**Sosiaali- ja terveysministeriö**
**Kirjaamo**

# Lausunto luonnoksesta hallituksen esitykseksi eduskunnalle laiksi sosiaali- ja terveystietojen tietoturvallisesta hyödyntämisestä sekä eräiksi siihen liittyviksi laeiksi (STM 011:00/2015)

CSC – Tieteen tietotekniikan keskus Oy kiittää mahdollisuudesta saada lausua luonnoksesta hallituksen esitykseksi. CSC on suomalainen tutkimuksen, koulutuksen ja julkishallinnon ICT-osaamiskeskus, joka ylläpitää opetus- ja kulttuuriministeriön toimeksiannosta korkeakoulujen valtakunnallista tietovarantoa. CSC:llä on tekninen valmius terveys- ja sosiaalitiedolle räätälöidyn kansallisen tason tietoturvallisen lupamenettelyn, tiedonsiirron ja käsittelyalustan toteuttamiseen. CSC:n osaaminen keskittyy tietotekniikkaan sekä tutkimus- ja tuotekehityksen tukemiseen yhteistyössä tiedon substanssiosaajien kuten Terveyden ja Hyvinvoinnin laitoksen kanssa. Kansainväliset datavarannot voidaan tuoda osaksi kansallisen terveystiedon tulkintaprosessia CSC:llä isännöidyn Euroopan biologisen tiedon infrastruktuurin osakeskuksen avulla (ELIXIR, Valtiosopimus 7/2015).

**CSC – Tieteen tietotekniikan keskus Oy esittää lausuntonaan seuraavaa:**

## Yleisiä huomioita

Luonnoksen ehdotus kansallisten sosiaali- ja terveystietojen avaamisesta tutkimukselle ja tuotekehitykselle entistä laajemmin on kannatettava. Suomen hallinnon järjestyneisyys ja kansalaisten kattava terveydenhuolto on tuottanut ja tuottaa dataa, joka on kansainvälisesti tunnistettu ja arvostettu tietolähde ihmisten terveyden edistämiseksi. Datan tekee erityisen arvokkaaksi sen rakenteellinen muoto ja aineistojen väestöpohjallinen kattavuus. Yhdessä geneettisen perimän kanssa ne muodostavat kasvupohjan terveys- ja hyvinvoinnin asiantuntijoiden uusille yrityksille ja työpaikoille vuosikymmeniksi eteenpäin. Lain valmistelussa tulee kuitenkin huomioida se, että sosiaali- ja terveystietojen kansallisen tason avaamisen ehdoton edellytys on, että datan käsittelyn tietoturvallisuus varmistetaan merkittävästi kattavammin ja kestävämmin kuin se nykymuotoisessa luonnoksessa on kuvattu. Lisäksi lainsäädännön jatkovalmistelussa tulee kiinnittää huomiota siihen, että nyt rakennettava lainsäädäntö on EU:n tietosuoja-asetuksen mukainen. Teknisen käyttöympäristön luominen ei riitä, vaan EU:n tietosuoja-asetuksen edellyttämät prosessit tulee olla kunnossa.

Luonnoksessa ehdotetaan, että erilaisten henkilö- ja asiakastietojen käyttöluvat myöntäisi jatkossa keskitetysti yksi lupaviranomainen, että lupakäsittelyä varten luotaisiin sähköinen lupaportaali, ja että luvan nojalla luovutettaville tiedoille luotaisiin tietoturvalliset sähköiset käyttöympäristöt ja käyttöyhteydet. Esityksen keskeisenä tavoitteena on sujuvoittaa ja nopeuttaa olennaisesti tietojen käyttölupiin liittyvää käsittelyä ja keventää siihen liittyvää, rinnakkaisista lupamenettelyistä aiheutuvaa hallinnollista taakkaa. Nämä ovat kannatettavia tavoitteita ja ne tukevat myös hallitusohjelmassa esitettyjä tavoitteita. Toisaalta, hyvien tavoitteiden saavuttamiseksi tulee kuitenkin kiinnittää perusteellisesti huomiota keinoihin, joilla nämä asetetut tavoitteet pyritään saavuttamaan.

EU:n tietosuoja-asetuksen analysointi onkin ehdotetussa hallituksen esityksessä puutteellinen eivätkä asetuksen edellyttämät henkilötietojen käsittelyä ohjaavat prosessit tule selkeästi esille ehdotuksen nykymuodossa. Ehdotuksessa ei esimerkiksi huomioida riittävällä tavalla EU:n tietosuoja-asetuksen edellyttämiä organisatorisia ja teknologisia suojauskeinoja henkilötietojen käsittelylle eivätkä asetuksen edellyttämät vaatimukset näin ollen kokonaisuudessaan täyty nykymuotoisessa ehdotuksessa. Asetuksen mukaisesti tietoturvan tulee olla sisäänrakennettuna (*by default* ja *by design*) prosesseihin ja työkaluihin, mikä on aivan keskeinen asia tämän lainsäädännön luomisessa, ja tulisi siksi vahvasti huomioida jatkovalmistelussa.

