi olla useita toimipaikkoja
- Kunnan sosiaalilautakunnan alaisilla virastoilla ja laitoksilla voi olla useita toimipaikkoja.

3.4.3 Toimipaikkojen ominaisuuksia

Toimipaikkaan liittyy mm. seuraavia ominaisuuksia

- Toimipaikalla on käyntiosoite.
- Samassa osoitteessa voi olla useiden toimintayksiköiden toimipaikkoja. Esimerkiksi lääkäriasemalla voi olla yksityisvastaanotto sekä työterveydenhuollon vastaanotto.
- Terveyskeskus voi tarjota samassa toimipaikassa sekä julkista terveydenhuoltoa että yksityistä työterveyshuoltoa.

Osana kansallista terveysprojektia tullaan toimipaikoille antamaan sähköinen asiointiosoite, jotka on saatavissa mm. Stakesin koodistopalvelimelta (liite B).

Potilas asioi yhdessä tai useammassa toimintayksikön toimipaikassa. Niinpä potilas varaa ajan tai menee käymään terveyskeskuksen tietyllä toimipaikalla ilman, että hän välttämättä tietää, mihinkä hallinnolliseen toimintayksikköön kyseinen toimintapaikka kuuluu. Potilas myös yleensä muistaa helpoiten sen, missä toimipaikoissa hän on asioinut.

Suostumusta hankittaessa ja luovutuspyyntöä laadittaessa tulee toimipaikan ja siihen kuuluvan toimintayksikön yhteys olla helposti selvitettävissä. Sähköisessä luovutusprosessissa tulee käytetyn tietojärjestelmän pystyä päättelemään oikea toimintayksikkö myös silloin kun käytetään toimipaikan nimiä. Tämä merkitsee käytännössä sitä, että kullakin toimintayksiköllä tulee olla luettelo siihen kuuluvista toimipaikoista. Tätä luetteloa voidaan käyttää päättelemään toimintayksikkö, kun toimipaikka tunnetaan.

3.5 Saman toimintapaikan erilliset rekisterit

Käytännössä esiintyy tilanteita, että yhdessä toimipaikassa on usean eri lainsäädännön piirin kuuluvan rekisterinpitäjän toimintaa (esimerkiksi julkista terveydenhuoltoa ja työterveyshuoltoa). Tällöin sekä eri rekisterinpitäjien että saman rekisterinpitäjän eri käyttötarkoituksiin pidettävät tiedot on pidettävä erillään, kuten myös eri käyttötarkoitukseen pidettävät rekisterit.

Esimerkiksi seuraavilla terveydenhuollon tiedoilla on sekä eri rekisterinpitäjä että eri käyttötarkoitus:

- julkisen terveydenhuollon tiedot
- työterveydenhuollon tiedot

Sosiaalitoimen eri tehtävissä muodostuu erilliset henkilörekisterit, joilla on eri käyttötarkoitus, esimerkiksi: (Lähde: Tietosuojavaltuutetun toimiston ohje).

- lasten päivähoidon rekisteri
- kotipalvelun rekisteri
- vanhustenhuollon rekisteri
- toimeentulotuen rekisteri
- lastensuojelun rekisteri
- päihdehuollon rekisteri
- perheasiain sovittelun rekisteri
- vammaispalvelun rekisteri
- kehitysvammahuollon rekisteri
- lapsen huolto- ja tapaamisoikeuden rekisteri

- isyyden selvittämisen rekisteri
- lapsen elatuksen rekisteri
- kasvatus- ja perheneuvonnan rekisteri
- muut mahdolliset henkilörekisterit

On huomattavat, etteivät hallinnolliset järjestelyt muuta rekisterinpidon perusteita (esimerkkinä sosiaali- ja terveyslautakuntien yhdistäminen).

4. Luovutuspyynnön ja tietojen luovutuksen prosessikuvaus

Terveydenhuollossa on eri käyttötarkoituksiin perustettuja henkilörekistereitä (esimerkiksi terveyskeskuksen asiakastietojärjestelmä voi käsittää sekä julkisen terveydenhuollon potilasrekisterin että työnantajakohtaisen työterveydenhuollon rekisterin). *Eri käyttötarkoitukseen perustettujen rekistereiden välillä ei saa luovuttaa tietoja muutoin kuin potilaan asianmukaisella suostumuksella tai jos siitä on erikseen lailla säädetty*.

Tässä raportissa esitetyt prosessikuvaukset ja mallit käsittelevät eri rekisterinpitäjien/eri käyttötarkoituksiin perustettujen rekistereiden välistä tietojen luovutusta erityisesti sähköisen toimintaympäristön kannalta. On tärkeää huomata, että tietojärjestelmä (esimerkiksi terveyskeskuksen asiakastietojärjestelmä) ja henkilörekisteri eivät aina ole yhteneviä käsitteitä. Sillä sijaitsevatko ne mahdollisesti samassa teknisessä tietojärjestelmässä ei ole luovutusperiaatteiden kannalta merkitystä.

4.1 Yleistä

Perustilanteessa terveydenhuollon ammattihenkilö tarvitsee luonaan olevasta potilaasta tietoa, joka on talletettu toisen toimintayksikön potilasrekisteriin. Potilas antaa suostumuksensa kyseisten tietojen luovutukseen. Ammattihenkilö lähettää luovutuspyynnön ja luovutusta koskevan suostumuksen toiselle toimintayksikölle, joka vastaa luovuttamalla pyydetyt tiedot (esimerkiksi potilaskertomustiedot tai sen ydintiedot).

Terveydenhuollon ammattihenkilö voi tehdä luovutuspyynnön myös tilanteessa, jossa potilas ei ole läsnä. Luovutuspyyntö perustuu tällöin joko laista johtuvaan oikeuteen saada tiedot (esim. PotL 8 §), potilaan voimassa olevaan kyseistä käyttötarkoitusta koskevaan suostumukseen tai kokeilulaissa määriteltyyn omaneuvojasopimukseen.

Luovutuksen peruste tulee ilmetä luovutuspyynnön kuvailutiedoista. Mikäli luovutus perustuu suostumukseen tai sopimukseen, luovuttajan tulee voida todentaa niiden olemassaolo. Luovutuspyynnön perusteena voi olla suostumuksen sijasta laissa määrätty muu peruste (esimerkiksi lääninlääkäri pyytää kantelun ratkaisemiseksi lääkäriltä lisätietoja).

Ns. *yleistä kyselyä*, jossa luovutuksen pyytäjä tekee kyselyn, mitä tietoa potilaasta on mahdollisesti talletettu kyselyn kohteena olevaan rekisteriin, *ei voida tehdä*. Jo potilaan tietojen sijaitseminen potilasrekisterissä on salassa pidettävä tieto ja sen luovuttaminen vaatii potilaan suostumuksen.

Sähköiseen luovutusprosessiin liittyvät seuraavat asiakirjat: luovutuspyyntö, (mahdollinen) suostumus, luovutuksen kuvailutiedot ja luovutetut tiedot.

4.2 Yleiset vaatimukset sähköiselle luovutusprosessille

4.2.1 Huolellisuus- ja suojausvelvoite

Huolellisuus- ja suojausvelvoitetta on yleisellä tasolla käsitelty luvussa 2.2.2. Näiden periaatteiden "jalkauttaminen" sähköiseen luovutusprosessiin merkitsee mm. seuraavaa:

- Tietojen vaihtoon osallistuvien tietojärjestelmien käyttö on sallittu ainoastaan sellaisille käyttäjille, joilla on asianmukaiset käyttöoikeudet järjestelmien toimintoihin ja tietoihin.
- Käyttäjät tunnistetaan ja todennetaan riittävän vahvasti.
- Käyttäjien toimintaa valvotaan riittävän yksityiskohtaisilla lokitiedoilla.
- Tietoliikenteen suojaukseen ja salaukseen on kiinnitetty riittävää huomiota niin, että tietojen vuotaminen ulkopuolisille tai tietojen muuttuminen siirron aikana on estetty.
- Tietojenvaihtoon osallistuvat osapuolet ovat tutustuneet toistensa tietoturvapolitiikkaan ja sen käytännön järjestelyihin ja vakuuttuneet tietoturvan riittävästä tasosta ja tehneet asianmukaiset tietojen luovuttamissopimukset.
- Tuntemattomien tietojen luovuttajien tai luovutuspyyntöjen tekijöiden kanssa ei asioida, vaan ensin varmistutaan siitä, kenestä on kysymys ja voidaanko tietojen vaihtoa yleensä tehdä hyväksyttävällä turvatasolla.

4.2.2 Virheettömyys-, eheys- ja luotettavuusvaatimus

Virheettömyys-, eheys- ja luotettavuusvaatimuksia on käsitelty yleisellä tasolla luvussa 2.2.3. Sähköisessä luovutusprosessissa tulee:

- Tietojen luovuttajan varmistaa, että luovutettavat tiedot ovat virheettömiä
- Tietojen luovuttajan varmistaa, että oikean potilaan tiedot noudetaan potilasrekisteristä ja että etteivät tiedot poiminnan aikana muutu.
- Todennetaan luovutusta pyytävä ja luovuttava toimintayksikkö (esim. PKI-järjestelmän palvelujen avulla).
- Huolehtia, että siirrettävät tiedot (kuvailutiedot ja data) vahvistetaan sähköisellä allekirjoituksella ja että ne toimitetaan yhtenä kokonaisuutena esimerkiksi sähköisessä kirjekuoressa. Huolehditaan siitä, että kuvailutiedot ja siirrettävä data pysyvät yhtenäisenä kokonaisuutena. Sähköisellä allekirjoituksella avulla voidaan varmistua tietojen alkuperästä.

4.2.3 Tarpeellisuusvaatimus

Tarpeellisuusvaatimus merkitsee sähköisessä luovutusjärjestelmässä mm. seuraavaa:

- Luovutuksen vastaanottajan tietojärjestelmä varmistaa, että sen käyttäjät saavat järjestelmältä käyttöoikeuden vain työtehtäviensä hoidon kannalta tarpeellisiin tietoihin.
- Luovutuksen vastaanottajan käyttöoikeuksien hallinnan tietojärjestelmä varmistaa sen, että luovutettuja tietoja voivat käyttää vain ne ammattihenkilöt, joilla on työtehtäviensä johdosta siihen oikeus. Tämän periaatteen käytännön toteutus edellyttää kehittämistyötä, koska vielä ei ole olemassa vakiintunutta standardia luokitella siirrettäviä tietoja käyttöoikeuksien ja työtehtävien perusteella.

4.2.4 Yhteysvelvoite

Luovutuksen pyytäjän tietojärjestelmän tulee kyetä hallinnoimaan potilaan hoitosuhdetta tai asiayhteyttä organisaation tietoturvapolitiikan mukaisesti.

Luovuttajalla ei ole käytännössä mahdollisuuksia todentaa erikseen jokaisessa luovutustilanteessa hoitosuhteen tai muun asiayhteyden olemassaoloa, vaan se joutuu luottamaan luovutuksen pyytäjään. Luottamus voidaan synnyttää esimerkiksi siten, että luovuttaja auditoi luovutuksen pyytäjän tietoturvapolitiikan ja luovutuksen hallinnan tietojärjes-

telmän. Perusvaatimus on, että sekä luovutuksen pyytäjän ja luovuttajan tietoturvapolitiikoiden että niiden toteutuksen tulee täyttää lakien, asetusten, määräysten ja tämän ohjeistuksien vaatimukset. Minimissään tulee luovutuksen pyytäjän ja luovuttajan tietoturvapolitiikoiden olla saman tasoisia. Vaihtoehtoisesti voidaan käyttää auditointiin (tai sertifiointiin) luotettua kolmatta osapuolta. Luotettu kolmas osapuoli voi olla valtakunnallinen palvelu, josta luovuttaja voi tarkistaa keihin se voi luottaa.

4.2.5 Potilaan informointi

Informoinnissa tulee noudattaa henkilötietolain 24 §:n määräyksiä. Potilasta tulee antaa sekä yleistä, että asiakaskohtaista informoida siitä miksi, kenelle ja miten rekisterinpitäjä tietoja luovuttaa. Tämä informaatio on syytä tehdä suostumuksesta annettavan yleisen informaation yhteydessä (ks. suostumusraportti).

4.2.6 Luovutusten seurantavelvoite

Tietojen luovuttajan ja luovutuksen saajan on tehtävä merkinnät potilasasiakirjoihin tietojen luovutuksesta (mm. mitä tietoja, milloin, kenelle, mihin käyttötarkoituksen ja kuka luovutti) ja luovutuksen perusteesta. Sähköisessä toimintaympäristössä tästä tehtävästä huolehtii joko luovutuksen hallintajärjestelmä tai sähköinen arkistojärjestelmä. Lisäksi luovutusprosessista kirjautuu tietoja luovutuslokiin.

4.3 Tietojen sähköisen luovuttamisen mallitapaukset

Kuten luvussa 2.5 todettiin, tietojen luovutusta on kahta perustapaa:

- Luovutuspyynnön perusteella tapahtuva luovutus
- Luovuttajan aloitteesta ilman tiedon saajan pyyntöä tapahtuva luovutus

Seuraavassa käsitellään yksityiskohtaisesti kumpaakin tapausta.

Luovutuksen pyytäjällä tulee olla toimintayksikön antamat oikeudet laatia luovutuspyyntö. Vastaavasti luovutuspyynnön käsittelijä on luovuttavan toimintayksikön nimeämä henkilö (henkilötietolain kannalta rekisterinpitäjän edustaja), jolla on oikeus tehdä potilastietojen luovutuspäätös. Potilastietojärjestelmissä näitä oikeuksia ylläpitää tavallisesti käyttöoikeuksien hallinnan tietojärjestelmä.

Luovutuspyynnön tekninen tekijä on sähköisessä ympäristössä luovutusten hallinnan tietojärjestelmä. Vastaavasti luovutuspyynnön tekninen vastaanottaja on luovutusten hallinnan tietojärjestelmä. Luovutuksen teknisenä tekijänä on luovuttavan toimintayksikön tietojärjestelmä**.**

Tulevaisuudessa voi luovutuksen hallinnan tietojärjestelmä luovutussääntöihin perustuen toimia tietojen luovuttajana.

Luovutettavat tiedot valitaan luovutuspyynnössä ja sen liitteissä esitettyjen tietojen perusteella hyödyntäen niissä olevia määrityksiä ja luokituksia.

Luovutuspyynnön sisältämät tiedot tulee olla rakenteistettu siten, että luovutuksen tekijän luovutuksen hallinnan ohjelmisto pystyy varmistumaan luovutuksen edellytysten olemassaolosta ja tekemään teknisen luovutuksen. Vastaavasti luovuttavat tiedot tulee

olla rakenteistettu siten, että luovutuksen saajan ohjelmisto pystyy varmistumaan luovutuksen aitoudesta ja käsittelemään vastaanotetut tiedot.

4.3.1 Tietojen luovuttaminen luovutuspyyntöön pohjautuen

Tässä tapauksessa luovutuksen peruste on joko potilaan antama suostumus, sopimus tai se on muu laista johtuva peruste.

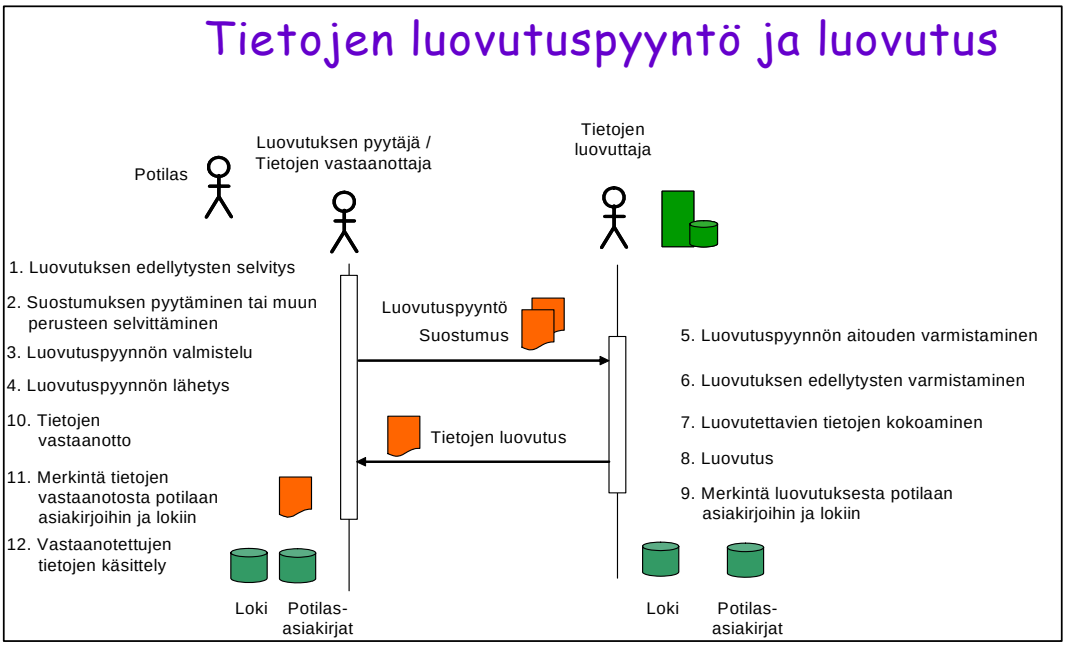
Luovutuspyyntö muodostuu:

1. Luovutuspyynnön kuvailutiedoista (metatiedoista)
2. Suostumusdokumentista (jos suostumus tarvitaan)

Luovutussanoma muodostuu:

1. Luovutuksen kuvailutiedoista (metatiedoista)
2. Luovutettavista tiedoista

Oheinen kuva 4 esittää pelkistetysti luovutuspyynnön ja luovutuksen työnkulkua eri osapuolten välillä kun tietojen luovuttamisen peruste on luovutuspyyntö.



Kuva 4 Tietojen luovutuspyyntö ja luovutus

Seuraavassa on kuvattu yksityiskohtaisella tarkkuudella luovutuspyynnön, luovutuksen ja luovutettujen tietojen vastaanoton tehtävät kuvan 4 mukaisesti. Tehtävien toteuttaminen voi jakaantua tietojärjestelmän ja ohjelmiston käyttäjän kesken. Käytännössä tietojärjestelmä tekee hyvin suuren osan tehtävistä. Se mm. täyttää pääosan suostumukseen ja luovutuspyyntöön tarvittavista tiedoista dokumentteihin automaattisesti.

