

Luonnos hallituksen esitykseksi eduskunnalle laiksi sosiaali- ja terveystietojen toissijaisesta käytöstä annetun lain 60 §:n muuttamisesta

ESITYKSEN PÄÄASIALLINEN SISÄLTÖ

Esityksessä ehdotetaan muutettavaksi sosiaali- ja terveystietojen toissijaisesta käytöstä annetun lain siirtymäsäännöstä siten, että lain tietoturvalliselta käyttöympäristöltä edellytettäviä vaatimuksia sovellettaisiin vasta 1 päivästä toukokuuta 2022. Ennen mainittua ajankohtaa tietoja voitaisiin kuitenkin luovuttaa luvansaajan käsiteltäväksi toisiolain nojalla, vaikka tietolupahakemuksessa ei osoitettaisi toisiolaissa tarkoitettua tietoturvallista käyttöympäristöä tietojen käsittelylle. Lisäksi siirtymäsäännöstä esitetään muutettavaksi siten, että lain merkittäviin kliinisiin löydöksiin perustuvia oikeuksia, velvoitteita ja toimenpiteitä sovellettaisiin 1 päivästä tammikuuta 2024.

Laki on tarkoitettu tulemaan voimaan mahdollisimman pian, kun se on vahvistettu.

SISÄLLYS

ESITYKSEN PÄÄASIALLINEN SISÄLTÖ.....	1
PERUSTELUT	3
1 Asian tausta ja valmistelu	3
Valmistelu	5
2 Nykytila ja sen arviointi.....	6
3 Tavoitteet	9
4 Ehdotukset ja niiden vaikutukset	10
4.1 Keskeiset ehdotukset.....	10
4.2 Pääasialliset vaikutukset.....	11
5 Muut toteuttamisvaihtoehdot	18
5.1 Vaihtoehdot ja niiden vaikutukset.....	18
5.2 Ulkomaiden lainsäädäntö ja muut ulkomailta käytetyt keinot	21
6 Lausuntopalaute.....	21
7 Säännöskohtaiset perustelut.....	22
8 Voimaantulo	23
9 Toimeenpano ja seuranta	23
10 Suhde muihin esityksiin.....	24
10.1 Esityksen riippuvuus muista esityksistä.....	24
10.2 Suhde talousarvioesitykseen	24
11 Suhde perustuslakiin ja säätämismenettely	24
LAKIEHDOTUS	31
sosiaali- ja terveystietojen toissijaisesta käytöstä annetun lain 60 §:n muuttamisesta.....	31
LIITE	32
RINNAKKAISTEKSTI.....	32
sosiaali- ja terveystietojen toissijaisesta käytöstä annetun lain 60 §:n muuttamisesta.....	32

PERUSTELUT

1 Asian tausta ja valmistelu

Tausta

Pääministeri Sanna Marinin hallituksen ohjelman 2019 tavoitteena on, että Suomi on kansainvälisesti houkutteleva paikka opiskella, tutkia ja investoida.

Laki sosiaali- ja terveystietojen toissijaisesta käytöstä (552/2019, jäljempänä toisiolaki) on tullut voimaan 1.5.2019.

Toisiolain tarkoituksena on luoda ajanmukaiset ja yhdenmukaiset edellytykset sosiaali- ja terveydenhuollon palvelutoiminnassa syntyvien henkilötasoisien asiakastietojen sekä muiden terveyteen ja hyvinvointiin liittyvien henkilötietojen käytölle tilastointiin, tutkimukseen, kehittämis- ja innovaatiotoimintaan, opetukseen, tietojohdantamiseen, viranomaisohjaukseen ja -valvontaan sekä viranomaisten suunnittelu- ja selvitystehtäviin. Laki mahdollistaa nykyistä laajemman sosiaali- ja terveydenhuollon asiakas- ja potilastiedon hyödyntämisen muussa kuin kyseisen tiedon alkuperäisessä käyttötarkoituksessa sosiaali- ja terveydenhuollon palvelujärjestelmässä.

Toisiolain keskeinen päätavoite edellä kuvatun tiedon laajemman hyödyntämisen ohella on suojata kaikessa sosiaali- ja terveystietojen toissijaisessa käsittelyssä henkilötiedot siten, että kansalaisten luottamusta voidaan vahvistaa suhteessa heidän tietojensa käsittelyyn toissijaisessa käyttötarkoituksessa. Toisiolaki mahdollistaa aiempaa paremman tietoturvan sosiaali- ja terveydenhuollon arkaluonteisten henkilötietojen toissijaisessa käsittelyssä. Tämä vahvistaa osaltaan myös luottamusta sosiaali- ja terveydenhuollon palvelujärjestelmään yleisesti. Sosiaali- ja terveysvaliokunta on mietinnössään (StVM 37/2018 vp) pitänyt välttämättömänä, että sosiaali- ja terveydenhuollon arkaluonteisia henkilötietoja käsitellään tietoturvallisesti siten, että ne eivät paljastu sivullisille. Sosiaali- ja terveysalan tietolupaviranomaisen (jäljempänä Tietolupaviranomainen) perustamisessa sekä ehdotettujen lakien toimeenpanossa tulee valiokunnan näkemyksen mukaan hyödyntää tarvittavaa korkean tason osaamista siten, että huomioidaan teknologian kehitys. Tietolupaviranomaisen käynnistäminen sekä toiminnan suunnittelu tulee sosiaali- ja terveysvaliokunnan näkemyksen mukaan toteuttaa siten, että siinä turvataan korkeatasoinen tietosuojan ja tietoturvan osaaminen sekä kokonaisuudessaan riittävät voimavarat.