Oikeudelliselta kannalta on lisäksi ongelmallista, että ehdotuksessa on puutteellisesti analysoitu kansalaisten ja rekisteröityjen oikeuksien toteutumista EU:n tietosuoja-asetuksen mukaisesti. Kaiken viranomaisen toiminnan tulee perustua lakiin ja henkilötietoja käsiteltäessä luottamus ja lainmukaisuus ovat tärkeitä itseisarvoja.

Jatkovalmistelussa tulisi myös keskittyä määrittelyyn, joka koskee yksiselitteisen ja selkeän suostumuksen antamista näytteiden yhdistämiseksi muihin rekistereihin. Henkilöiden oikeuksien toteutumisen kannalta on olennaista, että he tietävät tarkalleen, mihin antavat suostumuksensa.

Tietojen anonymisointi mainitaan ehdotuksessa useassa kohdassa, mutta sen määritelmää tulisi kuitenkin tarkentaa: anonymisointi viittaa siihen, että henkilön tunnistamisen mahdollistavat tiedot on peruuttamattomasti poistettu (ks. esim. linkki). Teknologian ja analytiikkakeinojen kehittyessä myös identifiointikeinot uudistuvat, jolloin aiemmin anonymisoidusta datasta voi olla tulevaisuudessa mahdollista löytää tunnistetietoja.

Tärkeää olisi kiinnittää tässä vaiheessa huomiota myös maiden rajat ylittävään tietojen hyödyntämiseen. Datan jatkokäyttö ja yhdistely ovat vahvasti EU:n agendalla, ja näitä teemoja pyritään edistämään komission digitaalisia sisämarkkinoita koskevalla strategialla (5/2015) ja siihen liittyvillä komission ehdotuksilla. Tieteen edistämisen ja innovaatioiden syntymisen kannalta datan laajempi käyttö on avainasemassa, mutta samanaikaisesti on muistettava, että toiminnan tulee perustua luottamukseen, oikeudelliseen varmuuteen ja vahvaan tietoturvaan.

Näiden tärkeiden periaatteellisten tekijöiden lisäksi haluamme nostaa seuraavat yksityiskohtaisemmat asiat huomioitavaksi jatkovalmistelussa:

## 1) Tietojärjestelmien ja datan integraatio

Pullonkaulana lain mahdollistaman vision toteuttamiselle ovat tällä hetkellä vaatimukset uusille tietojärjestelmille ja näiden tarjoamille rajapinnoille sekä organisaatioiden välisen yhteistyön sirpaleisuus.

Keskitetty käyttölupaviranomainen voisi oikein toteutettuna nopeuttaa datan saatavuutta organisaatioista ulos, mutta ei välttämättä vielä takaa datan laatua tai erilaisten terveydenhuollon datan tuotantoprosessien yhteensopivuutta. Esimerkiksi diagnoosia varten tehtävän lääketieteellisen kuvantamisen datamittauksista ja niiden suoritusolosuhteista ei välttämättä kerätä samanmuotoista dataa Helsingin ja Oulun yliopistollisessa sairaalassa, vaikka asiantuntijatyön lopputulos, kuten tautidiagnoosi rintasyöpätyypistä, olisi näissä organisaatioissa sama. Organisaatioiden yhteisistä periaatteista sen suhteen, miten dataa kerrytetään ja

minne ja minkälaisena rakenteena se tehdään uudelleen jaettavaksi jatkokäyttöä varten, pitäisi siksi myös säätää tässä laissa.

Tietolähteiden rajapinnat ovat tärkeä osa uutta palvelurakennetta: missä muodossa dataa tuottavista organisaatiosta, kuten yliopistollisesta keskussairaalasta tai Kelasta voidaan (koneellisesti) kysyä dataa, kun käyttölupa aineistoon ja/tai sen yhdistelyyn on myönnetty? Hyvin dokumentoiduilla ja ylläpidetyillä datalähteiden rajapinnoilla voidaan mahdollisesti välttää jälkikäteen tehtävät data-aineistojen työläät integraatiot, joita esimerkiksi potilastietojärjestelmien yhdistämisessä on kohdattu. Esimerkiksi julkisissa kilpailutuksissa tietojärjestelmätoimittajille voitaisiin lainsäädännössä edellyttää tiedon jakamiselle rajapinta- ja formaattivaatimus, joka tekee toimitettavat tietojärjestelmät ja tietopalvelut yhteensopiviksi Kanta-arkiston ohella kansainvälisen tieteen ja tutkimuksen ja tietoteknologian standardien kanssa. Muuten aineistojen käyttöarvo tuotekehityksessä on rajallinen, koska työ alkaa aina datan siivoamisella. Kanta-arkiston rakennetta ei voida ulottaa kattamaan kaikkia käyttötarkoituksia, siksi rakenteen pitäisi vaadittujen tietokenttien lisäksi sallia tiede/sovelluskohtaisten kenttien lisääminen lisätietona.