Luovutuspyyntö ja tietojen luovutus sisältävät seuraavat tehtävät:

	Luovutuspyynnön ja luovutuksen tehtävät		
Nro	**Tekijä**	**Tehtävä**	**Selityksiä**
1	Luovutuksen pyytäjä	Luovutuksen pyytäjä perustelee hoitosuhteen tai muun asiallisen yhteyden potilaaseen	Luovutuspyynnön edellytyksenä on pyytäjän ja potilaan välillä oleva hoitosuhde, muu asiallinen yhteys tai muu laista johtuva peruste. Luovutuksen pyytäjän tietojärjestelmän tulisi kyetä osoittaman tämä.
2	Luovutuksen pyytäjä	Mikäli suostumus tarvitaan: Luovutuksen pyytäjä laatii potilaan kanssa suostumuksen tietojen luovuttamiseksi tai käyttää voimassaolevaa suostumusta.	Potilas voi antaa suostumuksen voimassaolon pidemmäksi ajaksi (esim. tietyn sairauden hoitamiseksi), jolloin luovutuksen pyytäjä voi pyytää suostumuksen kohteena olevia tietoja samaan käyttötarkoitukseen myöhemminkin. Suostumusta ei voi antaa määräämättömäksi ajaksi (kts. suostumusraportti) Olemassa olevan suostumuksen käyttäminen on mahdollista vain suostumuksen saajalle edellytyksellä, että suostumuksessa mainittu asiayhteys ja käyttötarkoitus vastaavat luovutuspyynnön ongelmaa ja käyttötilannetta. Muussa tapauksessa on potilaan annettava uusi suostumus. Suostumus on yksi luovutuksen perusteista ja se merkitään luovutuspyynnön otsikkotietoihin. Tulee ilmetä onko kyseessä: - Kirjallinen suostumus. Tällöin tarvitaan myös viite suostumusdokumenttiin. - Potilaslain määrittelemissä tilanteissa annettu suullinen suostumus - Potilaslain määrittelemissä tilanteissa annettu asiayhteydestä ilmenevä suostumus
2	Luovutuksen pyytäjä	Mikäli suostumusta ei tarvita Määritellään muu luovutuksen peruste	Luovutuksen muita perusteita ovat mm. - Pakkotila - Luovutus PotL 13 § perusteella - Muu laista johtuva peruste (luokitus) - Toimeksiantosopimus - Kokeilulain mukainen omaneuvojasopimukseen sisältyvä suostumus - Kokeilulaissa määritelty sopimus
3	Luovutuksen pyytäjä	Luovutuksen pyytäjä laatii luovutuspyynnön ja vahvistaa sen	Luovutuspyyntö sisältää linkin mahdolliseen suostumusdokumenttiin
4	Luovutuksen pyytäjä	Luovutuksen pyytäjä lähettää luovutuspyynnön tietojen luovuttajalle.	Lähetys sisältää luovutuspyynnön sekä suostumusasiakirjan Tekninen lähetys tapahtuu käyttäen tietojärjestelmää ja tietoverkkoa
5	Luovuttaja	Luovuttaja varmistuu luovutuspyynnön aitoudesta	Luovuttaja todentaa luovutuksen pyytäjän ja varmistuu tämän noudattamasta tietoturvapolitiikasta ja tekee päätöksen jatkaa luovutuksen käsittelyä. Mikäli luovuttaja ei luota luovutuspyyntöön, hylkää luovuttaja luovutuspyynnön ja lähettää asianmukaisen ilmoituksen. Ilmoituksessa luovuttaja kertoo, mitä luovutuksen pyytäjän tulee seuraavaksi tehdä, mihin ottaa yhteyttä jne.

	Luovutuspyynnön ja luovutuksen tehtävät		
Nro	**Tekijä**	**Tehtävä**	**Selityksiä**
6	Luovuttaja	Luovuttaja tarkistaa luovutuksen edellytysten olemassaolon	Luovuttaja tarkistaa mm. seuraavat tiedot: - luovutuksen pyytäjän ja potilaan hoitosuhteen tai muun asiallinen yhteys potilaaseen olemassaolon. Nykytietojärjestelmät eivät tue hoitosuhteen tarkistusta, joten luovuttaja joutuu käytännössä luottamaan pyytäjän ilmoitukseen. Luovutuksen pyytäjän ja luovuttajan välinen luottamus tulee perustua samantasoiseen tietoturvapolitiikkaan ja/tai tietojärjestelmien auditointiin. Mikäli luovutuksen perusteena on sopimus sen olemassaolo ja soveltuvuus luovutustilanteeseen tarkistetaan. Suostumuksesta tarkistetaan: - suostumus on potilaan taikka tämän laillisen edustajan antama - suostumuksen voimassaolo – luovuttaja on se sama organisaatio kuin se jolta suostumuksessa tiedot pyydetään – luovutuksen pyytäjä on nimetty suostumuksessa tietojen vastaanottajaksi – luovutuspyynnössä nimetty käyttötarkoitus vastaa suostumuksessa nimettyä käyttötarkoitusta - luovutuspyynnössä nimetty asiayhteys vastaa suostumuksessa nimettyä asiayhteyttä - luovutuspyynnössä yksilöidyt tiedot ovat suostumuksen mukaisia luovutettavia tietoja – luovutuspyynnössä yksilöidyt tiedot ovat saatavissa potilasrekisteristä Mikäli luovutuksen edellytykset eivät ole voimassa, luovuttaja hylkää luovutuspyynnön ja lähettää hylkäyksen perustelevan vastauksen.
7	Luovuttaja	Luovuttaja laatii luovutuksen kuvailutiedot allekirjoittaa ne. Luovuttaja noutaa pyydetyt tiedot omasta tietojärjestelmästään. Luovuttaja sulkee kuvailutiedot ja luovutettavat tiedot sähköiseen kirjekuoreen	Sähköisessä ympäristössä sekä kuvailutiedot että luovutettavat tiedot varustetaan yksilöintitunnisteilla (OID-koodeilla). Allekirjoitus tulee olla sähköinen. Voidaan käyttää digitaalista kirjekuorta
8	Luovuttaja	Luovuttaja lähettää luovutettavat tiedot luovutuksen saajalle	Luovuttaja valitsee tarkoitukseen sopivan ja turvallisen tavan tietojen välitykseen. Luovuttaja varmistuu, että tiedonsiirron aikana tiedot eivät joudu sivullisen käsiin ja ne pysyvät eheinä.
9	Luovuttaja	Luovuttaja tekee merkinnät luovutuksesta potilasasiakirjoihin ja lokitietoihin	Merkintään STM:n asetuksen (A 21 §) mukaiset tiedot. Merkitään luovutuslokiin jäljempänä määritellyt tiedot.
10	Luovutuksen saaja	Luovutuksen saaja vastaanottaa luovutetut tiedot.	Luovutuksen saaja varmistuu luovutuksen aitoudesta ja tietojen muuttumattomuudesta. Luovutuksen saaja lähettää kuittauksen tietojen vastaanotosta.

	Luovutuspyynnön ja luovutuksen tehtävät		
Nro	**Tekijä**	**Tehtävä**	**Selityksiä**
			Mikäli luovutuksen saaja hylkää luovutuksen, on saajan käynnistettävä selvitys luovuttajan kanssa ongelman selvittämiseksi ja poistamiseksi.
11	Luovutuksen saaja	Luovutuksen saaja tekee merkinnät luovutuksesta potilasasiakirjoihin ja lokitietoihin	Merkintään STM:n asetuksen (A 21 §) mukaiset tiedot Merkitään lokiin jäljempänä määritellyt tiedot
12	Luovutuksen saaja	Luovutuksen saaja käsittelee potilastiedot luovutuspyynnön käyttötarkoitusta vastaavasti ja vain hoitotilanteessa.	Mikäli luovutuksen saaja siirtää saamiaan tietoja potilaan asiakirjoihin tulee niihin merkitä luovutettujen tietojen alkuperä.

4.3.2 Luovutuspyyntö voimassa olevan suostumuksen perusteella

Suostumusraportissa on ehdotettu, että tiettyyn käyttötarkoitukseen annettu suostumus voi olla voimassa (jos näin on potilaan kanssa sovittu) enintään kolme (3) vuotta. Ammattihenkilö voi käyttää tällaista voimassaolevaa suostumusta, kun hän tarvitsee sen voimassaoloaikana samaan yksilöityyn käyttötarkoitukseen potilaan tietoja muista toimintayksiköistä.

Tässäkin tapauksessa on luovutuksen edellytyksenä hoitosuhde, kokeilulain mukainen omaneuvojasopimus tai muu asiallinen yhteys. Suostumusdokumentti on liitettävä luovutuspyyntöön tai sen on muuten oltava luovuttajan käytettävissä, jotta tämä voi varmistua luovutuksen edellytysten voimassaolosta.

Tilanteessa tarvittavat ja syntyvät asiakirjat sekä työtehtävät ovat edellä kuvatun taulukon mukaisia.

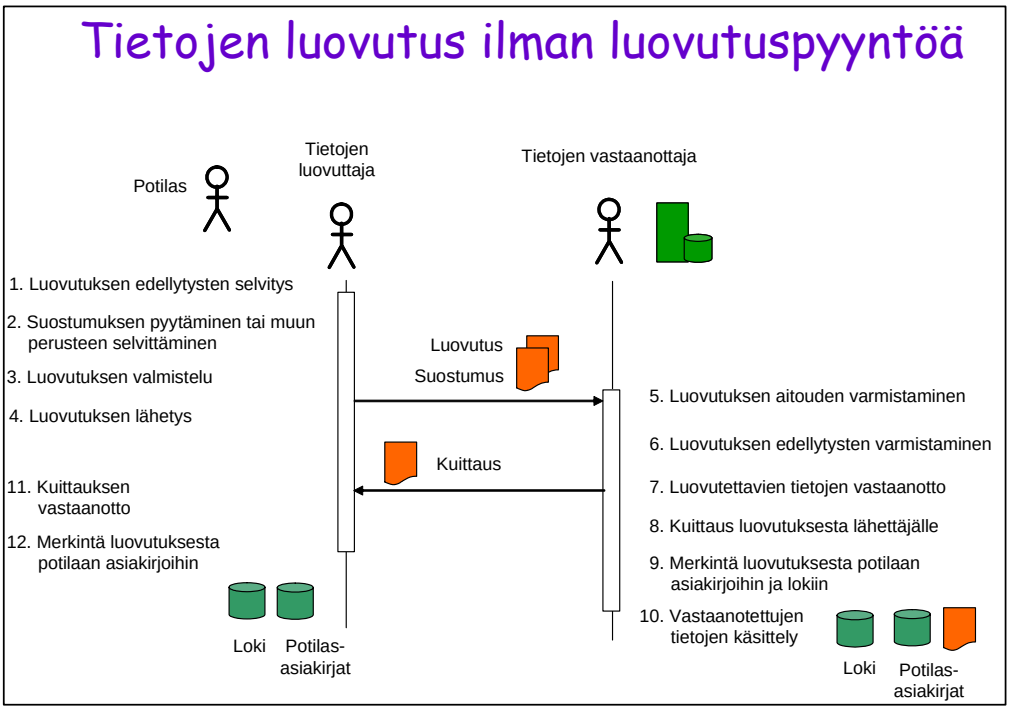
4.3.3 Luovutettujen tietojen edelleen luovutus

Edelleen luovutuksella tarkoitetaan tässä tilannetta, jossa luovutuksen saaja "jatkoluovuttaa" saamansa tiedot muulle rekisterinpitäjälle, henkilölle tai organisaatiolle. Lähtökohta on, että luovutuksen saaja voi luovuttaa tietoja edelleen vain laissa määrätyin edellytyksin ja että tietojen alkuperän on joka tapauksessa oltava aina näkyvissä. Nämä edellytykset tulee ilmetä potilaalle annettavasta yleisestä luovutusta koskevasta informaatiosta.

4.3.4 Tietojen luovuttaminen ilman luovutuspyyntöä

Kyseessä on tilanne, jossa tietojen luovuttaja tekee luovutuksesta joko aloitteen yhteistyössä potilaan kanssa tai luovutus tapahtuu ilman erillistä suostumusta lakiin tai sopimukseen perustuen. Tässäkin tapauksessa luovutus voi perustua joko kirjalliseen, suulliseen tai asiayhteydestä ilmenevään suostumukseen, sopimukseen tai luovutus tapahtuu potilaan suostumuksetta lain antamin perustein. Jos tällaisen luovutuksen peruste on suostumus, tulee siitä ilmetä luovutuksen antaja(t), luovutettavat tiedot mahdollisine rajauksineen ja niiden käyttötarkoitus (esimerkkejä ovat mm. lähete, hoitopalaute, konsultaatio, lausunto, todistus ja lääkemääräys). Suostumuksella potilas antaa luovuttajalle luvan kyseiseen luovutukseen.

Kuva 5 esittää pelkistetysti luovutusprosessia, kun luovutus tapahtuu ilman luovutuspyyntöä.



Kuva 5 Tietojen luovutus ilman luovutuspyyntöä

Luovutus sisältää seuraavat tehtävät:

	Tehtävät luovutettaessa tietoja ilman luovutuspyyntöä		
Nro	**Tekijä**	**Tehtävä**	**Selityksiä**
1	Luovuttaja	Luovutuksen edellytysten selvitys	Potilaalla on hoitosuhde tai muu asiallinen yhteys luovuttajaan Luovuttajalla ja luovutuksen vastaanottajalla on keskinäinen sopimus (esim. toimeksiantosopimus), joka lain mukaisesti mahdollistaa, joko potilaan suostumuksella tai suostumuksetta tapahtuvan tiedon luovuttamisen. Luovutus tapahtuu suostumuksella ja laista johtuvien perustein. Lähetteen tapauksessa luovutuksen tekijä on lähettävä lääkäri ja saaja on se toimintayksikkö, johon lääkäri kirjoittaa lähetteen. Lähetteen yhteydessä käytetään yleensä suullista suostumusta. Vrt suostumusraportti Hoitopalautteen tapauksessa luovuttaja on se toimintayksikkö jossa potilas on hoidossa tai yksityinen ammatinharjoittaja. Luovutuksen saaja on tavallisesti lähetteen laatinut toimintayksikkö. Organisaatioiden välisen konsultaatiopyynnön tapauksessa luovuttaja on se toimintayksikkö , jossa konsultaatiota pyytävä lääkäri on töissä. Luovutuksen saaja on konsultaatiopyyntöön vastaava toimintayksikkö. Osapuolet voivat olla myös itsenäisiä ammatinharjoittajia. Todistuksen tai lausunnon luovuttaja on se toimintayksikkö, jossa ao. ammattihenkilö on töissä. Luovutuksen saaja on lausunnon tai todistuksen tarvitsija, esimerkiksi Kela, työnantajan työterveyslääkäri, muu vakuutusyhtiö tai muu viranomainen.
2a	Luovuttaja	Luovuttaja selvittää potilaan kanssa luovutettavat tiedot, ellei kyseessä ole esim. lain mukaan vakuutusyhtiölle toimitettava lausunto.	Potilasta informoidaan luovutuksen tarkoituksesta ja selvitetään mitä tietoja luovutetaan.
2b	Luovuttaja	Jos suostumus tarvitaan, luovuttaja pyytää potilaalta suostumuksen luovutukseen	Suostumuksen laadinta on ohjeistettu suostumusdokumentissa
2c	Luovuttaja	Luovuttaja selvittää luovutuksen perusteet jos suostumusta ei tarvita	Luovutuksen perusteita voivat olla mm. - Pakkotila - Luovus PotL 13 § perusteella - Muu laista johtuva peruste (luokitus) - Osapuolten välinen toimeksiantosopimus - Omaneuvojasopimus - kokeilulain mukainen potilaan kanssa tehty sopimus

	Tehtävät luovutettaessa tietoja ilman luovutuspyyntöä		
Nro	**Tekijä**	**Tehtävä**	**Selityksiä**
3	Luovuttaja	Luovuttaja valmistelee luovutettavan tietosisällön	Luovuttaja kerää asiayhteyden ja käyttötarkoituksen kannalta tarpeelliset tiedot ja koostaa niistä luovutettavat tiedot. Sopimuksen tai muun perusteen tapauksessa luovuttaja kerää luovutettavat tiedot tietojärjestelmästään. Konsultaation tapauksessa konsultoiva lääkäri kerää tarvittavat tiedot.
4	Luovuttaja	Luovuttaja lähettää luovutettavan tiedot ja otsikkotiedot mukaan lukien luovutuksen saajalle	Luovuttaja valitsee turvallisen ja tarkoituksenmukaisen tiedonsiirtotavan. Konsultaation tapauksessa konsultoiva lääkäri lähettää tarvittavat tiedot. Mikäli tiedonsiirtotavan turvallisuudessa on epävarmuutta, luovuttaja informoi potilasta ja sopii luovutuksen tekotavasta. Suostumuksellakaan ei saa laiminlyödä suojausta.
5	Luovutuksen saaja	Luovutuksen saaja varmistaa asiakirjan aitouden ja varmistuu oikeasta luovuttajasta	Luovutuksen saaja tarkistaa luovuttajan sähköisen allekirjoituksen tai muulla tavalla varmistuu oikeasta luovuttajasta asiakirjan aitoudesta sekä sen sisällön muuttumattomuudesta. Mikäli aitoudesta syntyy epäily, lähettää luovutuksen saaja kuittauksen vastaanoton hylkäyksestä.
6	Luovutuksen saaja	Luovutuksen saaja varmistuu, että luovutus vastaa mukana olevaa suostumusta	Luovutuksen saaja varmistuu siitä, että potilaan antama suostumus ja luovutetut tiedot vastaavat toisiaan. Mikäli luovutus ei täytä suostumuksen ehtoja, lähettää luovutuksen saaja ilmoituksen vastaanoton hylkäyksestä mukaan lukien hylkäämisperusteet perusteet. Luovutuksen perustuessa osapuolten väliseen sopimukseen luovutuksen saaja varmistuu siitä, että luovutetut tiedot ovat sopimuksen mukaisia.
7	Luovutuksen saaja	Luovutuksen saaja vastaanottaa luovutetut tiedot	Tietojen eheys tarkistetaan. Tarkistetaan saadut tiedot jottei niissä esiinny haittaohjelmia (mm. viruksia)
8	Luovutuksen saaja	Luovutuksen saaja lähettää teknisen kuittauksen luovutuksen onnistuneesta vastaanotosta.	Luovutuksen saaja lähettää kuittauksen luovutuksen vastaanotosta.
9	Luovutuksen saaja	Luovutuksen saaja tekee merkinnät luovutuksen vastaanotosta potilasasiakirjoihinsa.	Merkitään STM:n asetuksen mukaiset tiedot
10	Luovutuksen saaja	Luovutuksen saaja käsittelee vastaanottamansa tiedot	Lähetteen tapauksessa lähetteen käsittelijä voi lähettää lähettävälle lääkärille vastauksen lähetteen aiheuttamista toimenpiteistä tai pyytää lisätietoja.
11	Luovuttaja	Luovuttaja vastaanottaa kuittauksen luovutuksesta.	Mikäli vastaanotto hylätään, on luovuttajan käynnistettävä selvitys luovutuksen saajan kanssa ongelman selvittämiseksi ja poistamiseksi.
12	Luovuttaja	Luovuttaja tekee merkinnät luovutuksesta potilaan asiakirjoihin.	Merkitään lokiin jäljempänä määritellyt tiedot.