Sosiaali- ja terveysvaliokunta on edellä mainitussa mietinnössään todennut, että valtioneuvoston on tarpeen seurata ja arvioida sääntelyn toimeenpanoa ja toimivuutta huolellisesti siten, että lainsäädäntö vastaa teknisen kehityksen muutosten mukanaan tuomiin tarpeisiin siten, että varmistetaan tietojen toissijaisen käytön sujuva toteutus, korkean tason tietoturva arkaluonteisten sosiaali- ja terveystietojen käsittelylle sekä tietojen toissijaisen käytön vaikuttavuus sosiaali- ja terveydenhuollon palvelujärjestelmälle. Valiokunta korosti, että ehdotetun järjestelmän kokonaisuuden sekä sitä sääntelevän lainsäädännön toimivuutta tulee seurata ja arvioida huolellisesti myös silloin, kun toiminta on jo käynnissä, jotta toiminnassa hyödynnetään asianmukaisella tavalla teknologian kehitystä turvaamaan henkilötietojen suoja. Tarvittaessa lainsäädäntöä tulee myös muuttaa.

Tietoturvallinen käyttöympäristö on toisiolain hallituksen esitykseen ([HE 159/2017 vp](#)) kirjoitettu keskeinen toimi, joka turvaa yksilön henkilötietojen suojaa. Tietoturvaisella käyttöympäristöllä on merkittävä rooli väärinkäytösten estämisessä ja kyberturvallisuuden toteuttamisessa. Se on myös kilpailuetu Suomelle, koska voimme siten osoittaa, että täällä huolehditaan vahvasti arkaluonteisten henkilötietojen suojasta.¹ Myös Euroopan parlamentin ja neuvoston asetuksessa (EU) 2016/679, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (jäljempänä *yleinen tietosuoja-asetus*) edellytetään riittäviä suojatoimia, kun käsitellään arkaluonteisia henkilötietoja.

Toisiolain 60 §:n 1 momentissa säädetään siirtymäajasta, jonka jälkeen Tietolupaviranomainen voisi luovuttaa luvansaajalle tunnisteellisia tietoja vain 20 §:n 3 momentissa tarkoitettuun tietoturvaiseseen käyttöympäristöön käsiteltäviksi. Toisiolain 20 §:n 1 momentin mukaan Tietolupaviranomainen ylläpitää yksin tai yhdessä muiden viranomaisten kanssa tietoturvallista käyttöympäristöä, jossa voidaan varmistaa Tietolupaviranomaisen tai muun tässä laissa tarkoitettun viranomaisen toisiolain nojalla luovuttamien tietojen tietoturallinen, luvan mukainen käsittely. Sanotun pykälän 3 momentin mukaan, jos tietolupahakemuksessa pyydetään luovuttamaan tietoaaineistoja käsiteltäviksi muussa kuin 1 momentissa tarkoitettussa käyttöympäristössä, hakemuksessa on erikseen perusteltava syyt, joiden vuoksi tämä on välttämätöntä. Tietolupaviranomainen tai muu toisio-laissa tarkoitettu viranomainen saa tällöin luovuttaa tiedot hakijalle vain, jos käyttöympäristö täyttää toisiolain 20 §:n 2 momentissa ja 21—29 §:ssä säädetty edellytykset.

Tunnisteellisia henkilötietoja luovutetaan tyypillisesti tutkimustarkoituksissa yhdistettäväksi terveydenhuollon potilasasiakirjoissa oleviin tietoihin. Tällöin niitä usein käsitellään toimintayksikön omissa, tutkijoille tarkoitetuissa tietojärjestelmissä, joissa ei toistaiseksi ole toteutettuna kaikkia edellytetyjä tietosuoja- ja turvavaatimuksia. Siirtymäajan tarkoitus oli turvata se, ettei terveydenhuollon tutkimus tyrehdy lain voimaantultua. Asianomaisten toimintayksiköiden olisi kuitenkin velvollisuus huolehtia, että tutkijoiden käyttämät tietojärjestelmät vastaavat viimeistään siirtymäajan päätyttyä 20 §:n 3 momentissa asetettuja vaatimuksia.

Lain valmistelun yhteydessä arvioitiin, että tietoturvallisten käyttöympäristöjen rakentaminen veisi hyväksymisen jälkeen noin kaksi vuotta ja siirtymäajaksi esitettiin 1.5.2021, joka on nyt myös toisiolain 60 §:ssä säädetty siirtymäaika.