Uutena tietolähteenä lähivuosina viranomaisten terveys- ja hyvinvointidataan liittyvät henkilöiden itse kokoamat ja heidän käyttöön lupaamansa aineistot mm. elintavoista. Monet kansalaiset haluavat antaa oman dataansa tutkimuskäyttöön, jotta tutkimukset tukisivat ennaltaehkäisevän hoidon edistämistä yhdistelemällä viranomaisten tietolähteitä, tutkimusinfrastruktuurien referenssitietoja ja yksilöiden omaa dataa. On tärkeää tukea mekanismeja, joilla hyöty terveys- ja sosiaalialan datapohjaisesta tutkimuksesta saadaan kansalaisten ulottuville tulevaisuudessa. Näin kansalaiset kokevat suoran hyödyn uusista palveluista, ja tämä kasvattaa luottamusta datan uusiokäyttöön sekä uusien sovellusten kehittämiseen. Esimerkkinä voidaan ajatella henkilön oma terveystili, johon liittyvät palvelutoimijoiden riskikartoitukset ja arviot siitä, kuinka henkilön hyvinvointia voidaan suunnitelmallisesti kohentaa. Toisaalta sairauden yllättäessä halutaan käyttää genomidataa, sillä esimerkiksi syövän parhaiden hoitomuotojen valitseminen vaatii syvällistä diagnoosia.

Esimerkkihankkeita Suomessa ovat mm. sydän- ja verisuonitautien terveydenhoidollisten riskien hankkeet Kardiokompassi, Generisk ja SISU, joiden tietojärjestelmien toteutuksessa on hyödynnetty CSC:n alustoja. Näiden käyttötapausten puitteissa voidaan integroida teknisiä konsepteja ja palvelukomponentteja (sähköinen palveluiden integraatio, esim. palveluväylässä sähköinen henkilöiden tunnistus - eSuomi, yksilöiden oma suostumus datan käyttöön - MyData, datan käyttölupien sähköinen palvelu - REMS, tietoturvallinen pilvialusta - ePouta, yhteydet kansainvälisiin bio- ja terveysalan tietovarantoihin - ELIXIR) lain sallimissa puitteissa suurempaan kansalliseen kokonaisuuteen.

Jatkovalmistelussa pyydämme kiinnittämään huomiota erityisesti tietovarantojen säilymiseen Suomen lainsäädännön piirissä. Pitkäaikaisena tavoitteena on ulkomaisten investointien ja työpaikkojen synty Suomeen tietovarantojen avaamisen ja organisoinnin kautta syntyvän innovaatiopotentiaalin avulla. Lainsäädännössä pitää turvata se, että tämä tietoa kokoava ja avaava toiminta on laillisesti mahdollista ja resurssit strategialle ovat järjestettävissä. Toisaalta tulee huomioida, että mahdollisissa konflikteissa riitojen ratkominen tapahtuu sen maan oikeuskäytäntöjen mukaan, missä tietovaranto ja tietoa yhdistävät palvelut on luotu.

## 2) Tietoturvavaatimukset

Sosiaali- terveystietojen tietojen (tieto)turvallisen käsittelyn varmistaminen luo myös merkittäviä uusia mahdollisuuksia sekä tutkimukselle, terveydenhuoltojärjestelmän kehittämiselle että yritysten toiminnalle. Tietosuojaan, tietoturvallisuuteen ja tiedon saattavuuteen liittyvät riskit ovat kuitenkin merkittäviä, eivätkä nyt käytössä olevat suojaamistoimenpiteet pysty riittävästi torjumaan riskejä. Hallinnolliset, julistuksenomaiset tai symboliset turvakontrollit eivät missään tapauksessa ole riittäviä nykyaikaisessa kyberympäristössä, jossa hyökkäykset ja pyrkimykset häikäilemättä hyödyntää tietoja käyttötarkoitusten tai suostumusten vastaisesti ovat arkipäivää. On myös kiinnitettävä huomiota EU:n tietosuoja-asetukseen, joka määrittelee lisäksi merkittäviä sanktiota (10/20 Meur) tahoille, jotka laiminlyövät asetuksen mukaisten tietosuojavaatimusten toteuttamisen ja valvonnan. Uuden lain tuleekin olla linjassa EU:n tietosuoja-asetuksen kanssa yksilöä koskevan sensitiivisen datan turvaamiseksi.

Ehdotamme, että hallituksen esityksessä edellytetään laissa tarkoitettujen aineistojen käsittelyyn käytettävien tietojärjestelmien ja prosessien tietoturvallisuusriskien arviointia ja niiden edellyttämiä toimenpiteitä. Tietojen käsittelyn toteutukset tulee aina varmistaa järjestelmällisesti, esimerkiksi Kyberturvallisuuskeskuksen hyväksymän arviointilaitoksen toimesta ja havaitut puutteet tulee korjata sovitun aikataulun mukaisesti. Yksilön salassa pidettävien tietojen turvaaminen tulee perustua selkeästi määriteltyihin tietoturvanormeihin, joiksi kelpaavia ovat vaatimus ISO/IEC 27001 sertifioinnista sekä tietojen käsittely ST III (suojataso) mukaisesti.

Sosiaali- ja terveystietojen hallittu ja valvottu käyttö on Suomelle kansallinen etu, ja Suomen tulee edistää näiden tietojen säilyttämisen ja niiden käsittelyn pysymistä Suomessa. Ehdotamme, että hallituksen esitykseen lisätään säädös ko. tietojen säilytyksen ja kaiken käsittelyn tapahtuvan Suomessa sijaitsevilla tietojärjestelmillä ja tietokoneilla. Tämä on keskeinen elementti yksilöiden luottamuksen säilyttämisessä. Jos tietoja sallitaan luovutettavan ulkomaille tai EU:n ulkopuolelle, yksilön tietosuojan säilymisen varmistaminen on erittäin haastavaa tai usein mahdotonta. Kaikilta toimijoilta tulee edellyttää samanlaista tietojärjestelmien varmistusta, ja lisäksi turvallisuusvaatimusten tulee kattaa myös kansalliset ja kansainväliset alihankkijat, joiden tulee myös olla samantasoisen valvonnan piirissä.