5. Perusluovutusta monimutkaisemmat luovutustilanteet

Monimutkaisemmat luovutustilanteet on mahdollista hallita siten, että ne palautuvat luvussa 4.3 kuvattuun kahteen luovutuksen perustyyppiin tai ovat niiden yhdistelmiä.

5.1 Lähetteen tietojen täydennyspyyntö

Suostumusraportissa (ks. Osaavien keskusten verkoston raportti 2/2004) on käsitelty ns. *vuorovaikutteista lähetettä*, jonka yhteydessä lähetteen käsittelijä voi pyytää lisätietoja hoitopäätöksen tekemistä varten. Tätä toimintaa voidaan kutsua myös lähetteen tietojen *täydennyspyynnöksi*. Lähetteen yhteydessä käytetään suostumusraportin suosituksen mukaisesti suullista suostumusta. Tällöin potilasta tulee informoida siitä, että

- lähetteen mukana luovutetaan tarpeelliset hoitotiedot,
- lähetteen käsittelijälle voidaan tarvittaessa luovuttaa tähän käyttötarkoitukseen liittyviä lisätietoja.

Lisätietojen pyytäminen ja niiden luovuttaminen sähköisesti tapahtuu pyyntö- ja luovutusmekanismia käyttäen. Perusluovutukseen verrattuna tarkoittaa lähetteen täydennyspyyntö sitä, että lisätietoja pyydettäessä ilmoitetaan tietojen käyttötarkoitukseksi "lähetteen vuorovaikutteinen käsittely" ja suostumukseksi merkitään potilaan suullinen suostumus (joka on annettu lähettävässä toimintayksikössä) ja tehdään asianmukainen merkintä potilasasiakirjaan.

5.2 Toimintayksiköiden välinen konsultaatio

Sellaisen toiseen toimintayksikköön osoitetun konsultaatiopyynnön tekeminen, josta käy ilmi potilaan henkilöllisyys, vaatii potilaan antaman suostumuksen tietojen luovutukseen (PotA 15 §).

Konsultoitava ammattihenkilö vastaa konsultaatiopyyntöön antamalla lausunnon tai muuten ilmaisemalla kantansa kyseessä olevaan asiaan. Konsultaatiopyynnön tekijä tekee merkinnät konsultaatiopyynnöstä sekä saamastaan vastauksesta potilasasiakirjoihin. Vastaavasti konsultaatiopyyntöön vastaava ammattihenkilö tekee merkinnät konsultaatiopyynnöstä sekä antamastaan vastauksesta oman toimintayksikön potilasasiakirjoihin. Näistä vastauksista tulee laatia erillinen rekisteri, jota ei voi yhdistää potilaalla mahdollisesti ko. toimintayksikössä jo oleviin tietoihin. Konsultaatiopyyntöön vastaaminen ei edellytä potilaan suostumusta.

Konsultaatiopyyntö ja vastaus välitetään luovutussanomia käyttäen.

5.3 Hoito- ja palveluketjusuunnitelman toteuttamiseen liittyvä tietojen luovutus

Hoito- ja palveluketjusuunnitelman laatimisen yhteydessä potilas antaa suostumuksensa suunnitelman toteuttamiseen osallistuville toimintayksiköille tietojen luovuttamisesta tähän käyttötarkoitukseen tarvittavista, toisissa toimintayksiköissä sijaitsevista hoitotiedoista (katso tarkemmin suostumusraportti).

Tietojen luovuttamisesta voidaan myös tehdä potilaan kanssa kokeilulaissa määritelty omaneuvojasopimus, johon sisältyy asiakkaan antama kirjallinen suostumus, jonka pe-

rusteella omaneuvojalla on oikeus saada tehtävänsä suorittamiseksi koskevia tietoja (kohta 3.2).

Osapuolet tallettavat itseään koskevat suostumukset omiin potilastietojärjestelmiin. Suostumukset ja palveluketjusuunnitelmat voidaan tallettaa myös esimerkiksi viitetietojärjestelmää käyttävään aluetietojärjestelmään.

Tietojen luovuttamisessa noudatetaan sitä, mitä on esitetty rekisterin pitäjien välisestä tietojen luovuttamisesta.

5.4 Palvelujen ulkoistaminen

Silloin, kun terveydenhuollon rekisterinpitäjä hankkii palveluja toiselta rekisterinpitäjältä, on näiden tehtävä sopimus potilasasiakirjojen rekisterinpitoon ja tietojen käsittelyyn liittyvistä tehtävistä ja vastuista. Tietosuojavaltuutetun toimiston www-sivuilta löytyy ulkoistamiseen liittyviä mallisopimuksia.

Ulkoistaminen voi tapahtua usealla eri tavalla. Voidaan ulkoistaa pelkästään rekisterinpito tai palvelua ulkoistettaessa sopia, kuka on rekisterinpitäjä. Tässä raportissa *suositellaan*, että palveluja ulkoistettaessa rekisterinpitäjänä säilyy palveluja ulkoistava toimintayksikkö (ts. palvelut ulkoistetaan tilaajan lukuun). Tällöin hoitotiedot kuuluvat palveluja ulkoistaneelle rekisterinpitäjälle. Palveluita tuottava rekisterinpitäjä ei voi tässä tapauksessa käyttää näitä tietoja omassa toiminnassaan ilman asiakkaan antamaa suostumusta tai laista johtuvaa muuta syytä.

Palvelujen ulkoistamiseen liittyvissä luovutuspyynnössä tulee luovutuksen perusteena käyttää osapuolten välistä ulkoistamissopimusta.

5.5 Erikoissairaanhoidon tuottamat palvelut muille kuntayhtymän toimintayksiköille

Erikoissairaanhoitolain 10b §:ssä käsitellään sairaanhoitopiirin toimintayksiköiden tuottamia palveluita muille saman kuntayhtymän toimintayksiköille. Näissäkään tilanteissa ei palveluiden tuottamiseen tarvittavien ja tuottamisessa syntyneiden tietojen luovuttamiseen tarvita potilaan suostumusta. Palveluja tuottava sairaanhoitopiiri tai sen toimintayksikkö voi tallettaa tällaisessa toiminnassa syntyvät tiedot omaan vastaavia tietoja sisältävään rekisteriinsä sekä käyttää tietoja potilaidensa hoidon järjestämisessä ja toteuttamisessa. Palveluista on syytä pitää erillistä tilaajakohtaista osarekisteriä. Vaikka tietoja voidaan käyttää omien potilaiden hoitoon, ei niitä saa luovuttaa ulkopuolisille. Sairaanhoitopiirin potilastietojärjestelmän käyttäjänhallinnan tule huolehtia siitä, että tietoja käsitellään asianmukaisesti (ks. luku 2).

5.6 Muut nimenomaisesti säädetyt tilanteet

Potilaslain 13 §:n perusteella voidaan tarpeellisia hoitotietoja luovuttaa tutkimuksen ja hoidon järjestämiseksi ilman potilaan antamaa suostumusta, mikäli potilaalla ei ole mielenterveyshäiriön, kehitysvammaisuuden tai muun vastaavan syyn vuoksi edellytyksiä arvioida annettavaa suostumusta eikä hänellä ole laillista edustajaa taikka suostumusta ei voida hankkia tajuttomuuden tai siihen verrattavan syyn vuoksi. Luovutus on voitava aina perustella.

Tietojen luovutuspyyntöön ja/tai luovutussanoman otsikkoon on tehtävä merkintä tämän syyn perusteella tapahtuvasta luovutuksesta.

5.7 Alueen toimintayksiköiden yhteiskäytössä olevat tietojärjestelmät

Yhteistoiminta-alueiden toimintayksiköt voivat hankkia yhteiseen käyttöön tietojärjestelmiä. Tällaisia ratkaisuja kutsutaan usein "aluejärjestelmiksi". Koska alueellisista rekisterinpitäjistä ei toistaiseksi ole lainsäädäntöä, säilyy rekisterinpidon vastuu tällaisissa järjestelmissä sillä toimintayksiköllä, joka potilastiedoista on kysymys. Jotta eri toimintayksiköiden tiedot voidaan pitää erillään, tulee aluejärjestelmien tietokannoissa olevissa potilastiedoissa olla merkintä tiedon rekisterinpitäjästä. Tällaisissa aluetietojärjestelmissä tapahtuva toisen toimintayksikön tietojen katselu on tietojen luovutusta ja sen yhteydessä tulee noudattaa tässä raportissa esitettyjä periaatteita.

6. Tiedon luovuttaminen toisiin maihin

6.1 Tiedon luovuttaminen toiseen EU-maahan

EU:n henkilötietodirektiivi (95/46/EC) luo itsessään yhtenäisen tietosuojan laillisuusympäristön. Direktiivin lisäksi tulee noudattaa kunkin maan kansallista lainsäädäntöä. Henkilötietodirektiivin lähtökohtana on, että potilaan (ns. data subjektin) suostumus tarvitaan tiedonsiirtoon joka tapahtuu yli valtakunnan rajojen, ellei kyseessä ole potilaan elintärkeä etu. Jotta henkilötietojen siirto tai antaminen käsiteltäväksi olisi laillista, tulee tietojen siirron olla kyseisessä tapauksessa sallittu myös Suomessa. Myös Suomen lainsäädännössä olevia salassapitosäädöksiä tulee noudattaa.

Lähtökohta luovutettaessa potilastietoja Suomesta toiseen EU-maahan on se, että potilastietoja voidaan luovuttaa vain potilaan asianmukaisella suostumuksella tai laissa olevan nimenomaisen säännöksen perusteella. ETA- maat on henkilötietolaissa rinnastettu EU-maihin (ETA-maihin kuuluvat mm. Islanti, Liechtenstein ja Norja). Tietosuojavaltuutetun toimisto on laatinut ohjeistuksen "Henkilötietojen siirto ulkomaille henkilötietolain mukaan (25.2.2002, www.tietosuoja.fi), josta löytyy yksityiskohtaisemmat ohjeet.

Henkilötietodirektiivin pohjalta on laadittu eurooppalainen standardi "CEN TC 251 Guidance on Handling Personal Health Data in International Applications in the Context of the EU Data Protection Directive". Standardi keskittyy tiedonvaihtosopimuksiin ja se painottaa, että tiedon luovuttajan tulee varmistaa se, että tiedon vastaanottaja noudattaa direktiivin vaatimuksia ja että tarpeelliset toimenpiteet tiedon suojaamiseksi on tehty ja että lainmukainen henkilötietojen käsittely toteutuu. Tiedon luovuttajan tulee pitää huolta, että mm. tietopalveluun, varastointiin ja tiedonvälitykseen liittyviin toimeksiantosopimuksiin on sisällytetty varotoimet (ns. ”safeguards”) yksityisyyden suojan ja perusoikeuksien turvaamiseksi. Nämä varotoimet voivat sisältyä osapuolten väliseen sopimukseen. Sopimukset puolestaan säätelevät tiedon haltijan ja käsittelijän keskinäisten vastuiden jakamista. Tiedon luovuttajan tulee yksityiskohtaisesti määritellä mitä tiedon vastaanottaja saa tehdä ja mitä se ei saa tehdä. Pääsääntöisesti tiedon luovuttajalla on vastuu tiedon mahdollisesta vahingoittumisesta tai laittomasta käytöstä tiedon siirron aikana ellei sopimuksellisesti tätä vastuuta ole siirretty tiedon siirtäjälle. Tärkeä periaate on, ettei tiedon vastaanottaja saa jatkolähettää tietoa kolmansille osapuolille.

6.2 Tiedon luovuttaminen Euroopan unionin tai Euroopan talousalueen ulkopuolelle

Lähtökohta luovutettaessa potilastietoja Suomesta toiseen EU-maahan tai EU:n ulkopuolisiin maihin on sama. Lisäksi on otettavat huomioon henkilötietolain 5 luvussa olevat säännöksen henkilötietojen siirrosta Euroopan unionin ulkopuolelle.

Henkilötietolain (HetL 22 §) pääsäännön mukaan henkilötietoja voidaan siirtää Euroopan unionin jäsenvaltioiden alueen tai Euroopan talousalueen ulkopuolelle ainoastaan, jos kyseisessä maassa taataan tietosuojan riittävä taso. Tietosuojan tason riittävyyden asianomaisessa kolmannessa maassa arvioi kussakin tapauksessa rekisterinpitäjä ja tietosuojavaltuutettu, jolle rekisterinpitäjän on ilmoitettava henkilötietojen siirrosta. Tietoja voidaan siirtää myös niihin kolmansiin maihin, joissa komissio on todennut taattavan

tietosuojan riittävä taso. Näitä maita ovat mm. Sveitsi, Yhdysvallat (ns. safe-harbour järjestelmän) ja Kanada. Yhdysvaltojen osalla tämä tarkoittaa niitä organisaatioita, jotka ovat sitoutuneet noudattamaan em. safe-harbour järjestelmää (ks. Tietosuojavaltuutetun toimisto: Henkilötietojen siirto ulkomaille henkilötietolain mukaan 25.2.2002)

Henkilötietolain 23 §:n perusteella voidaan tietoja siirtää kolmansiin maihin, vaikka niiden tietosuojan taso ei olisikaan riittävä, jos mm.

- rekisteröity on antanut yksiselitteisen suostumuksen siirtoon,
- siirto on tarpeen rekisteröidyn elintärkeän edun suojaamiseksi,
- siirto tehdään rekisteristä, josta yleinen tai erityisin perustein tapahtuva tiedonsaanti on nimenomaisesti säädetty,
- rekisterinpitäjä antaa sopimuslausekkein tai muulla tavoin riittävät takeet henkilöiden yksityisyyden suojan ja oikeuksien suojasta, eikä komissio ole todennut takeita riittämättömäksi,
- siirto tapahtuu henkilötietodirektiivin 26 artiklan 4 kohdassa tarkoitettuja komission hyväksymiä mallisopimuslausekkeita käyttäen. Mallisopimuslausekkeet ovat tulostettavissa tietosuojavaltuutetun toimiston kotisivujen kautta (www.tietosuoja.fi).

6.3 Tietojen luovuttaminen sähköisesti toisiin maihin

Sähköisen tiedonsiirron näkökulmasta yksityisyyden suoja ja tietosuoja muodostuvat erityiseksi ongelmaksi, kun potilastietoja siirretään toisiin maihin mm. silloin kun

- Tietoa pyytävien palveluntuottajien tietoturvapolitiikka ja implementaation taso ei ole tiedossa.
- Tiedonsiirrossa käytetään avointa ja turvatonta tiedonsiirtoverkkoa (esim. Internet).

Tällä hetkellä ei ole käytössä kansainvälistä terveydenhuollon palveluntuottajien ja ammattihenkilöiden todentamisjärjestelmää, jonka avulla voitaisiin varmistua siitä, että tietojen vastaanottaja on se mitä se kuka ja mitä se väittää olevansa.

Tietojen luovuttajan tuleekin varmistua huolellisesti siitä, että tietojen pyytäjä on kuka ja mitä hän todellisuudessa väittää olevansa. Tunnisteellisten tietojen lähettämistä tulee välttää ja tunnisteelliset tiedot tulee sähköisessä viestinnässä lähettää aina salattuna.

7. Sähköisen luovutuksen erityistilanteita

7.1 Luovutuspyynnön hylkäys

Tietojen luovutuspyyntöön voi tulla luovutettavien tietojen rekisterinpitäjältä kielteinen vastaus. Luovutuspyynnön käsittelijä voi todeta, että luovutuspyyntö ei täytä luovutuksen edellytyksiä. Syitä tähän voivat olla mm:

- Luovutuspyynnön saaja ei kykene varmistumaan tietojen pyytäjästä.
- Luovutuspyynnön tekijän tietoturvapolitiikka ei täytä lain, asetusten ja ohjeiden vaatimuksia.
- Luovutuspyyntöasiakirjojen aitous ja muuttumattomuus eivät ole kunnossa.
- Luovutuspyyntö ja/tai siihen liittyvä suostumus on puutteellinen.
- Luovutuspyynnön kohteena oleva henkilö ei ole ollut pyynnön vastaanottajan potilaana.
- Luovutuspyynnön saajalla ei ole luovutuspyynnössä mainittuja tietoja.

Tällaisessa tilanteessa luovuttaja antaa luovutuksen pyytäjälle kielteisen päätöksen tehneen henkilön (tai luovutuksen hallinnan järjestelmän) vahvistaman perustelun luovutuspyynnön hylkäämiseen ja pyytää tarvittaessa lisäselvityksiä. Merkintä hylätystä luovutuspyynnöstä ja hylkäyksen peruste merkitään lokitietoihin.

Luovutuspyynnön tekijän tulee samaten tehdä merkintä hylätystä luovutuspyynnöstä oman toimintayksikkönsä lokiin.

Luovutuspyynnön tekijä voi täydentää puutteellista luovutuspyyntöä ja tarvittaessa tehdä kokonaan uuden luovutuspyynnön.

7.2 Luovutuspyynnön peruutus

Luovutuspyynnön tekijä voi peruttaa tekemänsä luovutuspyynnön ennen kuin luovuttaja on ehtinyt tehdä tietojen luovutuksen. Luovutuspyynnön vastaanottajan on lähetettävä kuittaus peruutetusta luovutuspyynnöstä. Mikäli luovutus on jo tapahtunut, ei luovutuspyyntöä voi enää peruuttaa.