Lähtökohta sosiaali- ja terveystietojen käsittelylle on tiedon luokittelu kontrolloidulla ja jäljitettävällä tavalla siten, että luokittelu säilyy, vaikka tieto siirtyy toiseen ympäristöön. Luovutettavien tietojen luokittelu on lupaviranomaisen tärkeä tehtävä ja olennaisesti edistää myös tietojen vastaanottajan ymmärrystä. Se on myös edellytys hallituksen esityksessä mukana oleville salassapitosopimuksille.

Lupaviranomaisen tehtävistä yksi haastavimmista on tiedon anonymisointi, joka on samalla erittäin keskeinen tehtävä yksilöiden tietosuojan kannalta. Käytännössä anonymisointi on usein toteutettu heikosti ja helposti murrettavalla tavalla ja siksi on ensiarvoisen tärkeää, että lupaviranomaisella ja myös kaikilla sosiaali- ja terveystietoja luovuttavilla tahoilla on käytössään riippumattomasti luotettaviksi todennetut anonymisointimenetelmät tai -palvelut.

Lisäksi laissa tulee varautua tahattomiin virheisiin siten, että tietosuoja varmistetaan EU:n tietosuoja-asetuksen edellyttämällä tavalla usein eri keinoin: teknisin, hallinnollisin, sopimuksellisin ym. tavoin. Eräs tällainen asia luonnoksessa jo on eli tietojen saajan salassapitosopimus. Samaa ja samanlaisia periaatteita tulee soveltaa kaikki toimijoihin.

Lisäksi ehdotamme, että varmistetaan, että ko. lainsäädäntö edellyttää yksilön suostumusta samalla tavalla kuin nykyhetkellä edellytetään kuitenkin siten, että Suomen terveysviranomaisten ja terveyspalvelutuottajien palvelukehitykseen ja terveydenhuoltojärjestelmän kehittämiseen suostumusta ei välttämättä tarvittaisi. Lisäksi erityisesti tutkijan omaan dataan yhdistettäessä potilastietoa tulee edellyttää

yksilöiden suostumuksia. Suostumusten käsittely tulee automatisoida ja tietojen siirtyminen järjestelmästä toiseen tulee varmistaa.

## 3) Lupaviranomaisen suhde biopankkeihin

Laissa kuvattuja sähköisiä palveluja tarvitaan myös biopankkitoiminnassa. Kustannussäästöjä olisi mahdollista saavuttaa, jos lupaviranomainen voisi tuottaa palveluja myös yhdessä muiden asiaankuuluvien toimijoiden kanssa tai ottaa hoitaakseen myös muiden toimijoiden lupa-asioita osittain tai kokonaan.

## 4) Yksityisyyden suojan varmistamisen vastuuttaminen

Pyydämme kiinnittämään huomiota seuraaviin kysymyksiin:

Mitä toimenpiteitä lupaviranomainen velvoitetaan tekemään yksityisyyden suojan varmistamiseksi? Mikä taho vastaa yksilön tietosuojasta?

Onko laissa annettu lupaviranomaiselle oikeus arvioida ja päättää, riittääkö tutkimuksen tekemiseksi aggregoitu tieto vai tarvitaanko yksilötason tietoa? Onko lupaviranomaisen velvollisuus pienentää yksilön suoran tai epäsuoran tunnistamisen riskiä? Millä toimenpiteillä lupaviranomainen voi tähän vastata?

Onko lupaviranomaisella oikeus päättää myös tarvittavan datan määrästä eli yksilöiden ja yksilöön liittyvien tietojen määrästä? Onko lupaviranomaisella oikeus pilkkoa tai edellyttää hakijaa pilkkomaan tutkimussuunnitelma pienempiin kokonaisuuksiin selkeämpien ja riittävien tietokokonaisuuksien muodostamista varten? Miten estetään tarpeettoman suurten aineistojen luovuttaminen hakijalle?

## 5) Kansalaisten luottamus järjestelmään kanavoituu suostumuksen kautta

Käsillä oleva hallituksen esitys perustuu olennaisesti kansalaisten luottamukseen siitä, miten heistä sosiaali- ja terveydenhuollon järjestelmien prosesseissa kerättyä tietoa hyödynnetään osana uusia palveluita. Lakimuutoksen tavoitteena on vahvistaa jo nykyistä vahvaa kansalaisten luottamusta viranomaisiin korostamalla yksilön tietosuojaa heistä kerättyjen tietojen sekundäärisessä hyödyntämisessä. Luottamus tähän monimutkaiseen järjestelmään kanavoituu kansalaisen antaman suostumuksen kautta.

Kansalaisen suostumus tulisi ensisijaisesti ymmärtää suostumuksena kansallisen terveyden- ja sosiaalihuollon prosesseihin, tämän järjestelmän kehittämiseen sekä uusien hoitoprosessien tutkimiseen. Suostumus voisi olla myös riippuvainen maantieteellisestä sijainnista, jolloin ns. opt-out-mallia voitaisiin soveltaa Suomessa tapahtuvaan käsittelyyn ja ns. opt-in-mallia Suomen ulkopuolella tapahtuvaan käsittelyyn. Kansalaisille on taattava lakiesityksen valmistelun puitteissa riittävä ja oikea-aikainen tieto siitä, miten tätä informaatiota käytetään hyväksi sosiaali- ja terveydenhuollon järjestelmien ulkopuolella. Iso-Britanniassa vastaavan prosessin puutteellinen kommunikointi aiheutti kansalaisissa hämmennystä ja vähensi luottamusta viranomaisten toimintaan. Tästä johtuen Iso-Britanniassa suostumusprosessia yksinkertaistetaan – esimerkiksi suunnitelmissa on mahdollistaa kansalaisen suostumus informaation käyttötarkoituksen mukaisesti. Tämä malli sopii myös ns. opt-out-malliin, mikäli suostumuksen hallinnointijärjestelmä tukee selkeästi informaation jälleenkäytön estämistä halutuissa palveluissa. Suostumusta tulisi lisäksi hallinnoida yhden luukun periaatteella (Lähde: Caldicot Review 2016).

## 6) Sanktiot

Hallituksen esitykseen tulee lisätä väärinkäytöksistä koituvat sanktiot. Lisäksi tulee tutkia mahdolliset väärinkäyttötapaukset ja asettaa näitä varten asiaankuuluvia kontrolleja tai esteitä.

## 7) Sosiaali- ja terveystiedon hyödyntämisen taloudelliset mallit muualla

Iso-Britanniassa terveystiedon ja erityisesti yksilöistä kerätyn genomi-informaation käytön taloudellisia vaikutuksia on arvioitu paikallisen terveydenhuollon (NHS) kustannustehokkuuden parantamisessa. Valtio on rahoittanut 100 000 potilaan genomin analysoimisen osana yksilöiden hoitoprosessia. Projektista vastaa Iso-Britannian sosiaali- ja terveysministeriön omistama yhtiö Genomics England Ltd. (GEL), joka myös tarjoaa pääsyn potilaista kerättyyn tietoon yksityissektorin toimijoille. Kustannusmallit sekä lupajärjestely on kuvattu osana datan käyttölupamenettelyn dokumentaatiota[1]. Iso-Britannian malli on pitkälti samanlainen kuin lakiesityksessä mainittu uusi yhtiömuoto, joka huolehtisi palveluiden tarjoamisesta eri sektoreille ja palvelumaksujen keräämisestä puhtaan viranomaistoiminnan sijaan.

## Kommentteja yksittäisiin pykäläehdotuksiin

**Yleisiä kommentteja**

- Viranomaisten tehtäviä, teknisiä palveluita että tietojärjestelmiä on selvyyden vuoksi hyvä käsitellä erillisinä asioina.
- Yksilön salassa pidettävien tietojen turvaaminen tulee perustua selkeästi määriteltyihin tietoturvanormeihin, joiksi kelpaavia ovat vaatimus ISO/IEC 27001 sertifioinnista sekä tietojen käsittely ST III (suojataso) mukaisesti.
- Sähköinen käyttölupaportaali kuvataan luonnoksessa tarpeettoman yksityiskohtaisesti ja ainakin osittain virheellisesti sekä sähköisiin palveluihin tai tietojärjestelmiin liittyvä terminologia ei vastaa käytäntöjä. Ks. tarkennetut kommentit.

## 3§ Määritelmät

Kohta 4. tunnisteellinen tieto, jonka perusteella rekisteröity voidaan välittömästä yksilöidä.

- Minkälaisia määreitä sanaan ’välittömästi’ liittyy? Tarkoittaako ajallisesti nopeaa yksilöintiä tai vähin toimenpitein tehtävää yksilöintiä? Sisältääkö koodatun tiedon eli kun henkilötunnus ja muut suorat tunnisteet on korvattu koodilla, jonka purkuavain on olemassa ja mahdollisesti toisen toimijan hallussa?
- Ehdotus, että ’välittömästi’ jätetään pois.

Kohta 5. Ehdotus lisäykseksi:

- ”…yhden tai useamman henkilölle tunnusomaisen fyysisen, fysiologisen, psyykkisen, taloudellisen, kulttuurisen tai sosiaalisen **tai muun** tekijän perusteella”.

[1] https://www.genomicsengland.co.uk/download/ig6-data-access-and-acceptable-uses-policy/

Kohta 11. kehittämis- ja innovaatiotoiminta.

- Mitä tarkoitetaan tieteellisellä tiedolla? Innovaatio ei välttämättä edellytä tieteellistä tietoa, vaan sen ydin voi olla myös täysin uusi tapa hyödyntää tai käsitellä uutta tai vanhaa tietoa.

Kohta 16. tekninen käyttöyhteys, joka on tietoturvallinen.

- Miten yhteyden tietoturvallisuus osoitetaan? Minkälainen tietoturvataso vaaditaan?
- Tietoturvataso tulee valita sen mukaan, mihin luokkaan käsiteltävät aineistot on turvaluokiteltu. Nykyisten VAHTI-ohjeiden perusteella potilastiedoissa on kyse salassa pidettävästä aineistosta ja siten potilastietoja sisältävien aineistojen suojaustaso on III, ja niiden käsittely edellyttää järjestelmiltä korotettua tietoturvatasoa.