7.3 Luovutuksen hylkäys

Luovutuksen vastaanottaja voi hylätä saamansa luovutuksen. Syitä voi tähän olla esimerkiksi:

- Luovutuksen saaja ei luota luovuttajan tietoturvapolitiikkaan tai kykene varmistumaan luovuttajasta
- Luovutussanoman aitous ja muuttumattomuus eivät ole kunnossa
- Luovutuksen sisältö on puutteellinen
- Luovutetut tiedot ovat virheellisiä (esim. henkilötunnus ei mene tarkistuksesta läpi)

Luovutuksen vastaanottajan tulee ilmoittaa luovutuksen tekijälle hylkäyksestä ja hylkäyksen syy mahdollisimman tarkasti. Merkintä hylätystä luovutuksesta ja hylkäyksen perusteesta tulee merkitä lokitietoihin. Luovutuksen tekijä tallettaa myös merkinnän hylätystä luovutuksesta omaan lokiinsa.

Luovutuksen tekijä voi täydentää hylättyä luovutusta tai kokonaan tehdä uuden luovutuksen.

7.4 Luovutuksen peruutus

Luovutuksen tekijä voi peruuttaa tekemänsä luovutuksen. Peruutus voi tulla tarpeelliseksi esimerkiksi virheellisesti valitun vastaanottajan tapauksessa. Luovutus on peruutettava aina kokonaisuutena, sillä peruutuksella ei voida vaarantaa viestien eheyttä. Luovutuksen vastaanottajan tulee mitätöidä saamansa peruutustiedon perusteella mahdollisesti tekemänsä merkinnät potilasasiakirjoihin. Luovutuksen saajan tulee lähettää tieto vastaanottamastaan peruutustiedosta luovuttajalle.

7.5 Luovutetun tiedon korjaus

Tiedon luovuttaja voi joutua korjaamaan aiemmin lähettyä virheellistä tietoa omassa tietojärjestelmässään. Mikäli järjestelmässä on merkintä tiedon luovutuksesta, on tieto virheellisen tiedon korjauksesta lähetettävä mahdollisuuksien mukaan luovutuksen saajalle.

7.6 Sähköisen ja manuaalisen tietojärjestelmän välinen tietojen luovutus

Potilastietojen luovutuksessa saattaa tulla eteen tilanne, jossa toinen toimintayksikkö käyttää manuaalista tietojärjestelmää ja toinen käyttää sähköistä tietojärjestelmää. Tällaisessa tilanteessa varsinainen tietojen vaihto on suoritettava paperimuodossa.

Se osapuoli, joka käyttää sähköistä järjestelmää, tulostaa tarvittavat luovutuspyynnöt tai luovutusasiakirjat ja luovutettavat tiedot paperille ja lähettää ne manuaalista tietojärjestelmää käyttävälle osapuolelle. Samoin sähköistä järjestelmää käyttävä osapuoli kirjaa vastaanottamansa paperiset luovutuspyynnöt tai luovutetut tiedot tietojärjestelmäänsä.

Tietosisällöt ja tietojen vaihdon prosessikuvaukset ovat periaatteiltaan samat kuin jos kummallakin osapuolella olisi käytössään sähköinen tietojärjestelmä. Tarvittavat allekirjoitukset ovat luonnollisten henkilöiden tekemiä.

8. Potilas rekisterinpitäjänä

Potilaan toimiessa itseään koskevien hoitotietojen rekisterinpitäjänä (esimerkkinä diabetes-kotipäiväkirjan pitäminen tai verenpainetietojen kerääminen henkilökohtaiseen tietokoneeseen), päättää potilas kenelle tietoja luovuttaa. Jos tietoja luovutetaan terveydenhuollon toimintayksikölle, tulee luovutusprosessissa noudattaa tämän raportin esittämiä vaatimuksia ja käytäntöjä.

9. Tietojen luovuttaminen potilastietojärjestelmien välillä

Tähän tilanteeseen pätevät tässä raportissa aikaisemmin esitetyt lakien ja asetusten säätämät velvoitteet ja vaatimukset sekä tämän raportin esittämät hyvän toiminnan suositukset. Tietoja luovuttavan rekisterinpitäjän potilastietojärjestelmä vastaa luovutuksen edellytysten voimassaolosta ja luovutuksen lainmukaisuudesta.

Yleisimmät potilastietojärjestelmien väliset tietojen luovutusratkaisut perustuvat joko sanomapohjaiseen tiedonvaihtoon potilastietojärjestelmien välillä tai tietojen katseluun teknisen käyttöyhteyden avulla toisen rekisterinpitäjän potilastietojärjestelmästä.

Sanomiin perustuvalle tiedonsiirrolle on raportissa Tietoturvallinen kommunikaatioalusta: Suositus kansallisesti noudatettaviksi standardeiksi (Osaavien keskusten verkosto 7/2004) suositeltu mm. HL7 CDA R2, HL7 CDA R1 paikallistettu, Hl7 2.x ja XML-sanomien käyttämistä.

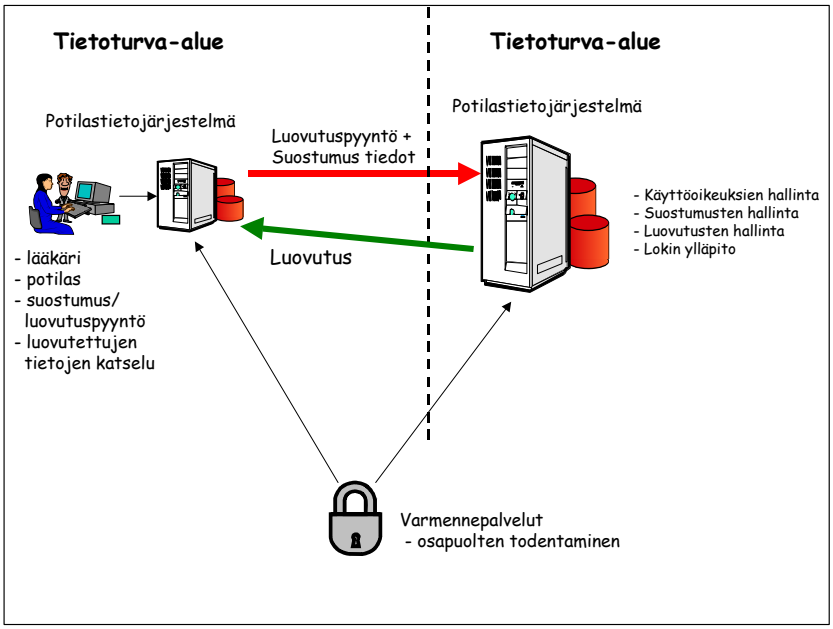
Jokainen toisessa organisaatiossa sijaitsevien tietojen katselutilanne on henkilötietolain mukaista tietojen käsittelyä, joka edellyttää, että käsittelijällä on lakiin, suostumukseen tai sopimukseen perustuva oikeus käsitellä tietoja. Tietojen katselu teknisellä käyttöyhteydellä (esim. www-selaimella) toisesta toimintayksiköstä on tämän raportin linjauksien mukaan tietojen luovuttamista.

Potilastietojärjestelmän käyttöoikeuden luovuttaminen toisessa toimintayksikössä työskentelevälle henkilölle edellyttää sen mahdollistavan lainsäädännön olemassa oloa. Siksi *käyttöoikeuden jakamista toisiin toimintayksikköihin ei voi pitää asianmukaisena toimintana*.

Periaatteessa olisi mahdollista käyttää esimerkiksi kyselytekniikkaa ja lähettää tietoverkon kautta kysely muihin potilastietojärjestelmiin niissä mahdollisesti löytyvästä potilastiedosta (esim. ”löytyisikö teiltä tietoa potilaasta xx ?”). Tällaista *toteutusmallia ei voi pitää lainmukaisena, koska luovutuspyyntö tulee olla yksilöity* ja pelkästään tieto siitä, että tietyn potilaan tietoja on tallennettu tietojärjestelmään on salassa pidettävä tieto.

9.1 Sähköisen luovuttamisen vaihtoehtoisia toteutusmalleja

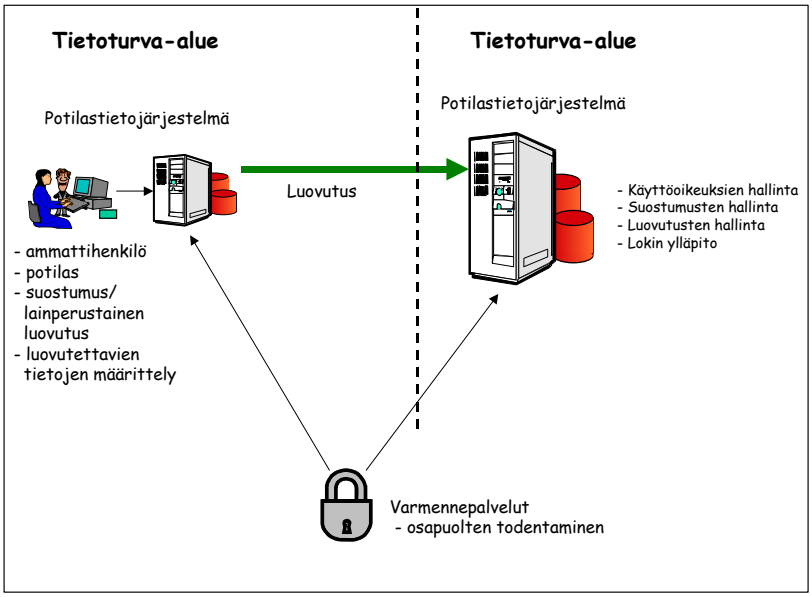
Potilastietojärjestelmien välisen tietojen luovutuksen perusmalli on kuvan 6 mukainen kahden terveydenhuollon toimintayksikön välinen tietojen luovutus. Tietojen välitys tapahtuu tavallisimmin sanomapohjaisella tiedonvälitystekniikalla. Tietojärjestelmien välinen tietoliikenneyhteys voidaan toteuttaa esim. VPN- yhteydellä tai käyttämällä avoimia tietoverkkoja ja vahvaa salausta.



Kuva 6 Tietojen luovutus potilastietojärjestelmien välillä luovutuspyynnön perusteella

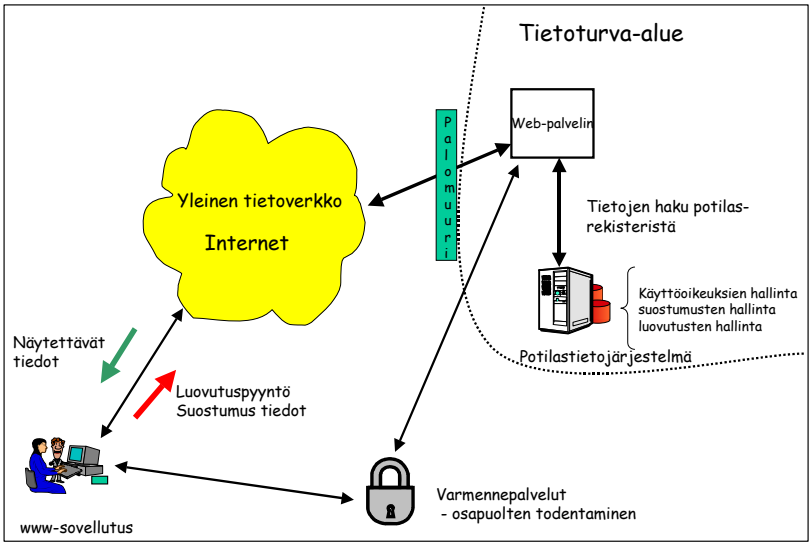
Kuvan 6 tapauksessa kummankin rekisterinpitäjän potilastietojärjestelmät muodostavat oman tietoturva-alueensa, joilla on oma tietoturvapolitiikka, suostumusten, luovutusten ja käyttöoikeuksien hallinta. Kumpikin potilastietojärjestelmä ylläpitää omaa luovutus-lokiaan. Tietoturva-alueiden keskinäinen luottamus voidaan synnyttää esimerkiksi siten, että osapuolet yhdessä tarkistavat toistensa tietoturvapolitiikat, suostumusten hallinnan ratkaisut sekä luovutusten hallinnan ja käyttöoikeuksien hallinnan tietojärjestelmät ja laativat sopimuksen tietojen vaihdosta. Vaihtoehtoisesti voidaan käyttää luotettua kol-matta osapuolta todentamaan osapuolien tietojärjestelmien toiminnan lainmukaisuus (vrt. Ehdotus sosiaali- ja terveydenhuollon sähköisen asioinnin arkkitehtuuriksi - ter-veydenhuollon PKI-arkkitehtuuri, Osaavien keskusten verkoston julkaisuja 4/2002).

Kuvassa 7 on esitetty toinen yleisesti esiintyvä järjestely. Siinä luovutus tapahtuu potilastietojärjestelmien välillä ilman luovutuspyyntöä. Tällaista luovutusta kutsutaan tässä raportissa "PUSH-luovutukseksi". Tässä tapaus vastaa luvussa 4.3.4 esitettyä prosessikuvausta.



Kuva 7 Tietojen luovutus potilastietojärjestelmien välillä kun luovutuspyyntöä ei ole (ns. PUSH-luovutus)

Alla olevassa kuvassa 8 tietojen luovutus tapahtuu potilastietojärjestelmästä käyttäen www-yhteyttä (ts. luovutus tapahtuu siten, että loppukäyttäjä "katselee" työasemansa selaimella potilastietoja toisen potilastietojärjestelmän tietoja). Tietoyhteys voi perustua joko yleisen (turvattoman) tietoverkon käyttöön tai se on toteutettu suljetulla ratkaisulla (esim. VPN-yhteys).



Kuva 8 Tietojen luovutus katselemalla selaimella tietoja toisesta potilastietojärjestelmästä

Katseluyhteys muodostetaan luovuttavan toimintayksikön palvelimeen, joka tarkistaa luovutuksen edellytykset, tekee tarvittavat tunnistukset ja todennukset sekä hakee luovutettavat tiedot potilastietojärjestelmästä. Palvelimen tehtävänä on varmistaa, että vain kyseisen potilaan tietoja näytetään luovutuksen saajalle. *Tässäkin toteutusmallissa tulee järjestelmien välillä vaihtaa jäljempänä esitetyt luovutuspyynnön, suostumuksen ja luovutuksen tietosisältöä vastaavat tiedot.*

9.2 Luovutus potilastietojärjestelmästä muuhun kuin toiseen potilastietojärjestelmään

Sen lisäksi, että tietoja luovutetaan potilastietojärjestelmien välillä, voidaan potilastietojärjestelmästä luovuttaa tietoja mm.

- lainsäädännön perusteella valvovalle viranomaiselle (mm. terveydenhuollon oikeusturvakeskus (TEO), lääninhallitukset),
- lainsäädännön perustella viranomaisille menevinä ilmoituksina, mm. tartuntatautiilmoitukset, epäilyt ja todetut ammattitaudit sekä työperäiset sairaudet työsuojelupiireille, HILMO-tiedot Stakesille, syöpäilmoitukset syöpärekisterille, kuolinsyytodistukset ja ilmoitukset oikeuslääkäreille,
- vakuutusyhtiöille, kelalle ja sosiaalihuollon viranomaisille,
- ulkoistamissopimuksen perusteella tietojärjestelmää ylläpitävälle yritykselle,
- potilaalle

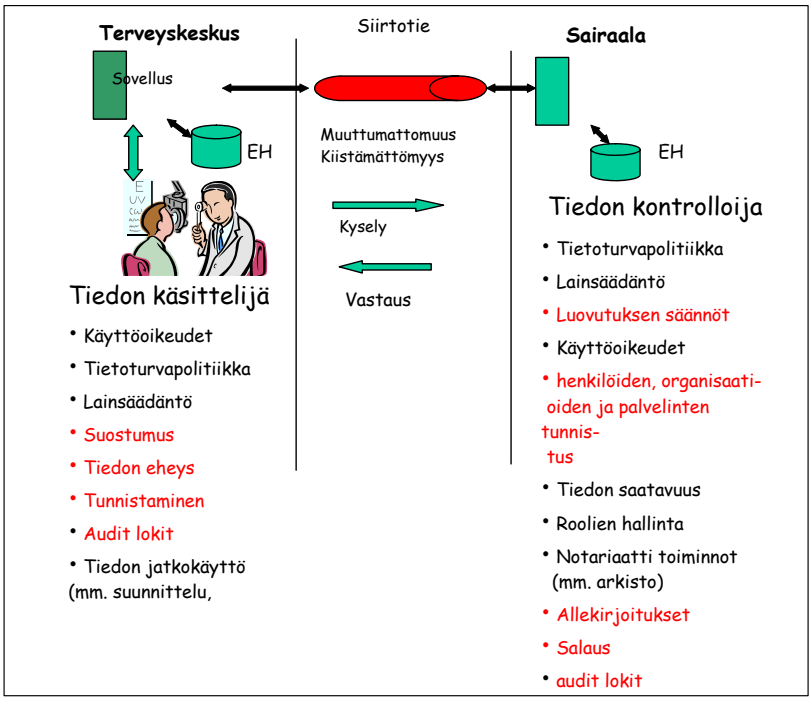
Sähköisessä toimintaympäristössä nämä tapaukset palautuvat kuvien 6, 7 ja esittämiin tapauksiin siten, että tietoa vastaanottava tietojärjestelmä on muu kuin potilastietojärjestelmä.

9.3 Riittävä suojaus

Henkilötiedon luovutuksen edellytys vastaanottajalle/pyytäjälle on, että luovutuksen saaja on ryhtynyt riittäviin toimenpiteisiin tiedon suojaamiseksi ja että

- tiedon luovuttaminen perustuu voimassa oleviin lakeihin ja säädöksiin,
- henkilötietilain 32 §:n mukaisesta suojaamisvelvollisuudesta on huolehdittava,
- tiedon luovutus on tarpeen, jotta voidaan toteuttaa tiedon kohteena olevan henkilön ja tiedon käsittelijän välistä sopimusta tai,
- tiedon luovutus on tarpeen täytettäessä tiedon hallinnoijan ja kolmannen osapuolen välistä sopimusta jonka tarkoituksena on potilaan edun mukainen toiminta,

Kuvassa 9 on hahmotettu ne keskeiset toiminnot ja tietojärjestelmät, joiden avulla edellytysten tarkastaminen ja suojaus voidaan toteuttaa.



Kuva 9 Tieturvallinen tiedonvälitys kahden organisaation välillä (lähde. P. Ruotsalainen ja H. Pohjonen, European Security Framework for Health care, kirjassa Advanced health telematics and Telemedicine, The Magdeburg Expert Summit Textbook, IOS Press, Studies in Health Technology and Informatics, 2003).

9.4 Tiedon suojaamismenetelmät

Tiedon suojaamismenetelmät ovat sekä teknisiä että organisatorisia toimenpiteitä henkilötiedon suojaamiseksi sekä vahingossa tapahtuvaa että laitonta tiedon käyttöä ja luovuttamista, tiedon muuttumista ja häviämistä vastaa erityisesti kun tietoa siirretään tietoverkkojen kautta.

Tämä tarkoittaa terveydenhuollossa mm. sitä, että:

- Sekä tietoja luovuttavalla että vastaanottavalla toimintayksiköllä tulee olla lakien, asetusten, määräysten ja annetut ohjeet täyttävä dokumentoitu tietoturvapolitiikka. Hyvä lähtökohta on se, että osapuolilla on samantasoinen tietoturvapolitiikka. Rekisterinpitäjien tulee siis laatia tietoturvapolitiikka ja keskinäiset sopimukset tietojen luovutuksen menettelyistä ja vastuista.
- Toimintayksikön (ts. tietoturva-alueen) käyttäjänhallinnan tulee varmistaa, että potilaan tietoa voidaan käyttää vain sille määriteltyihin tarkoituksiin.
- Tietoa luovuttavalla tietojärjestelmällä on oltava sekä riittävän korkeatasoinen käyttäjänhallinta, luovutuksen hallintajärjestelmä että lokitietojen ylläpitojärjestelmä, jotta se voi huolehtia siitä, etteivät sivulliset pääse käyttämään luovutettuja tietoja.
- Tiedon luovuttajan luovutuksenhallintajärjestelmän tulee kyetä tarkistamaan, että tiedon luovutuksen edellytykset on täytetty ennen tiedon luovuttamista.
- Käyttäjänhallinnan, tunnistamisen, todentamisen ja salauksen avulla tulee varmistaa, ettei tieto toimintayksikön sisällä joudu ulkopuolisten käsiin.
- Sekä luovutuspyynnön lähettäjä että luovutuksen vastaanottaja tulee voida tunnistaa ja todentaa luotettavasti. Myös luovutuksen vastaanottava palvelin tulee voida tun-

nistaa ja todentaa. Nämä vaatimukset voidaan toteuttaa mm. toimintayksiköiden keskinäisillä auditoinneilla tai käyttämällä varmenteita (kts. PKI-raportti ja saumattoman palveluketjun jatkolaki 12 §).

- Luovutuspyyntö liitteineen tulee sulkea sähköiseen kirjekuoreen silloin, kun sitä siirretään ei turvallisessa verkossa käyttäen esimerkiksi Soap-standardia (kts. osaavien keskusten verkoston julkaisu 7/2004)
- Luovutussanoman tiedot tulee sulkea sähköiseen kirjekuoreen silloin kun sitä siirretään ei turvallisessa verkossa käyttäen esimerkiksi Soap-standardia.
- Tiedonvälityksen aikana tiedon eheys turvataan sähköisellä allekirjoituksella, digitaalisella kirjekuorella tai vastaavalla muulla turvatekniikalla.
- Tiedonvälityksen aikana tietoa siirrettäessä avoimissa verkoissa turvataan salakirjoituksella, ettei tieto voi joutua sivullisten käsiin. Suositeltavia suojausmenetelmiä tiedon siirrossa ovat myös kiinteät linjat ja riittävään salaukseen perustuvat ratkaisut kuten VPN-yhteydet. Avoimessa verkossa voidaan käyttää mm. SSL-salattuja yhteyksiä tai VPN-yhteyksiä.
- Tiedon kiistämättömyys tulee varmistaa mm. kuittauksilla, aikaleimoilla ja varmennejärjestelmän palveluilla.
- Tiedon haltijalla tulee olla koko tiedon säilytysajan kattava suunnitelma, jolla varmistetaan tiedon saatavuus ja käytettävyys.
- Tiedon luovuttamisesta on pidettävä luovutuslokia, jonka eheys on varmistettava.
- Käytetään palomuureja ja vastaavia ratkaisuja rajaamaan käyttäjiä ja suodattamaan tietoliikennettä.
- Tiedon säilytyspaikan fyysinen turvallisuus on turvattava.
- Luovutettavat tiedot tulee tarkistaa ennen luovutusta viruksia, matoja ja troijalaisia vastaan.

9.5 Riskianalyysi

EU direktiivistä (kts. CEN TC 251, Guidance on Handling Personal Health Data in International Applications in the context of EU Data Protection Directive) voidaan johtaa vaatimus, että tietojärjestelmän ja prosessien riskianalyysi on tehtävä sekä tekniseltä että organisatoriselta näkökulmalta. Tämä voi olla myös osa tietojärjestelmän laajempaa arviointia.

9.6 Koodistopalvelimelle sijoitettavat tiedot toimipaikoista ja rekistereistä

Toimintayksikköön kuuluvien toimipaikkojen luettelo on luontevaa sijoittaa Stakesin koodistopalvelimelle. Sinne ollaan jo nyt kokoamassa Suomen terveydenhuollon organisaatioiden toimipaikkaluetteloa. Tämän yhteyteen on mahdollista tehdä ristiintaulukointi kunkin toimintayksikön toimipaikoista ja toisaalta toimipaikan osalta, mihin toimintayksikköön se kuuluu.

Koodistopalvelimelle on tarpeen sijoittaa myös erillään pidettävien rekistereiden luokittelukoodisto.

Toimipaikkojen lisätiedoiksi tarvitaan tieto toimipaikassa mahdollisesti olevista erillään pidettävistä rekistereistä ja niiden rekisterinpitäjästä. Näiden tietojen perusteella kyetään yhdistämään toimintayksikkö toimipisteet ja erillään pidettävät rekisterit.

10. Ehdotus luovutuksen tietosisällöksi

Suomessa sanomanvälitys on laajalti käytetty menetelmä tietojärjestelmien välisessä tiedonvaihdossa. Sanomanvälitysstandardeista HL7 sanomat ovat laajimmalle levinneitä. Lisäksi on käytössä enenevästi selainpohjaisia ratkaisuja. Tässä raportissa tehdään ehdotus luovutukseen liittyvien sanomien tietosisällöksi. Ehdotukset on puettu dokumenttimuotoon, joiden pohjalta niistä on helppo muodostaa HL7/XML-sanomia. Ehdotuksen *ydin on tietosisällöt*, ei se käytetäänkö kommunikaatiossa sanomia vai ei.

Tässä ehdotuksessa lähdetään siitä, että tässä luvussa esitetyt tiedot tulee vaihtaa osapuolten välillä myös siinä tapauksessa, ettei käytetä esimerkiksi HL7/XML sanomia.

Määriteltyjä tietosisältöjä ovat:

- Luovutuspyynnön kuvailutiedot
- Luovutuksen kuvailutiedot, kun luovutus tapahtuu pyynnön perusteella.
- Luovutuksen kuvailutiedot, kun luovutus tapahtuu ilman pyyntöä.
- Luovutuslokin tietosisältö

Suostumusraportissa on erikseen määritelty suostumussanoman tietosisältö.

10.1 Sanomanvälitykseen perustuva tietojen luovutus

Suositeltavaa on käyttää HL7-standardin mukaisia CDA-dokumentteihin perustuvia määrityksiä ja avoimia rajapintoja toteuttavia adaptereita tietojen siirtoon.

Tietojen siirtoon liittyy oleellisena tekijänä yhteinen sopiminen tietotyypeistä ja niiden ilmaisemisesta teknisellä tavalla. Suositeltavaa on käyttää HL7 CDA -standardissa käytettyjä tietotyyppejä.

Tietojen koodaamiseen ja luokitteluun tarvitaan lukuisa joukkoa koodistoja. Suositeltavaa on käyttää Stakesin koodistopalvelin-hankkeen myötä kehitettäviä, ylläpidettäviä ja jaeltavia koodistoja.

10.2 Luovutuspyynnön kuvailutiedot

Luovutuspyynnön kuvailutiedot muodostuvat seuraavista tiedoista:

	Luovutuspyynnön kuvailutiedot	
Nro	**Tieto**	**Selite**
1	Luovutuspyynnön kuvailuosan yksilöivä tunniste	Tunniste on luovutuspyyntöasiakirjan OID-tunnus. Se sijoittuu luovutuksen pyytäjän OID-juureen.
2	Potilas	Henkilö, jonka hoitoa koskevia tietoja pyydetään luovutettaviksi. Tunnistetiedot
3	Luovutuksen pyytäjä	(Ammatti)henkilö, joka pyytää potilaan tietoja. Tarvitaan henkilötiedot ja tehtävä organisaatiossa. Luovutuksen pyytäjän toimintayksikkö, viranomainen, muu organisaatio tai potilas itse
4	Luovuttaja	Toimintayksikkö (rekisterinpitäjä) jolta tiedot pyydetään Yksikön nimi ja OID-koodi Itsenäinen ammatinharjoittaja (nimi ja tunnistetiedot)
5	Luovutuksen saaja	Toimintayksikkö, jolle tiedot luovutetaan Tämä on se toimintayksikkö, jossa luovutuksen pyytäjä työskentelee Viranomainen, organisaatio tai henkilö jolle tiedot luovutetaan Nimi ja OID-koodi
6	Luovutuksen pyytäjän asiallinen yhteys potilaaseen	Selvitys asiallisesta hoitosuhteesta tai muuta asiallisesta yhteydestä
7	Luovutettavien tietojen käyttötarkoitus	Kuvaus käyttötarkoituksesta, johon luovutuksen pyytäjä pyytää tietoja luovutettaviksi
8	Asiayhteys	Asiayhteys (kts. Suostumusraportin suositus asiayhteydeksi suostumussanomassa)
9	Luovutuspyynnön kohteena olevat asiakirjojen yksilöinti	Luovutettavien potilasasiakirjojen tai niiden osien yksilöinti. Yksilöinnissä käytetään asiakirjan OID-tunnusta, mikäli ne ovat tiedossa. Muussa tapauksessa käytetään suostumuksessa tai pyynnössä ilmaistuja luokitustekijöitä, joiden avulla luovuttaja voi tunnistaa luovutuspyynnön kohteena olevat asiakirjat.
10	Luovutuspyynnön ajankohta	Luovutuspyynnön päivämäärä
11	Luovutuksen perusteena oleva suostumus tai muu peruste	Viite luovutuksen perusteena olevaan suostumukseen (myös OID tunnus) Vaihtoehtoisesti muu luovutuksen peruste luokiteltuna (kts. luku 4.3)
12	Luovutuspyynnön vahvistaminen	Luovutuspyynnön tekijän sähköinen allekirjoitus, jos on.

10.3 Suostumuksen tietosisältö

Suostumusdokumentti sisältää seuraavat tiedot: (Tarkempi selostus on suostumusraportissa).

	Luovutuspyyntöön liittyvä suostumusdokumentti	
Nro	**Tieto**	**Selite**
1	Suostumuksen yksilöivä tunniste	Suostumusasiakirjan yksilöivä koodi (OID-koodi)
2	Suostumuksen pyytäjä	Terveydenhuollon ammattihenkilö tai itsenäinen ammatinharjoittaja, jolla on työtehtäviensä johdosta oikeus pyytää suostumus
3	Potilas/Asiakas	Henkilö, jonka hoitotietojen luovuttamisesta on kyse
4	Suostumuksen antaja	Potilas (tai hänen laillinen edustajansa) Tunnisteena nimi ja henkilötunnus
5	Hoitotiedon luovuttaja	Toimintayksikkö tai itsenäinen ammatinharjoittaja jolta tietoja pyydetään
6	Luovutettavat hoitotiedot	Hoitotiedot joiden luovuttamisen potilas/asiakas antaa suostumuksen. Tiedot on syytä kytkeä tietojen käyttötarkoituksen ja asiakkaan ongelmaan. Yksilöidään ne asiakirjat, jotka pyydetään luovutettavaksi kokonaisena tai osittain. Yksilöinnissä käytetään asiakirjan OID-tunnusta, mikäli ne ovat tiedossa. Muussa tapauksessa käytetään sellaisia rajaus- ja luokitustekijöitä, joiden avulla luovuttaja voi tunnistaa luovutuspyynnön kohteena olevat asiakirjat. - Potilaan tekemät rajaukset - Ajanjakso, jolta tiedot luovutetaan
7	Asiayhteys	Hoito/palvelukokonaisuus, jonka piirissä potilas on (kts. Suostumusraportti)
8	Käyttötarkoitus	Selvitys siitä, mihin tarkoitukseen tieto tarvitaan tietoja vastaanottavassa toimintayksikössä
9	Suostumuksen voimassaolo	Alkamis- ja päättymispäivämäärät Potilas ja tietojen luovutuksen pyytäjä sopivat tarkoituksenmukaisen voimassaoloajan kyseessä olevaan käyttötarkoitukseen (Suostumusraportissa suositus enintään 3v:n voimassaolosta)
10	Suostumuksen antamisen ajankohta	Päivämäärä, jolloin suostumus on annettu
11	Vahvistaminen	Suostumuksen antajan sähköinen allekirjoitus. Jos kyseessä on käyttötilanne, jossa riittää suullinen tai asiayhteydestä ilmenevä suostumus, tapahtuu vahvistaminen suostumuksen pyytäjän sähköisellä allekirjoituksella

10.4 Luovutettavien tietojen kuvailutiedot ja luovutettavat tiedot

Luovutus muodostuu luovutuksen kuvailutiedoista ja luovutettavista tiedoista. Kuvailutiedot ja luovutettavat tiedot muodostavat kokonaisuuden. Luovutukseen sisältyvät asiakirjat yksilöidään luovuttajan antamalla asiakirjojen OID-tunnuksella.

	Luovutuspyynnön perusteella tehtävä luovutuksen otsikkotiedot	
Nro	**Tieto**	**Selite**
1	Luovutuksen tunniste	OID-koodi
2	Viite luovutuspyyntöön	Luovutuspyyntödokumentin OID-tunniste
3	Potilas	Henkilö, jonka hoitotietoja luovutetaan Nimi ja henkilötunnus
4	Luovuttaja	Toimintayksikkö, joka luovuttaa tiedot Toimintayksikön nimi ja OID-koodi Itsenäisen ammatinharjoittajan nimi ja tunnistetiedot
5	Luovutuksen saaja	Toimintayksikkö, johon tiedot lähetetään Toimintayksikön nimi ja OID-koodi Mahdolliset tarkennukset (esim. toimipiste)
6	Luovutuksen pyytäjä	Henkilö, joka on tehnyt luovutuspyynnön
7	Luovutukseen sisältyvät asiakirjojen yksilöinti	Yksilöidään luovutettavat asiakirjat tyypeittäin Kukin asiakirja yksilöidään myös OID-tunnuksella Kunkin asiakirjan rekisterinpitäjä (nimi ja OID-koodi) ja rekisterin käyttötarkoitus (koodi) Kunkin asiakirjan sensitiivisyys (luokitus) ja erityissuojaus (luokitus Kunkin asiakirjan rekisterinpitäjä (nimi ja OID-koodi) ja rekisterin käyttötarkoitus Kunkin asiakirjan sensitiivisyys ja erityissuojaus luokka
8	Luovutuksen peruste	Selvitys luovutuksen perusteesta. Se voi olla suostumus, kokeilulaissa mainittu sopimus tai muu laissa mainittu luovutuksen peruste. Yksilöidään mahdollinen luovutukseen liittyvä suostumusdokumentti
9	Luovutuksen ajankohta	Luovutuksen päivämäärä
10	Luovutuksen vahvistaminen	Luovuttajan sähköinen allekirjoitus, joka kattaa myös luovutettavat tiedot

Luovutettavat tiedot:

	Luovutettavat tiedot	
Nro	**Tieto**	**Selite**
1	Tiedon yksilöinti	Yksilöinnissä käytetään apuna asiakirjan OID-tunnusta Asiakirjan tyyppi (luokitus) Nimetään asiakirjan tyyppi, esimerkiksi – lähete – hoitopalaute – konsultaatiopyyntö – lääkemääräys – lausunto – todistus
2	Data	Luovutettavat tiedot ovat tyypillisesti potilasrekisteristä, työterveyshuollon rekisteristä laboratoriojärjestelmästä tai kuvantamisen tietojärjestelmistä poimittuja tietoja

10.5 Luovutuksen kuvailutiedot ja luovutettavat tiedot kun luovutuspyyntöä ei ole

Luovutus koostuu luovutuksen kuvailutiedoista ja luovutettavista tiedoista. Kuvailutiedot ja luovutettavat tiedot muodostavat kokonaisuuden. Luovutukseen sisältyvät asiakirjat yksilöidään luovuttajan antamalla asiakirjojen OID-tunnuksella.

Luovutuksen kuvailutietoihin merkitään luovutuksen perusteeksi potilaan antama suullinen suostumus. Jos suotumusta ei tarvita, merkitään muu luovutuksen peruste. Suostumuksen vahvistaminen tapahtuu suostumuksen pyytäjän sähköisellä allekirjoituksella. Suostumusdokumentti liitetään osaksi luovutettavia tietoja.

Mikäli luovutukseen ei tarvita suostumusta merkittään kuvailutietoihin asianmukainen luovutuksen peruste.