Kohta 18. sähköinen lupaportaali.

- Määritelmässä puhutaan yhdestä verkkopalvelusta, ei portaalista, josta pääsee käyttämään useita verkkopalveluja -> sähköinen käyttölupapalvelu.
- Määritelmässä puhutaan asiointipalvelusta -> sähköisellä käyttölupapalvelulla verkkopalvelua, jonka välityksellä käyttöluvan hakija voi sähköisesti asioida lupaviranomaisen kanssa ja toimittaa käyttölupahakemuksen viranomaiselle ja saada viranomaisen päätöksen hakemukseensa.

## 4§ Asiakastietojen hyödyntämisen yleiset perusteet ja edellytykset

Kolmannessa momentissa: ”…saada ja yhdistellä…”.

- Momentissa puhutaan aggregaattitasoisista tiedoista, joiden tuottaminen edellyttää tietojen käsittelyä eli pelkkä yhdistäminen henkilötunnuksen avulla ei riitä. Muutosehdotus: ”…saada, yhdistellä **ja muutoin käsitellä**…”

## 5§ Tieteellinen tutkimus, kehittäminen ja innovaatiotoiminta

Ensimmäisen momentin 1. kohta: ”lupaviranomainen voi antaa hakijalle vain siinä tapauksessa, että hakija hakee useammasta lähteestä yhdistettyä tietoa”.

- Hakijan tulisi saada sama lupakäsittelypalvelu yhdestä ja samasta paikasta (yhden luukun palvelu) riippumatta datan lähteiden määrästä -> Lupaviranomaisella on oikeus luovuttaa tietoa myös vain yhdestä lähteestä ja lähteellä on oikeus itse luovuttaa omaa dataansa, jolloin hakija voi valita hakeeko keskitetystä palvelusta vai suoraan lähteestä. Tämä antaa myös eri viranomaisille mahdollisuuden siirtää kaiken tutkimuskäyttöön tarkoitetun tiedon luovutuksen keskitettyyn palveluun, jolloin voidaan saavuttaa kustannussäästöjä.
- Minkälaisia velvollisuuksia laissa mainituilla viranomaisilla on osallistua keskitetyn käyttölupapalvelun tuottamiseen? Jokainen viranomainen voi ja olisi syytä omien tietojensa parhaimpana asiantuntijana kuitenkin osallistua keskitettyyn palveluun vähintään asiantuntijana.
- Dataan hallinnoivien organisaatioiden täytyy kuvailla datalähteensä keskitettyyn lupapalveluun ja ottaa lupamenettelypalvelu käyttöön. Tämän työn tekemiseen pitää varautua näissä organisaatioissa, koska lupaviranomainen ei tee (eikä pystykään tekemään) sitä organisaation puolesta.

## 10§ Rekisteritietojen hyödyntämisen edellyttämät viranomaisten palvelut

- Ensimmäisen momentin lista sisältää sekä viranomaisten tehtäviä, teknisiä palveluita että tietojärjestelmiä. Nämä olisi selvyyden vuoksi hyvä esittää erillisinä asioina.
- Lupaviranomaisen tehtäviä:
  - yhteentoimivuuden varmistaminen ja yhteentoimivuuden edellytysten tuottaminen eri viranomaisten tietoaineistojen kuvaustyötä varten ja kuvausten ylläpitoa varten tietoaineistojen löytämisen ja hyödyntämisen mahdollistamiseksi.
  - tietoaineistojen hyödyntämiseen liittyvä neuvonta.
  - tietoaineistojen käyttölupien käsittely.
  - käyttöluvan edellyttämä tutkimussuunnitelmien tarkoituksenmukaisuuden ja asianmukaisuuden arviointi tarvittavien tietojen määrän ja laadun suhteen tietojen luovutuksen näkökulmasta.
  - käyttölupien keskitetty myöntäminen on hyvä kehityssuunta. Datan analyysissä usein tarvitaan sekä kansallisia että kansainvälisiä aineistoja. Kansallisessa prosessissa lupaviranomainen myöntää pääsyn aineistoihin. Kansainvälisissä aineistoissa luvan myöntää yleensä tutkimuskäyttöä valvova taho nk. Data Access Committee. Tietojärjestelmän, joka hallinnoi lupamyöntöjä täytyy pystyä integroimaan henkilöille ja organisaatoille myönnetyt luvat näiltä tahoilta.
  - käyttöluvan edellyttämä tutkimussuunnitelmien eettinen ennakkoarviointi.
  - tietojen yhdistäminen ja käsittely siten, että riskit yksilön tietosuojan murtumiseen minimoidaan sekä luovutettavan tietopaketin turvaluokittelu; käsittelyssä tulee käyttää riippumattomia ja luotettavia anonymisointimenetelmiä.
  - tietoaineistojen muodostaminen ja luovuttaminen hakijalle.
  - yksilön tunnistamisen mahdollistavan koodiavaimen ja tietojen muodostamisen menetelmien kuvaaminen ja säilyttäminen.
  - mahdollisen kliinisen löydöksen vastaanottaminen ja yksilön tunnistaminen purkamalla koodiavain sekä kliinisen löydöksen saattaminen yksilön hyödyksi.
  - luovutettujen tietojen käytön valvonta ja raportointi tietosuojaviranomaisille ja lupaviranomaisen toiminnan valvojalle.
- Sähköisiä palveluita: edellä mainittujen tehtävien hoitamiseksi viranomaisen tulee järjestää sähköisiä palveluja, joiden avulla hakijat voivat toteuttaa seuraavia tehtäviä ja asioida lupaviranomaisen kanssa. Sähköisten palvelujen tulee täyttää niissä käsiteltävien tietojen turvaluokituksenmukaiset ja muut asianmukaiset tietoturvavaatimukset. Viranomaisen tulee tuottaa sähköiset palvelut, joilla tietoaineistojen hakija tai käyttäjä voi:
  - saada tietoa käytettävissä olevista tietoaineistoista.
  - hakea käyttölupia.
  - vastaanottaa ja käsitellä saamiaan tietoja.
  - palauttaa lupaviranomaiselle mahdollisen kliinisen löydöksen tiedot.
  - raportoida lupaviranomaiselle tietoaineistojen käytöstä ja niillä saaduista tuloksista käyttöehtojen mukaisesti.
- Asianhallintajärjestelmä: viranomainen tarvitsee omaa toimintaansa varten sähköisen asianhallintajärjestelmän, joka on yhteentoimiva valtionhallinnon muiden tietojärjestelmien, yllä listattujen sähköisten palvelujen sekä muiden asiaankuuluvien järjestelmien kanssa. Asianhallintajärjestelmä sisältää kaiken lupaviranomaisen tämän lain tehtävää tuottaessaan synnyttämän tiedon sellaisessa muodossa, että siitä voidaan muodostaa asianmukaiset raportit toiminnasta sekä tietotilinpäätökset ja tarvittaessa jäljittää tehdyt päätökset ja muutokset.