	Luovutuksen kuvailutiedon sisältö, kun luovutuspyyntöä ei ole	
Nro	**Tieto**	**Selite**
1	Luovutuksen tunniste	OID-koodi
2	Potilas	Henkilö, jonka hoitotietoja luovutus sisältää Nimi ja henkilötunnus
3	Luovuttaja	Toimintayksikkö, joka luovuttaa tiedot Toimintayksikön nimi ja OID-koodi Itsenäisen ammatinharjoittajan nimi ja tunnistetiedot
4	Luovutuksen pyytäjä	Ei ole, koska luovuttaja tekee aloitteen luovutuksesta
5	Luovutuksen saaja	Toimintayksikkö, johon tiedot lähetetään Toimintayksikön nimi ja OID-koodi Mahdolliset tarkennukset (esim. toimipiste)
6	Luovutuksen antajan asiallinen yhteys potilaaseen	Selvitys asiallisesta hoitosuhteesta tai muusta yhteydestä
7	Luovutettavien tietojen käyttötarkoitus	Selvitys käyttötarkoituksesta, johon tietoja luovutetaan
8	Luovutukseen sisältyvät asiakirjojen yksilöinti	Yksilöidään luovutettavat asiakirjat tyypeittäin Kukin asiakirja yksilöidään myös OID-tunnuksella Kunkin asiakirjan rekisterinpitäjä (nimi ja OID-koodi) ja rekisterin käyttötarkoitus (koodi) Kunkin asiakirjan sensitiivisyys (luokitus) ja erityissuojaus (luokitus Nimetään asiakirjan tyyppi, esimerkiksi – lähete – hoitopalaute – konsultaatiopyyntö – lääkemääräys – lausunto – todistus Yksilöinnissä käytetään apuna asiakirjan OID-tunnusta Kunkin asiakirjan rekisterinpitäjä (nimi ja OID-koodi) ja rekisterin käyttötarkoitus Kunkin asiakirjan sensitiivisyys ja erityissuojaus luokka
9	Luovutuksen ajankohta	Luovutuksen päivämäärä
10	Luovutuksen peruste	Selvitys luovutuksen perusteesta. Se voi olla suostumus, kokeilulaissa mainittu sopimus tai muu laissa mainittu luovutuksen peruste. Yksilöidään mahdollinen luovutukseen liittyvä suostumusdokumentti.
11	Luovutuksen vahvistaminen	Luovuttajan sähköinen allekirjoitus

Luovutettavat tiedot

	Luovutettavat tiedot	
Nro	Tieto	Selite
1	Tiedon yksilöinti	Yksilöinnissä käytetään apuna asiakirjan OID-tunnusta Asiakirjan tyyppi (luokitus) Nimetään asiakirjan tyyppi, esimerkiksi – lähete – hoitopalaute – konsultaatiopyyntö – lääkemääräys – lausunto – todistus
2	Data	Luovutettavat tiedot ovat tyypillisesti potilasrekisteristä, työterveyshuollon rekisteristä laboratoriojärjestelmästä tai kuvantamisen tietojärjestelmistä poimittuja tietoja

10.6 Käyttöyhteydellä tapahtuva tietojen luovutus, www-selain

Tietojen luovutuksen yksi käytännössä esiintyvä (liite A) toteutustapa on se, että luovutuksen saajalle järjestetään selainyhteys luovuttavan rekisterinpitäjän tietojärjestelmään. Kuten aikaisemmin on todettu, ei toimintayksikön oman potilastietojärjestelmän käyttöoikeuksien jakaminen toimintayksikön ulkopuolelle ole oikea tapa toimia. Kaikissa tapauksissa tulee varmistaa, että selainkäyttäjä ei pysty saamaan käyttöönsä muiden kuin juuri sen potilaan tiedot, joihin hänellä on suostumuksen tai muun laista johtuvan syyn perusteella oikeus. Tämä voidaan toteuttaa esimerkiksi erillisellä "front-end" palvelimella, joka hallinnoi luovutuksen edellytyksiä, käyttäjien todentamista jne. tässä raportissa esitettyjen periaatteiden mukaisesti (kuva 8). Näitä ovat luovutuksen edellytysten tarkistamisen lisäksi mm.

- Lukujen 9.3-9.4 määritykset riittävästä suojauksesta ja suojaamismenetelmistä
- Luvun 10.2 -10.5 tietosisältömääritykset
- Jäljempänä esitetty suositus lokitiedon tietosisällöstä

Avoimessa verkossa tapahtuvassa www-selainkäytössä tulee kiinnittää erityistä huomiota osapuolten todentamiseen ja siirrettävän tiedon salaamiseen.

10.7 Puhelimitse tapahtuva tietojen luovutus

Puhelimitse tapahtuvassa tietojen luovutuksessa on tietojen luovuttajan varmistuttava luovutuksen edellytysten olemassaolosta yhtä huolellisesti kuin sähköisesti tapahtuvassa tietojen luovutuksessa. Käytännössä saattaa olla vaikeata varmistua kaikkien tiedon luovuttamisen edellytysten olemassaolosta. Siksi puhelimitse tapahtuvaa tietojen luovutusta ei suositella käytettäväksi kuin poikkeustapauksissa. Tällöinkin tulee osapuolten kyetä todentamaan toisensa luotettavasti.

11. Suositus luovutuslokin tietosisällöksi

Tietojen luovuttaja ja luovutuksen vastaanottaja pitävät kumpikin lokia tehdyistä luovutuspyynnöistä, tietojen luovutuksista ja luovutusten vastaanotoista.

Lokin tietosisällöksi suositellaan seuraavia tietoja:

	Lokitieto	
Nro	**Tieto**	**Selite**
1	Potilas	Henkilö, jonka hoitoa tietoja luovutuspyyntö tai luovutus sisältää - Nimi ja henkilötunnus
2	Luovuttaja	Toimintayksikkö, joka luovuttaa potilaan tiedot - Toimintayksikön nimi ja OID-koodi - Itsenäinen ammatinharjoittajan nimi ja tunnistetiedot
3	Luovutuksen pyytäjä	Ammattihenkilö, joka pyytää potilaan tietoja luovutettavaksi. - henkilötiedot, toimintayksikkö ja tehtävä toimintayksikössä. Luovutuksen pyytäjä voi olla myös muu organisaatio (esim. vakuutuslaitos, Kela, Stakes, Lääninhallitus)
4	Luovutuksen saaja	Terveydenhuollon toimintayksikkö, johon tiedot lähetetään Toimintayksikön nimi ja OID-koodi Muu organisaatio tai viranomainen , nimi ja OID-koodi Potilas (nimi ja henkilötunnus)
5	Luovutuksen pyytäjän asiallinen yhteys potilaaseen	Selvitys luovutuksen pyytäjän ja potilaan hoitosuhteesta tai muusta asiayhteydestä kun kyseessä on luovutuspyyntöön perustuva luovutus Selvitys luovuttajan ja potilaan hoitosuhteesta tai muusta asiayhteydestä kun kyseessä on luovutus ilman luovutuspyyntöä
7	Luovutettavien tietojen käyttötarkoitus	Selvitys käyttötarkoituksesta, johon luovutuksen pyytäjä pyytää tietoja luovutettaviksi Luovuttajan määrittämä käyttötarkoitus silloin kun luovutuspyyntöä ei ole
8	Luovutukseen sisältyneet asiakirjat	Yksilöidään luovutettavat asiakirjat .Yksilöinnissä käytetään asiakirjan OID-tunnusta Viite luovutettuihin asiakirjoihin Kunkin asiakirjan rekisterinpitäjä tunniste (nimi ja OID-koodi) Kunkin asiakirjan sensitiivisyys (luokitus) ja erityissuojausluokka
9	Luovutuksen ajankohta	Luovutuksen päivämäärä
10	Luovutuksen peruste	Selvitys luovutuksen perusteesta. Se voi olla suostumus, kokeilulaissa mainittu sopimus tai muu laissa mainittu luovutuksen peruste. - Luovutuksen perusteena olevan suostumusdokumentin yksilöinti (OID tunnuksella)
11	Erityistilanteet	Selvitys - luovutuspyynnön hylkäämisestä - luovutuspyynnön peruuttamisesta - Luovutuksen hylkäyksestä - Luovutuksen peruutuksesta - Luovutettujen tietojen korjauksesta
12	Lokitiedon tekoaika	Aikaleima
13	Lokitiedon varmentaminen	Sähköinen allekirjoitus

12. Jatkotoimet

Projektin tekemät haastattelut (ks. liite A) osoittivat, että hoitotietojen sähköinen luovuttaminen terveydenhuollossa on vasta vähitellen kehittymässä oleva käytäntö. On odotettavissa, että sähköisten potilaskertomusten yleistyminen, kansalliset käsite-, ydintieto- ja sanomamääritykset samoin kuin uusien toimintamallien yleistyminen (mm. hoito- ja palveluketjut sekä jaettu hoitovastuu) tulevat lisäämään toimintayksiköiden välistä hoitotietojen luovutusta. Myöskin potilaan mahdollisuus valita hänelle parhaiten sopiva toimipiste seutukunnan tai yhteistoiminta-alueen sisällä edellyttää nykyistä laajempaa tietojen siirtoa.

Nykyisellään tietojen luovuttaminen on kytköksissä toimintayksikköön. Toisaalta on sekä syntymässä että jo toiminnassa varsin suuria toimintayksikköjä (esim. sairaanhoitopiiri voi päättää, että se omat toimintayksiköt ja sairaalat muodostavat yhden toimintayksikön). Kainuun maakuntakokeilulaki mahdollistaa maantieteellisesti suuria toimintayksiköitä. Nykysäädösten perusteella ei potilaalta tarvitse pyytää suostumusta tietojen käyttöön toimintayksikön sisällä. Toimintayksikkö myös päättää, ketkä sen ammattihenkilöistä osallistuvat hoitoon ja ketkä ovat sivullisia. Edelleen potilaalla ei ole tarkistusoikeutta tietojen käyttö- eikä luovutuslokeihin. Kun tähän kokonaisuuteen lisätään se, että joidenkin asiatuntijoiden taholta on tuotu esille toive laajentaa potilaslain 13 §3 käyttöä muihinkin tarkoituksiin kuin jatkohoidon järjestämisen ja tutkimusten tilaamiseen, on potilaan asema itsemääräämisoikeuden käytön ja yksityisyyden suojan osalta epätyydyttävä.

Suositukset jatkotoimiksi

1. Tämän raportin ehdotukset luovutuspyyntö- ja luovutussanomista sekä lokitiedoista samoin kuin niiden tietosisällöstä tulee ottaa käyttöön.

2. Tässä raportissa ehdotetut luovutuspyynnön ja luovutuksen kuvailutiedot tulee standardisoida valtakunnallisella tasolla.

3. Tässä raportissa ehdotetut uudet koodistot tulee sekä kehittää että ottaa käyttöön valtakunnallisesti. Koodistoja tarvitaan mm. rekisterinpitäjälle, erillään pidettäville rekisterille, asiayhteydelle, tietojen käyttötarkoitukselle ja luovutuksen perusteelle.

4. Potilasasiakirjojen kuvailutietoihin (metatiedot) tulisi sisältyä sekä tieto niiden rekisterinpitäjästä, tietojen sensitiivisyydestä että mahdollisesta erillään pidosta.

5. Ehdotetut suojaustoimet tietojen luovutuksessa tulee ottaa käyttöön.

6. Hoito tulee suunnitella yhteistyössä potilaan kanssa ja siinä yhteydessä potilaalle tulee informoida kuka, miksi, miten, milloin ja mihin tarkoitukseen hänen tietojaan luovutetaan. Henkilötietolain 24 §:n edellyttämä informointi tulee toteuttaa. Luovutuksesta jaettava informaatio olisi hyvä toteuttaa samanaikaisesti suostumuksesta informoinnin kanssa.

7. Nykyisellään terveydenhuollon potilaalla ei ole henkilötietolain perustella tarkistusoikeutta omien hoitotietojensa katselua ja käyttöä koskeviin lokitietoihin. Eri asia on,

että julkisuuslain perusteella potilaalle voi syntyä tiedonsaantioikeus silloin, kun hän on asianosaisena esimerkiksi tutkittaessa epäilyä tietojen rikollisesta luovutuksesta.

Tehdyn selvityksen mukaan (liite A) käytössä olevat potilastietojärjestelmät eivät kykene varmistamaan tyydyttävästi luovutuksen pyytäjän ja potilaan välistä asiayhteyttä. Potilaalle tulisi kuitenkin turvata oikeus tietää, kuka on luovuttanut hänen tietojaan, milloin, mihin tarkoitukseen ja kenelle.

Esitetään, että kansalaisen ja potilaan asemaa vahvistetaan antamalla hänelle oikeus tietojen luovutuslokin tarkistamiseen. Luovutuslokin tarkastamiseen pitää suunnitella toimintamalli, jolla varmistetaan, että potilaalla on tarvittaessa myös yhdessä ammattihenkilön kanssa mahdollisuus käydä läpi luovutuslokin sisältö. Tietoteknisesti tällainen tarkistaminen voi tapahtua turvallisesti esimerkiksi www-selaimella, kun käytetään vahvaa potilaan tunnistamista ja tietoyhteyden salaamista.

8. Lainsäädäntöä tulisi kehittää siten, että tietojen luovutus ei ole kytketty toimintayksikköön. Ehdotetaan, että selvitetään miten jatkossa luovutus (samoin kuin suostumus, vrt. suostumusraportti) voidaan toimintayksikön asemesta kytkeä tiedon käyttötarkoituksen ja suojaustarpeisiin.

9. Lausuntokierroksen tuloksena useissa kommenteissa esitettiin kysymyksiä käyttöoikeuksien hallinnasta sekä rekisterinpitäjän tietojärjestelmän sisällä että niiden kesken tapahtuvassa tiedonvaihdossa. Erityisesti ns. alueellisesta käyttöoikeuksien hallinnasta on tarpeen laatia erillinen suositus.

LIITTEET

A. TIETOJEN SÄHKÖISEN LUOVUTUKSEN NYKYTILANNE

1. Nykytilanne luovutusten ja lokitietojen käsittelyn osalta

1.1 Kartoitus

Luovutusten ja lokitietojen hallinnan suositusten laatimisen yhteydessä suoritettiin kartoitus vallitsevista käytännöistä haastattelemalla potilastietojärjestelmiä kehittäviä yrityksiä ja niitä käyttäviä organisaatioita.

Kartoitettuja järjestelmiä olivat mm. (suluissa yritys tai asiakasorganisaatio):

- Effica (TietoEnator)
- Pegasos (Helsingin terveysvirasto)
- Oberon ja Miranda (MediciData)
- Mediatri (MediConsult)
- Doctorex, HealthNet (Mehiläinen, Doctorex)
- Navitas (Elisa)
- Fiale (Atkos)
- Terveystili (WM-Data Novo)
- Agfan kuva-arkisto (Agfa)

Luovutuksen toteutukselle esiintyi useita erilaisia ratkaisutapoja, joita on kuvattu jatkossa toiminnallisella tasolla.

1.2 Yleiset havainnot

Kartoituksen perusteella voitiin muodostaa seuraavia yleistettyjä johtopäätöksiä tietojen sähköisen luovutuksen nykytilasta:

- Tietojen luovutus sähköisesti on vielä verrattain vähäistä.
- Yhtenä esteenä on ollut mm. hankalina ja vaikeaselkoisina koetut tietosuojamääräykset.
- Käytännössä luovutusta pyytävän ammattihenkilön ja pyynnön kohteena olevan potilaan välillä olevan hoitosuhteen tai muun asiallisen yhteyden toteaminen on tietojärjestelmien avulla vaikeata.
- Käyttäjänhallinnan toteutuksissa olisi myös runsaasti parantamisen varaa. Käyttäjätunnuksiin ja salasanoihin perustuva tunnistaminen ja todentaminen saattaa olla liian helppo murtaa.
- Käyttäjien profiiliin perustuva käyttöoikeuksien luokittelu vaatii tietojen luokittelua. Esimerkiksi mitä tietoja lääkäri, hoitaja, sosiaalityöntekijä tai kotipalvelutyöntekijä saavat katsoa osallistuessaan potilaan kotona tapahtuvaan hoitoon. Tästä on tarpeen käynnistää jatkokehitysprojekti.

1.3 Tiedon siirto "Leikkaa-Liimaa" menetelmällä näytöltä toiselle

Teknisesti pelkistetty toteutuksena esiintyi menetelmä katsella luovutettavia tietoja luovuttavasta järjestelmästä, leikata tarpeelliset tiedot leikepöydälle ja liimata ne vastaanottavaan järjestelmään. Tätä tekniikkaa käytetään mm. lähetteen tekemisessä ja hoitotietojen liittämisessä lähetteeseen.

Käyttöoikeuksilla ja käyttöliittymällä voidaan toimintayksikön sisällä rajata näkyviä tietoja vain luovutuksen kannalta tarpeellisiin. Haasteina ovat mm. potilaan informointi, suostumuksen pyytäminen ja luovutettavien tietojen yksilöinti.

1.4 Käyttöoikeuksien jakaminen

Lähtökohtana on toimintayksikkökohtaiset potilasrekisterit, jotka voivat sijaita fyysisesti eri laitteistolla tai samalla laitteistolla, mutta loogisesti erillään. Tässä ratkaisussa tietojen luovutus on järjestetty siten, että käyttäjät voivat käyttöoikeuksiensa puitteissa katsoa potilaan tietoa toistensa rekistereistä potilaan antaman suostumuksen nojalla.

Toteutuksen tekniikoita tuli esille useista. Näitä olivat mm.

- Tietojärjestelmät ovat erilliset ja käyttäjän työpöydälle avautuvat erilliset ikkunat kumpaankin järjestelmään
- Tietojärjestelmä on yhteinen, tietokannat ovat erilliset ja työpöydälle avautuvat erilliset ikkunat. Eri rekistereiden potilastietojen katselun on toteutettu käyttäjätunnuksella ja salasanalla. Sisäänkirjautumisen yhteydessä selvitetään yleensä toimintayksikkö ja käyttäjärooli. Käyttäjärooli määrää, mitä tietoja voi katsella eli luovutuksen saaja saa vain tarpeelliset tiedot.

Haasteina ovat mm:

- Katselijan eli luovutuksen saajan asiallisen yhteyden selvittäminen potilaan suhteen
- Käyttöoikeuksien rajaaminen vain kyseisen potilaan tietoihin ja siinäkin vain työtehtävien hoitamisen kannalta tarpeellisiin tietoihin
- Potilaan tiedustellessa puhelimitse tietojaan, jotka ovat toisessa järjestelmässä on kyseessä luovutus joka vaatisi suostumuksen. Puhelimessa tapahtuva suostumuksen laatiminen on ongelmallista samoin kuin potilaan informointi. Lisäksi tulisi voida varmistaa, että suullista suostumusta käytetään vain potilaslaissa määriteltyihin tarkoituksiin.

1.5 Pyyntö- ja vastaussanomien välittäminen rekistereiden välillä

Tässä toteutuksessa lähtökohtana olivat toimintayksikkökohtaiset rekisterit ja niiden välille järjestetty sanomaliikenne. Luovutuspyynnön kohteena olevia tietoja ovat tyypillisesti kertomustiedot, lausunnot, todistukset jne. Hyvin usein luovutuspyyntö ja luovutus tapahtuvat vielä paperimuodossa. Haasteena on tässäkin selvittää luovutuspyynnön esittäjän asiallinen yhteys potilaaseen.

Ilman luovutuspyyntöä luovutettavat tiedot olivat lähete, hoitopalaute, konsultaatiopyyntö ja siihen vastaus.

Tietosuojan kannalta hankalana käytäntönä voidaan pitää sitä, että jo siinä vaiheessa kun potilas tulee vastaanotolle tai kun hänet kirjoitetaan sisään sairaalaan häneltä pyydetään suostumus hoitopalautteen lähettämiseen lähettäjälle. Oikea käytäntö on pyytää suostumus hoitopalautteen lähettämiseen vasta käynnin tai osastohoitojakson päättyessä, jolloin potilas tietää, mitä tietoa ollaan lähettämässä.

1.6 Tietojen katselu viitetietojärjestelmän avulla

Tässä ratkaisussa perusjärjestelmät muodostavat potilaan tiedoista viitetietoja aluetietojärjestelmään. Viitteen avulla voidaan katsoa potilasta koskevaa tietoa. Viitteiden ja viitteen osoittaman sisällön katsominen on potilastiedon luovutusta ja vaatii potilaan suostumuksen.

Haasteena on viitteen sopivan karkeusasteen löytäminen, jotta lääkäri löytäisi hakemansa oleellisen tiedon nopeasti ja toisaalta, jotta potilas voisi antaa suostumuksensa riittävän tarkalla tasolla.

Toinen haaste liittyy suostumusprosessiin. Tätä ongelmaa on käsitelty tarkemmin suostumusraportissa.

1.7 Palveluketjusuunnitelman laatiminen

Palveluketjusuunnitelman laatimisen yhteydessä hankitaan potilaalta suostumukset siihen, että palveluketjun osapuolet voivat katsoa häntä koskevia tietoja palveluketjun toteuttamiseksi. Haasteena on se, että suunnitelmaan osallistuvien osapuolten tulee olla läsnä suunnitelmaa laadittaessa ja suostumusta pyydettäessä. Suostumusta tietojen luovuttamiseen ei tule pyytää toisen toimintayksikön puolesta.

Erikseen tulee pohtia, onko mahdollista, että palveluketjuun osallistuvat toimintayksiköt sopivat etukäteen yhteisesti potilaalle tehtävästä palveluketjusta ja siihen liitettävistä osapuolista sekä laativat ehdotuksen näiden välisestä tietojenvaihdosta, jonka potilas voisi hyväksyä yhdellä kertaa.

1.8 Puhelinneuvonta

Puhelinneuvonta on yleistymässä oleva palvelumuoto. Puhelinneuvontaan liittyä tietojen luovutus muodostaa oman haasteensa. Haastatteluissa nousi esiin mm. seuraavia luovutukseen liittyviä kysymyksiä:

- Voiko puhelinneuvoja mennä katsomaan potilaan tietoja perusjärjestelmästä?
- Onko puhelinneuvojalla ja milloin hoitosuhde neuvoa kysyvään potilaaseen?
- Miten toteutetaan potilaan suullisen suostumuksen edellyttämä informointi, suostumuksen dokumentointi ja todentaminen?
- Miten rajataan neuvojan käyttöoikeudet ainoastaan kyseiseen potilaaseen ja ainoastaan tarpeellisiin tietoihin?

B. TARVITTAVAT UUDET LUOKITUKSET

1. Luokitusten tarve

Sähköisissä suostumuksissa ja luovutuksissa on tarve ilmaista erilaisia asioita sekä käyttäjien että sovellusten ymmärtämällä tavalla. Tähän tarkoitukseen on tarpeen kehittää kutakin ilmaistavaa käsitettä varten luokitus. Luokituksessa kerrotaan, mikä on luokiteltava asia, ja mitä arvoja se voi saada.

2. Luokiteltavia asioita

Suostumuksen ja luovutuksen yhteydessä tarvitaan mm. seuraavia luokituksia:

- Tietorakenteiden luokittelu
- Luovutettavien tietojen rajausta tukevat luokitukset kuten käyttötarkoitus, asiayhteys, rekisterinpitäjä, erityissuojaustarve ja tietojen sensitiivisyys.
- Ajanjaksojen ilmaisemiseen liittyvät luokitukset. Esimerkiksi on tarpeen voida ilmoittaa, että suostumus on voimassa meneillään olevan hoitojakson ajan.
- Rajausten ilmaisemisessa on tarvetta myös ns. kielteisen ilmaisun käyttöön, esimerkiksi "kaikki tiedot paitsi" -tyyppisesti voidaan antaa suostumus kaikkia muita hoitojaksoja paitsi viimeisintä koskeviin tietoihin. Tämä edellyttää tietorakenteisiin perustuvaa yksilöintiä.

3. Luokitusten kehittäminen

Luokitusten kehittäminen kannattaa kytkeä Stakesin koodistopalvelin-hankkeen yhteyteen.

C. KESKEISET LAIT, ASETUKSET JA OPPAAT

Sosiaali- ja terveydenhuollon tietojen käsittelyä ohjataan mm. seuraavilla lailla ja ohjeistuksilla:

Henkilötietolaki (HeTiL)

- Laki 1999/523.

Laki terveydenhuollon ammattihenkilöistä

- Laki 559/1994

Kokeilulaki

- Laki sosiaali- ja terveydenhuollon saumattoman palveluketjun ja sosiaaliturvakortin kokeilusta 22.9.2000/811. Lain voimassaoloa on jatkettu vuoden 2005 loppuun saakka ja samalla sitä on tarkistettu. Uutena asiana on mm. säädetty sähköisestä tunnistamisesta ja allekirjoittamisesta. Laki 19.12.2003/1225.

Potilaslaki (PotL)

- Laki potilaan asemasta ja oikeuksista 1.8.1992/785.

Potilasasiakirja-asetus (PotA)

- Sosiaali- ja terveysministeriön asetus potilasasiakirjojen laatimisesta sekä niiden ja muun hoitoon liittyvän materiaalin säilyttämisestä 99/2001. Asetuksessa annetaan yksityiskohtaisia määräyksiä potilastietojen käsittelystä ja luovuttamisesta. Sen liitteessä on myös määräykset eri asiakirjojen säilytysajoista.

Potilasasiakirjaopas

- Potilasasiakirjojen laatiminen sekä niiden ja muun hoitoon liittyvän materiaalin säilyttäminen, Opas terveydenhuollon henkilöstölle, Sosiaali- ja terveysministeriö, Oppaita 2001:3.

Sähköinen resepti asetus

- Sähköisen reseptin käytöstä säädetään STM:n asetuksella. Asetus 771/2003 sähköisen lääkemääräyksen kokeilusta.

D. KESKEISET KÄSITTEET

Aluetietojärjestelmä

Aluetietojärjestelmä on yleisluonteinen nimitys saumattoman palveluketjun kokeilulakiin perustuvalle, alueellisten sähköisten palveluiden kokonaisuudelle, jota eri yritykset toteuttavat. Aluetietojärjestelmän palvelukokonaisuus sisältää minimissään käyttäjien ja käyttöoikeuksien hallinnan, koodistojen hallinnan, viitetietokannan, palveluketjujen hallinnan, suostumusten hallinnan ja lokitiedot. Aluetietojärjestelmä voidaan laajentaa sisältämään myös muita sähköisiä palveluita, kuten konsultointi ja sähköinen kuvaarkisto. Kokeilulakialueet (HUS, Pirkanmaa ja Satakunta) ovat yhteistyössä teettäneet Aluearkkitehtuuri 2002 määrittelyn, jossa laajemmin kuvataan aluearkkitehtuuriin perustuvan aluetietojärjestelmän toiminnallisuutta ja palveluita.

Toimintayksiköiden käytössä olevat perusjärjestelmät tuottavat toimintayksikkökohtaisesti viitetiedot viitetietokantaan HL7-yhdistyksen määrittelemien avoimien rajapintojen mukaisesti ns. adaptereiden avulla.

Aluetietojärjestelmän käyttäjinä voivat olla sosiaali- ja terveydenhuollon ammattilaiset ja asiakkaat.

Potilas/asiakas

Potilaalla tarkoitetaan potilaslaissa terveyden- ja sairaanhoitopalveluja käyttävää tai muuten niiden kohteena olevaa henkilöä (Potilaslaki 2&).

Asiakas on kokeilulaissa (3 § 1 kohta) määritelty potilaslain mukaisesti. Asiakkaalla tarkoitetaan terveyden- ja sairaanhoitopalveluja käyttävää tai muuten niiden kohteena olevaa henkilöä taikka sosiaalihuollon asiakkaan asemasta ja oikeuksista annetussa laissa tarkoitettua asiakasta sekä muun sosiaaliturvan hakijaa tai saajaa

Palveluntuottajan näkökulmasta terveydenhuollon asiakkaita ovat todelliset asiakkaat ja lainsäädännön perusteella terveydenhuollon palvelun kohteena olevat henkilöt.

(Samoin palvelun tuottajan näkökulmasta asiakkaita ovat palvelun maksajat kuten kunta, kuntayhtymä, valtio, vakuutusyhtiö tai yksityiset säätiöt, mutta tämä asiakkuusnäkökulma ei koske tätä suositusta.)

Ks. Hoitosuhde tai muu asiallinen yhteys

Asiakkaan ongelma

Asiakkaan ongelma ilmaisee asiakkaan tarpeen saada palveluja ja kuvaa, miksi asiakas hakee, tarvitsee tai saa palveluja. Ongelma voi palveluketjun edetessä muuttua. Rekisterinpitäjän näkökulmasta tarkasteltuna asiakkaan ongelma kuvastaa myös asiakkaan ongelman poistamiseksi tarvittavien palveluiden kokonaisuutta (esim. vatsavaiva, päänsärky, alkoholismi, diabetes).

Henkilörekisteri

Henkilörekisterillä tarkoitetaan käyttötarkoituksensa vuoksi yhteenkuuluvista merkinnöistä muodostuvaa, henkilötietoja sisältävää tietojoukkoa. Henkilörekisteriä käsitellään osin tai kokonaan automaattisen tietojenkäsittelyn avulla, tai se on järjestetty kortistoksi, luetteloksi tai muulla näihin verrattavalla tavalla siten, että tiettyä henkilöä koskevat tiedot voidaan löytää helposti ja ilman kohtuuttomia kustannuksia (HetiL 3.1 kohta 3).

Henkilörekisterin käyttötarkoitus tulee määritellä siten, että siitä ilmenee, minkälaisten rekisterinpitäjän tehtävien hoitamiseksi henkilötietoja käsitellään. Esim. terveydenhuollossa eri käyttötarkoitus on yleisen terveydenhuollon ja sairaanhoidon toteutuksen yhteydessä ylläpidettävällä rekisterillä kuin työterveyshuollon toteuttamiseksi pidettävällä rekisterillä. Sosiaalitoimessa eri tehtäviä ovat mm. lastensuojelu, päivähoito, kasvatus- ja perheneuvonta, toimeentulotukiasiat, vanhustenhuolto sekä kotipalvelu, minkä vuoksi ne vaativat oman henkilörekisterin.

Eri käyttötarkoituksiin perustettujen rekistereiden välillä noudatetaan tavanomaisia henkilötietolain mukaisia luovutusedellytyksiä.

Hoitosuhde tai muu asiallinen yhteys

Hoitosuhde on terveydenhuollossa suhteellisen vakiintunut käsite. Hoitosuhde on tiettyyn palveluvastuuseen tai hoitotilanteeseen liittyvä sosiaali- ja terveydenhuollon ammattihenkilön ja yksilöasiakkaan luottamuksellinen vuorovaikutussuhde.

Henkilötietolain kannalta asiakassuhde syntyy ja oikeus tietojen tallettamiseen muodostuu silloin, kun asiakas hakeutuu tai tulee palveluntuottajan (rekisterinpitäjä) asiakkaaksi, ts. asiallinen yhteys ko. palveluntuottajaan syntyy.

Tietojärjestelmien kannalta impulssi hoitosuhteen alkamisesta on esim. se, kun asiakas ilmoittautuu hoitoon ja ilmoittautuminen on kirjattu järjestelmään. Muu asiallinen yhteys syntyy esim. silloin, kun

- lähete on saapunut organisaatioon; lähete on kirjattu järjestelmään tai hoitoaika on annettu ja se on kirjattu järjestelmään,
- asiakas on ottanut yhteyttä hoidonvarausta tai ajanvarausta tai muuta syytä varten: hoitoaika on annettu ja ajanvaraus on tehty järjestelmään,
- asiakas hakee todistuksen terveydentilastaan jonkin etuuden hakemiseksi.

Hoitosuhde päättyy vastaavasti esim. kun

- asiakas on kirjattu ulos vuodeosastolta ja kaikki hoitojaksoa koskevat tiedot on käsitelty,
- kaikki vastaanottokäyntiä koskevat tiedot on käsitelty.

Hoitosuhde alkaa myös kun esim. ensihoitotilanteessa asiakkaalle on hälytetty ensihoidon yksikkö paikalle antamaan asiakkaalle ensiapua.

Hoitotiedot

Hoitotieto on terveydenhuollossa suhteellisen vakiintunut käsite. Hoitotiedot tarkoittavat asiakkaasta terveydenhuollon toimintayksiköissä kerättyjä asiakaskohtaisia, hoidon järjestämiseen, suunnitteluun, toteutukseen ja seurantaan liittyviä tietoja, jotka merkitään arkistoitavaan potilaskertomukseen. Sähköisessä tietojenkäsittelyssä tiedot kerätään potilaskertomusjärjestelmiin.

Jatkohoito

Jatkohoidolla tarkoitetaan potilaslain 13 §:n mukaan hoidon järjestämistilannetta, jossa asiakas suostumuksensa mukaisesti lähetetään samaan sairauteen/ongelmaan liittyen välittömästi tai erikseen määritellyllä tavalla toteutettuna toiseen toimintayksikköön.

Lain mukaan jatkohoidon järjestämistilanteessa riittää suullinen, potilasasiakirjaan merkitty suostumus.

Jatkohoidolla ei tarkoiteta tilannetta, jossa asiakas menee sovitusti muussa asiassa tai erillisessä sairaustilanteessa toiseen toimintayksikköön eikä tilanteetta, jossa kysymys ei ole sovitusta jatkohoidosta toiseen toimintayksikköön.

OID-tunnus

Tietojärjestelmien yhteistoiminnallisuus vaatii kohteiden yksikäsitteisen tunnistamisen. Siksi tietojärjestelmiltä tullaan edellyttämään jatkossa valmiutta yksilöidä sovitut kohteet yksiselitteisesti riippumatta siitä, kenen rekisterinpitäjän käytössä järjestelmä on tai kenen toimittajan toteuttama se on. Yksilöitäviä kohteita ovat mm. toimipaikat, henkilöt ja potilasasiakirjat (esim. suostumus) sekä koodistot.

Sosiaali- ja terveydenhuollon alueellisissa tietojärjestelmäratkaisuissa suositellaan OID-koodiston käyttöä yksilöinnissä. OID-järjestelmän avulla yksilöidään vastuutaho sekä vastuutahon hallitsemat kohteet. Vastuutahot eli rekisterinpitäjät laativat, ylläpitävät ja julkaisevat muille osapuolille tietojen vaihdossa käyttämänsä koodiluettelot. Luettelot tullaan julkaisemaan Stakesin hallitseman valtakunnallisen koodistopalvelun kautta.

Yksityiskohtaiset, valtakunnalliset ohjeistukset ja pysyvä toimintamalli syntyvät v. 2004 aikana saumattomien palveluketjujen ja sähköisen reseptin kokeilualueilla pilotoinneista saatavista kokemuksista. Stakes valmistelee ohjeistuksen.

Yksilöinnin periaatteet on kerrottu mm. Osaavien keskusten verkoston julkaisussa 'Selvitys asiakas- ja potilasasiakirjojen sähköisestä säilytyksestä ja kiistämättömyydestä'. Yksityiskohtaiset määritykset tietojärjestelmille implementointia varten on kuvattu 'Avoimet Rajapinnat'- ja 'OpenCDA-projektien' määrityksissä (HL7 Finland ry).

Palvelu

Palvelu on terveydenhuollossa suhteellisen vakiintunut käsite. Palvelulla tarkoitetaan sosiaali- ja terveydenhuollon organisoidun toiminnan tuloksena syntyvää hyödykettä, joka on tarkoitettu asiakkaiden tarpeiden tyydyttämiseksi.

Palveluketju

Saumattomalla palveluketjulla tarkoitetaan kokeilulain (3 § 2 kohta) mukaan ”toimintamallia, jossa asiakkaan sosiaali- ja terveydenhuollon ja muun sosiaaliturvan asiakokonaisuuteen liittyvät palvelutapahtumat yhdistyvät asiakaslähtöiseksi ja joustavaksi kokonaisuudeksi riippumatta siitä, mikä toiminnallinen yksikkö on palvelujen järjestäjä tai toteuttaja”.

Saumaton palveluketju on tiettyyn ongelmakokonaisuuteen kohdistuva, suunnitelmallinen ja yksilöllisesti toteutuva palveluprosessien kokonaisuus. Se voi olla myös sosiaali- ja terveydenhuollon rajat ylittävä. Palveluketju voi olla suunnitteilla, avoin tai päättynyt. Palveluketjulla on tunnus (Koodi), johon palvelutapahtumat liitetään.

Rekisterinpitäjä, toimintayksikkö

Potilaslain 2 §:ssä määritellyt terveydenhuollon toimintayksiköt ja ammatinharjoittajat, joiden käyttöä varten potilasrekisterit perustetaan ja joilla on oikeus määrätä rekistereistä, ovat henkilörekisterilain tarkoittamia rekisterinpitäjiä. Terveydenhuollon toimintayksiköitä, eli rekisterinpitäjiä ovat esimerkiksi: terveyskeskus, sairaanhoitopiirin toimintayksiköt, työterveyshuollon toimintayksikkö ja yksityisen terveydenhuollon palvelujen tuottaja (esim. lääkäriasema).

Kunnan sosiaalitoimessa rekisterinpidon hallinnollinen vastuu on ao. lautakunnalla. Lautakunnan tehtävänä on määritellä tehtävien organisoinnin ja henkilörekistereiden eri käyttötarkoitusten perusteella toiminnalliset rekisterinpidon vastuut.

Yksityisessä sosiaalitoimessa rekisterinpitäjä on ao. itsenäinen toimintayksikkö tai itsenäinen ammatinharjoittaja.

Kun yksityinen sosiaalitoimen tai terveydenhuollon toimintayksikkö toimii julkisen sektorin toimintayksikön lukuun, ao. palvelut ostanut julkisen sektorin toimintayksikkö on ko. yksityisessä toimintayksikössä kertyvien asiakaskohtaisten hoitotietojen rekisterinpitäjä. Yksityinen toimintayksikkö toimii sopimusvastuussa, minkä vuoksi sopimuksessa on tarkoin määriteltävä hoitotietojen käsittelyyn liittyvät tehtävät ja vastuut esim. suostumusten hallinnan osalta.