Tämä pykälän muuttaminen vaikuttaa useaan jäljempään kohtaan lakitekstissä.

## 14§ Sähköinen käyttölupaportaali

Pykälässä kuvataan tarpeettoman yksityiskohtaisesti ja virheellisesti viranomaisen tuottamaa teknistä palvelua, ks. yllä kuvatut viranomaisen tehtävät, tuottamat sähköiset palvelut sekä asianhallintajärjestelmä. Sähköisiin palveluihin tai tietojärjestelmiin liittyvä terminologia on myös osin virheellistä.

Lupaviranomainen voisi tuottaa sähköisiä palveluja yksin tai yhdessä muiden asiaankuuluvien toimijoiden kanssa sekä teknisesti että sisällön osalta. Lupaviranomaiselle ei tarvitse olla itsellään syvää aineistojen tuottajan asiantuntemusta, jota tarvitaan aineistojen hyödyntämiseen.

Käyttölupaportaali ei voi toimia asianhallintajärjestelmänä. Käyttölupaportaali on palvelu, johon asiakkaat tunnistautuvat ja voivat esimerkiksi hakea pääsyä dataan. Portaali asioi rajapintojen yli esimerkiksi datan jakelujärjestelmän ja muiden taustajärjestelmien ja mahdollisesti kansallisen palveluväylän[2] kanssa. Arkkitehtuurissa täytyy olla myös erillinen paikka, johon dataa hallinnoivilta tahoilta tulevat aineistot kootaan asiakkaan prosessointi varten.

## 17§ Tietoturvallinen käyttöympäristö

Pykälässä tulee tarkentaa tietoturvan määrittelyä: valittu tietoturvataso riippuu ympäristössä käsiteltävien aineistojen turvaluokituksesta sekä sen kytköksistä muihin tietojärjestelmiin. VAHTI-ohjeistuksen mukaan suojaustason III tietoja kuten salassa pidettäviä potilastietoja tulee käsitellä korotetun tietoturvatason vaatimukset täyttävissä tietojärjestelmissä. Hyviin perusteluihin perustuen (taloudellinen, käytettävyys) voidaan dataa käsitellä matalamman suojaustason tietojärjestelmissä. Lisäksi siirtymäkausi tulee määritellä lopullisessa hallituksen esityksessä.

## 18§ Koodiavainten säilytyspalvelu

Pykälässä käytetään samaa termiä kahdesta erilaisesta asiasta: aineistojen koodiavaimesta ja menetelmästä, jolla aineisto tuotetaan tai poimitaan. Koodiavain tarvitaan, kun aineistossa esiintyvä yksilö on kuvattu aineistossa koodilla, ja koodia vastaava henkilö halutaan tunnistaa. Koodiavaimella koodi voidaan tulkita henkilön suoriksi tunnisteiksi. Aineiston tuottamisessa tai tietojen poiminnassa muodostetaan menetelmä tai skripti, jolla aineiston halutut tietokentät valitaan ja halutut kriteerit täyttävät yksilöt valitaan. Muodostetun aineiston sijaan voidaan arkistointia varten säilyttää myös tuo menetelmä, jolloin säästetään tallennustilaa.