Suostumus

Suostumuksella tarkoitetaan henkilötietolain (3 § 7 kohta) mukaan kaikenlaista vapaaehtoista, yksilöityä, informoitua ja tietoista tahdonilmaisua, jolla rekisteröity hyväksyy henkilötietojensa käsittelyn. Suostumuksesta tulee ilmetä, kuka suostumuksen antaa, se toimintayksikkö/ammattihenkilö/ammatinharjoittaja, joka tietoja luovuttaa, mille toimintayksikölle/ammatinharjoittajalle tietoja luovutetaan, mitä tietoja luovutetaan ja mitä käyttötarkoitusta varten. Suostumuksen sisältämät tiedot pitää aina yksilöidä asianmukaisella tasolla, eikä ns. avointa suostumusta voida käyttää.

Tietojen käyttö

Tietojen käytöllä tarkoitetaan henkilötietolain (3 § 2 kohta ja 7 §) mukaan terveys- ja potilaskertomustietojen käyttöä rekisterinpitäjän omassa sisäisessä toiminnassa.

Tietojen luovutus

Tietojen luovutuksella tarkoitetaan henkilötietolain (3 § 2 kohta) mukaan terveys- ja potilaskertomustietojen vaihtoa kahden tai useamman eri rekisterinpitäjän välillä. Tässä suosituksessa otetaan lisäksi huomioon potilaslain 13 §:n mukaiset tietojen antamisedellytykset terveydenhuollossa. Tietojen luovutusta voi tapahtua lainsäädännön perusteella kahdella eri tavalla

- suostumuksella tapahtuva asiakaskohtaisen tiedon luovutus

- ilman suostumusta tapahtuva asiakaskohtaisen tiedon luovutus

Tietoturvallinen kommunikaatioalusta

Tietoturvallinen kommunikaatioalusta sisältyy Kansallisen terveydenhuoltoprojektin osahankkeeseen 4.1.3, Valtakunnallisen sähköisen sairauskertomuksen käyttöönotto yhtenä osa-alueena, jota Stakes koordinoi. Tämän työn tuloksena syntyvät seuraavat toiminnalliset suositukset mm. alueiden käyttöön toimintamallien kehittämistä varten sekä yrityksille tuotekehitystä varten:

- sähköisen suostumuksen periaatteet
- PKI-järjestelmä: Todentaminen ja varmentaminen
- luovutuksen periaatteet
- yksikäsitteiset tunnisteet
- sähköinen arkistointi
- lokitiedot
- sähköinen allekirjoitus
- perusstandardit

Viiteluettelo

Viiteluettelo on tietyin rajauksin (esim. asiakkaan viitetiedot) tehty lista viitetietokantaan talletetuista viitetiedoista.

Viitetieto

Viitetieto on kokeilulain (3 § 5 kohta) mukainen eksakti käsite. Viitetiedolla tarkoitetaan kyseisen lainkohdan mukaan tietoa siitä, ”että mainitussa sosiaali- ja terveydenhuollon toiminnallisen yksikön sähköisessä asiakasrekisterissä tai osarekisterissä on tiettynä ajankohtana talletettuna rekisterinpitäjän toiminnassa syntyneitä kyseessä olevaa asiakasta koskevia henkilötietoja”.

Viitetietona talletetaan viitetietokantaan asiakkaan nimi, henkilötunnus, tiedon sijaintipaikka, yleisluonteinen kuvaus viitetiedon osoittamasta tiedosta, viitetiedon tallettamisaika sekä viitetietokannan toiminnan edellyttämät tekniset tiedot.

Viitetiedon osoittama hoitotieto sisältää asiakkaan hoitotiedot kokonaisuudessaan esim. tehdyn laboratoriotutkimuksen nimi ja arvo, eikä sitä talleteta viitetietokantaan.

Viitetietokanta

Viitetietokannalla tarkoitetaan kokeilulain (3 § 6 kohta) mukaan ”viitetietojen ja niiden luovuttamista koskevien suostumusten muodostamaa sosiaali- tai terveydenhuollon asiakasrekisterin osarekisteriä, johon talletetaan myös lokitiedot”.

Viitetietokannan käyttötarkoituksena on asiakkaan saumattoman palveluketjun edistäminen nopeuttamalla asiakastietojen hakua ja luovuttamista sekä helpottamalla asiakkaan kokonaistilanteen hahmottamista. Viitetiedot luo ja tallettaa viitetietokantaan sekä luovuttaa ja muuten käsittelee järjestettäessä ja toteutettaessa kukin kokeilun piirin kuuluva sosiaali- tai terveydenhuollon rekisterinpitäjä omalta osaltaan. Näitä tehtäviä voidaan suorittaa myös kokeilun piiriin kuuluvan sosiaali- tai terveydenhuollon rekisterinpitäjän lukuun kirjallisen toimeksiantosopimuksen perusteella.

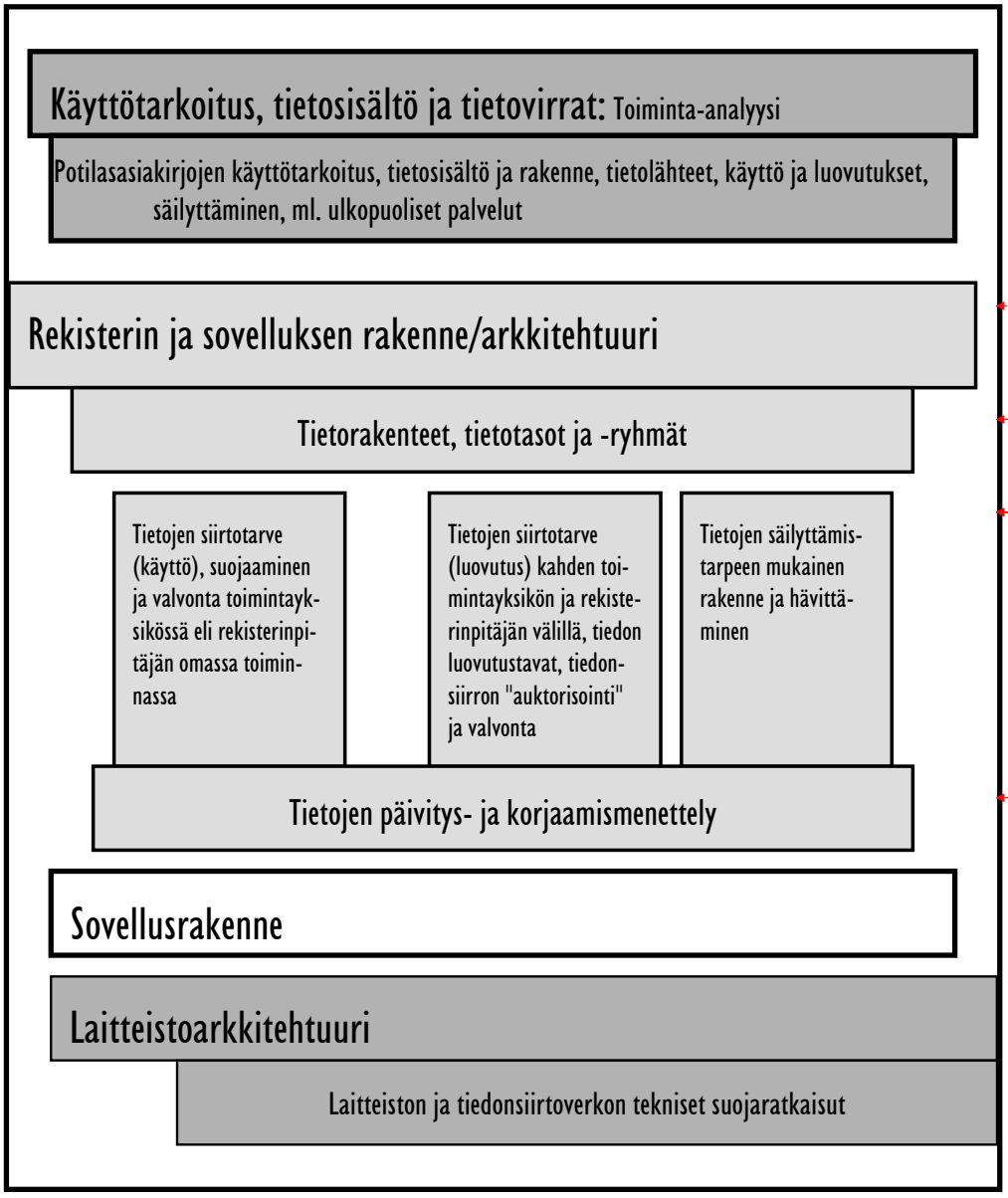
Viitetietokantaan talletetaan viitetiedot, mutta ei viitetiedon osoittamaa hoitotietoa.

E. LAUSUNTOKIERROKSEN YHTEYDESSÄ ESILLE NOUSSEITA KYSYMYKSIÄ

Esitetty näkemys/kysymys	**Tämän raportin vastaus/kommentti**
Kahdella tai useammalla sairaanhoitopiirillä ja tulevaisuudessa terveyskeskuksilla on yhteinen alueellinen tietojärjestelmä.	Lait ja asetukset eivät tunne rekisterinpitäjänä yhteisiä alueellisia tietojärjestelmiä
Alueellisessa tietojärjestelmässä kyse on alueellisesta kertomuksesta ja koko ajan samasta potilastietojärjestelmästä.	Potilaskertomusta pitää kukin toimintayksikkö (kts. 3.4.1) Juridisesti ei ole olemassa alueellista potilaskertomusta. Tietojärjestelmä voi sinänsä olla yhteinen, mutta toimintayksiköiden potilaskertomusten tulee olla erillisiä.
Alueellisessa tietojärjestelmässä tietoja ei siirretä eikä luovuteta vaan katsellaan. Kyse katseluoikeudesta, luovutus on kyseessä vain jos tieto siirtyy yhteisen-organisaation ulkopuolelle.	Toisen toimintayksikön tietojen kaikki käsittely, kuten katselu on luovuttamista myös ko. tietojärjestelmän sisällä.
Alueellinen tietojärjestelmä on sairaanhoitopiirien yhteinen organisaatio.	Yhteinen tietojärjestelmäorganisaatio ei muuta rekisterinpidon perusteita. Tällainen organisaatio ei ole rekisterinpitäjä., ellei lainsäädännössä toisin määrätä (esim. kokeilulait)
Suostumuksella tulisi eri organisaatioiden ammattihenkilöiden voida tutustua myös kokonaisuudessaan potilaan hoitoon liittyviin asioihin. (tavoite hoitokäytäntöjen yhtenäistäminen). Organisaatiot sopivat mitä tietoja potilaan luvalla voidaan siirtää. Suostumus hoitoketjulle tilatuille tutkimuksille tulisi olla eri rekisterinpitäjien ammattihenkilöiden käytössä.	Organisaatiolla tarkoitettaneen tässä toimintayksikköä. Toisen toimintayksikön ammattihenkilö voi käsitellä (käyttää) tietoja, jos siihen on potilaan suostumus tai muu laillinen peruste. Potilas päättää mitä tietoja hänen suostumuksellaan voidaan luovuttaa. Tietojen käsittelyyn perusteena on aina hoitosuhde tai muu asiallinen yhteys. Vain tarpeellinen tietoa saa käsitellä ja käsiteltävän tiedon salassapidosta on huolehdittava. Pitää huolehtia siitä etteivät sivulliset saa tietoja käyttöönsä. On huomattava myös mahdolliset eri käyttötarkoituksiin perustetut rekisterit tässä yhteydessä. Katso myös suostumusraportin määrittelyt.
Voidaanko hoitosuhde katsoa syntyvän koko rekisterinpitäjän hallussa oleviin tietoihin yhden lähetteen muodossa ?	Kyseessä on toimintayksikössä tapahtuva tietojen käsittely, kts. 1.4.1
Potilaskontaktissa tulee voida kirjata potilaan yleinen suostumus tietojärjestelmään.	Ei ole lainmukainen menettely
Milloin kyseessä on hoitosuhde ?	Hoitosuhteen ja muun asiallisen yhteyden selkeä määrittely tarvitaan valtakunnallisesti
Voidaanko tietoturvapolitiikka tarkistaa sopimusten yhteydessä ?	Se tulee tarkistaa sopimusten teon yhteydessä (vrt. henkilötietolain mukainen suunnitteluvelvollisuus)
Rekisterinpitäjä on usean sairaanhoitopiirin yhteistoimintayksikkö. Rekisterinpitäjäksi tulee sopia alueellisen tietokannan ja rekisterinpitäjän käsite. Toimipaikkana voisi toimia diagnostisen tiedon aluevarasto joka olisi potilastiedoista erillisiä re-	Tällaista yhteistoimintayksikköä ei potilaslaki tunne rekisterinpitäjänä. Rekisterinpitäjyys on sidottu perinteiseen .toimintayksikön määritelmään. Nämä varastot ovat osa kunkin toimintayksikön

kistereitä (sairaanhoitopiirin aluevarasto)	potilasrekisteriä
Aluetietojärjestelmä on tietojen luovuttaja	Tietojen luovuttaja on rekisterinpitäjä. Aluetietojärjestelmä ei ole rekisterinpitäjä, ellei sitä ole laissa erikseen säädetty.
Kokeilulain mukaisessa tietojärjestelmässä ei ole nähty tarpeelliseksi merkitä potilasasiakirjoihin luovutettujen tietojen alkuperää kuin siinä tapauksessa, että asiakastiedot kopioidaan suoraan .	Potilasasiakirja-asetuksen (PotA 21 §) merkinnät on tehtävät aina kun tietoja luovutetaan. On siis merkittävä kuka tiedot on luovuttanut. Merkinnät on tehtävä riippumatta siitä onko kyseessä osittainen vai kokonainen kopiointi. Asetuksen 7&:n mukaan merkinnät on tehtävä myös silloin, kun tietoa on saatu luovutuksella
Mikä on luovutussanoma aluetietojärjestelmässä	Luovutus tapahtuu ns. aluetietojärjestelmässä rekisterinpitäjien välillä. Aluetietojärjestelmä ei ole rekisterinpitäjä. Aluetietojärjestelmässäkin luovutus tapahtuu perusjärjestelmien välillä. Tässä raportissa aluetietojärjestelmälle ei ole esitetty omaa luovutussanomaa.
Rekisterinpitoon liittyvien toimeksiantosopimuksen yhteydessä ei ole kyse tietojen luovuttamisesta	Jos kyseessä on henkilötietojen käsittelyyn liittyvästä tai henkilötietojen käsittelyä sisältävästä toimeksiannosta, kysymys ei ole tietojen luovuttamisesta vaan tietojen antamisesta toimeksiantajan lukuun toimeksisaajalle. Jos kysymys on muusta toimeksiantosopimuksesta , kysymys on luovuttamisesta.
HeTiL 24 § mukaista informointipakettia ei tule kytkeä ajanvarauskirjeeseen. Tiedonantovelvoitteesta voidaan poiketa, jos asianomainen on jo saanut ko. tiedot	Suostumusraportti suosittelee mm. että ns. yleinen informaatio voidaan toimittaa esim. ajanvarauskirjeen mukana. Informointiin olisi hyvä synnyttää kansallisesti yhtenäinen malli.
Miksi suostumuksen rajaaminen on tarpeen, koska HeTiL 12 § ei sitä edellytä? Rajaaminen tulisi perustua potilaan ongelmaan.	Potilas käyttää suostumuksella itsemääräämisoikeuttaan. Voimassa oleva lainsäädäntö ei salli käytettävän "avointa valtakirjaa" vaan edellyttää nimenomaista suostumus (kts. suostumusraportti). Suostumus annetaan käyttötarkoitukseen, joka sinänsä merkitsee Tule myös ottaa huomioon käyttötarkoitussidonnaisuus, tarpeellisuusvaatimus ja yhteysvelvoite. Suostumuksella tarkoitetaan kaikenlaista, vapaaehtoista, yksilöityä ja tietoista tahdonilmaisua, jollaa rekisteröity hyväksyy henkilötietojensa käsittelyn (HeTiL 3&) Katso myös suostumusraportin suositukset.
Aluetietojärjestelmää käytettäessä käyttöoikeuksien hallinta ole pelkästään perustietojärjestelmien tehtävä.	Tarvitaan ohjeistus "alueellisen käyttäjänhallinnan periaatteista".
Voiko se, jolta luovutusta pyydetään luovuttaa myös niitä tietoja joita se on muilta saanut eikä ole tiedon alkuperäinen tallettaja vaan on saanut tiedot ilman edelleen luovutusoikeutta.	Lähtökohtaisesti ei niin kauan kun tietoja ei ole kirjattu potilasasiakirjoihin. Sen jälkeen, kun tiedot on kirjattu, niitä voidaan luovuttaa suostumuksesta riippuen potilaan hoitoa varten.

LIITE F HENKILÖTIETOJEN KÄSITTELYN KUVAUKSEN, LAINMUKAISUUDEN VARMISTAMISEN JA TEKNISEN TOTEUTUKSEN ERI VAIHEET JA ELEMENTIT



Muotoiltu: Tyyli1

Muotoiltu: Kuvan tekstit 16, Keskitetty

Muotoiltu: kuvateksti

Muotoiltu: kuvateksti

Muotoiltu: kuvateksti

Muotoiltu: Kuvan tekstit 16, Keskitetty

Kuva: Maija Kleemola, Tietosuojavaltuutetun toimisto

Käsittelyvaihe/vastuu	Kuvaa toiminta/tarpeet osatehtävittäin	Tekninen toteutus ja käytännön menettely osatehtävittäin - kuka tekee - mitä tekee	Määrittele ja varmista oik. edellytykset
Käyttötarkoitus			HetiL 3.1 § k3, 6 §, TTL
Rekisterinpitäjä			HetiL 3.1 §
Tietosisältö - mitä tietoja - tietolähteet			HetiL 9 §, TTL PotilasL, STM:n asetus, SHAsiakasL, muut mahd. lait
Luovuttaminen - mihin - mihin tarkoitukseen - mitä tietoja			PotilasL 13 §, TTL, SHAsiakaslaki, muut mahd. lait
Suojaaminen ml. tietoturva - sisäinen käyttö ja muu käsittely			HetiL 5 §, 32 § JulkL 18 § PotilasL 13 §, STM:n asetus, SHAsiakaslaki, muut mahd. lait
Säilyttäminen ja hävittäminen			ArkistoL, HetL, PotilasL, STM:n asetus
Rekisteröityjen informointi ja oikeudet			HetiL 24 §, 26-29 § PotilasL SHAsiakaslaki
Muut tarpeellisten käsittelyvaiheiden kuvaukset			

HUOM!

Ks. tietosuojavaltuutetun ohje "Malli henkilötietojen käsittelyyn/henkilörekisterin rekisteritoimintojen analysoimiseksi (TSV:n malli 1/2001, 15.8.2001)