## 19§ Tietoturvallinen tekninen käyttöyhteys

Pykälässä kuvataan kaksi tietomäärältään hyvin erilaista prosessia: käyttölupakäsittely ja tietoaineiston luovutus. Käyttöluvassa käsitellään olennaisesti pientä tietomäärää kun taas tietoaineisto voi olla erittäin suuri. Näihin prosesseihin ja palveluihin tarvitaan erilaiset käyttöyhteydet ja laitteistot ja infrastruktuuripalvelut. Kts. yllä pykälän 10 kommentti.

## 20§ Sähköinen tietoturvallinen käyttöympäristö

Lause jää kesken: ...luovuttamaan muita kuin tai aggregaattitasoisia…

Pykälän tekstistä saa käsityksen, että tunnisteelliset tai koodatut tiedot tulee käsitellä ensisijaisesti lupaviranomaisen tietoturvallisessa käyttöympäristössä. Jos näin halutaan, se olisi hyvä ilmaista suoraan. Suoraan voidaan ilmaista myös, että aggregaattitasoinen anonyymi tieto voidaan luovuttaa myös muualla käsiteltäväksi kuin lupaviranomaisen tietoturvallisessa käyttöympäristössä, jos näin halutaan ja tarkoitetaan. Pykälässä tulee määritellä mitä tarkoitetaan tietoturvallisella käyttöympäristöllä ja miten tietoturvallisuus riippumattomasti todetaan.

[2] http://www.finlex.fi/fi/laki/alkup/2016/20160571

## 22§ Käyttöluvan myöntämisen perusteet

Ensimmäisen momentin kohta 2. tarkoituksenmukaisimmin: tähän kohtaan vaikuttaa pykälän 10 tehtävien määrittely ja jaottelu. Kohdassa 2 tulisi erikseen tuoda esiin tarkoituksenmukaisuuden arvioinnissa tutkimuksessa tarvittavan tiedon muuttujien tai parametrien määrä ja tarvittavien yksilöiden määrä sekä tietojen turvaluokitus siten, että ensisijaisesti pyritään aggregaattitasoiseen ja täysin anonyymiin aineistoon ja tunnisteellisen tai koodatun aineiston tapauksessa pyritään minimoimaan luovutettavien parametrien ja yksilöiden määrä. Tämä saattaa myös edellyttää tutkimuksen pilkkomista pienempiin yksiköihin, jolloin suunnitellun tutkimuksen toteuttamiseen voidaan luovuttaa useampia itsenäisiä aineistoja koodauksineen. Näin eri aineistoissa sama koodi tarkoittaa eri henkilöitä eikä tiedon käyttäjälle synny suurta tietomäärää yhdestä yksilöstä, mikä pienentää välillisen tunnistamisen mahdollisuutta.

## 24§ Tietojen luovutus käyttöluvan myöntämisen jälkeen

Ensimmäinen momentti:

- ".. se hankkii, yhdistelee ja koodaa…"

Kohta 1.

- "…asianmukaisella aggregoinnilla anonymisoitu..."
- "…toimitetaan yksilötasoisina tai rekisteröityjen tasolla (ei rivitasoisina)…"
- "…että hän tietojen käsittelyn kuluessa anonymisoinnista huolimatta tunnistaisi välillisesti jonkun rekisteröidyistä..."

Anonymisointi ei ole onnistunut tai kyseessä ei ole todellinen anonymisointi tämän lain alussa olevien määritelmien mukaan, jos tunnistaminen on mahdollista.

Kohta 2. teksti sisältää oletuksen, ettei tietoturvallisesta käyttöympäristöstä ole mahdollista siirtää aineistoja ulkopuolelle. Tämä tulisi lisätä esim. termin määritelmään lain alussa.

## 25§ Merkittävät kliiniset löydökset

Kliinisesti merkittävä löydös olisi hyvä määritellä lain alkuosassa.

Jos löydöksestä ilmoittaminen asetetaan velvollisuudeksi, tulisi arvioida halutaanko lakitekstissä tukea tätä. Löydöksen hyödyntäminen eli saattaminen yksilön hyödyksi edellyttää, että tietoaineistossa yksilöt ovat tunnistettavissa eli aineisto on koodattua. Koska on kyse toiminnan sivutuotteesta eikä lain fokuksesta, ei liene perusteltua pyrkiä muuhun kuin mahdollisimman anonyymiin aineistojen käsittelyyn. Jos kliinisiä löydöksiä pidetään merkittävinä elementteinä toiminnassa, voidaan miettiä olisiko johdonmukaista valita velvollisuuden ja oikeuden väliltä kuten biopankkilaissa on asetettu. Prosessi olisi myös perusteltua olla samankaltainen eli löydöksestä ilmoitettaisiin tiedot luovuttaneelle lupaviranomaiselle, jolla on mahdollisuus purkaa koodatun tiedon tapauksessa yksilön tutkimuskoodi.

Espoossa, 30.9.2016

CSC-Tieteen tietotekniikan keskus Oy

Kimmo Koski
Toimitusjohtaja

Satu Tissari
Kokonaisarkkitehti

**Lisätietoja:**

Satu Tissari, TkT, kokonaisarkkitehti, 09 457 2039, satu.tissari@csc.fi
Tommi Nyrönen, FT Dos, ELIXIR osakeskuksen johtaja, 050 381 9511, tommi.nyronen@csc.fi

**Referenssejä**

Caldicot Review 2016 - https://www.gov.uk/government/publications/review-of-data-security-consent-and-opt-outs