Tietolupaviranomainen saadun tiedon mukaan 1.5.2021 mennessä ei kenelläkään toimijalla, Tietolupaviranomaista itseään lukuun ottamatta, ole toisiolain 20 §:n edellyttämää tietoturvallista käyttöympäristöä, jonne tietoaaineistoja voisi luovuttaa luvansaajan käsiteltäväksi. Myöskään ulkomaisilla toimijoilla ei ole kattavaa tietoa tästä auditointivelvoitteesta, eikä kukaan ulkomainen toimija ole ryhtynyt auditoimaan omia järjestelmiä toisiolain mukaisiksi. Tietolupaviranomaisen käyttöympäristö ei myöskään vielä pysty käsittelemään kaikkea sellaista tietoaaineistoa, joita erityisesti lääketieteen tutkimuksessa olisi tarve käsitellä. Esimerkkinä voi mainita terveydenhuollon kuvantamisaineistot (esimerkiksi röntgenkuvat, ultraäänikuvat ja EKG-talenteet), jotka kuuluvat aineistona toisiolain soveltamisalan piiriin. Kuvantamisaineistot edellyttävät käytännössä laitteistoja ja ohjelmistoja, joita on vain terveydenhuollon toimijoilla. Kuvantamisaineiston käsittely edellyttää myös lähes aina sitä, että käsittelyn tekee tai siihen osallistuu kyseiseen alaan erikoistunut lääkäri. Tämänkin vuoksi on tärkeää, että muun muassa mer-

¹ ks. asiantuntijalausunto tietoturvasta <https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-229672.pdf>

kittävimmit terveydenhuollon toimijat Suomessa ehtivät auditoida omat käyttöympäristöt vaatimuksia vastaaviksi ja siten pystyvät käsittelemään näitä erityisiä tietoaineistoja myös omissa ympäristöissään.

Toisiolain 55 §:n mukaan tietoluvan saajalla on oikeus ilmoittaa Tietolupaviranomaisen nimeämälle vastuuhenkilölle kliinisesti merkittävästä löydöksestä, jonka perusteella olisi mahdollista ehkäistä tietyn potilaan terveyteen liittyvää riskiä tai parantaa merkittävästi hoidon laatua.

Jos ilmoituksen perusteena olevat tiedot ovat pseudonymisoituja, sanotun vastuuhenkilön on selvitettävä, ketä tai keitä tieto koskee. Kun Tietolupaviranomaisen vastuuhenkilöllä on tiedossaan henkilö tai henkilöt, joita ilmoitus koskee, vastuuhenkilön on toimitettava ilman aiheetonta viivytystä tiedot Terveiden ja hyvinvoinnin laitoksen nimeämälle asiantuntijalle. Asiantuntijan on yhteistyössä laitoksen nimeämien muiden asiantuntijoiden kanssa arvioitava tiedon merkittävyys ja sen pohjalta toteutettavissa olevien toimenpiteiden odotettavissa oleva hyöty. Jos hyöty arvioidaan niin ilmeiseksi, että tutkittava olisi tärkeää saada hoidon piiriin, Terveiden ja hyvinvoinnin laitoksen asiantuntijan on ilmoitettava löydöksestä kunkin henkilön terveydenhuollosta alueellisesti terveydenhuoltolain nojalla vastuussa olevalle toimintayksikölle. Toimintayksikön on otettava yhteys potilaaseen ja selvitettävä, haluaako tämä tiedon kliinisesti merkittävästä löydöksestä ja sen perusteella mahdollisesti tehtävistä tutkimus- ja hoitotoimenpiteistä sekä niistä odotettavissa olevasta hyödystä.

Potilaalla on oikeus kieltää kliinisesti merkittävän löydöksen perusteella tehtävät yhteydenotot. Kielto kirjataan asiakastietolain 14 a §:ssä tarkoitettuun potilaan tiedonhallintapalveluun. Potilas voi tehdä kiellon kirjallisesti missä tahansa julkista terveydenhuoltoa tuottavassa toimintayksikössä taikka sähköisesti asiakastietolain 19 §:ssä tarkoitetun kansalaisen käyttöliittymän välityksellä.

Kansaneläkelaitokselta ja Terveiden ja hyvinvoinnin laitokselta saadun tiedon mukaan, koska toisiolain 55 §:n vaatimat muutokset edellyttävät muutoksia potilastietojärjestelmiin, valtakunnallisiin tietojärjestelmäpalveluihin ja tutkijoiden tietoturvallesiin käyttöympäristöihin, lain edellyttämiä muutokset olisi perusteltua yhdistää uuden asiakastietolain hallituksen esityksessä (HE 212/2020 vp) esitettyyn tahdonilmaisupalvelua ja kieltoja, koskeviin muutosehdotuksiin. Muutoksia ei ole tehty, mutta muutokset olisi toteutettavissa siten, että toisiolain 55 § voisi astua voimaan 1. päivänä tammikuuta 2024.²

Valmistelu

Hallituksen esitys on valmisteltu sosiaali- ja terveysministeriön ja Tietolupaviranomaisen sisäisenä virkamiestyönä.

² Kelan ja THL:n näkemyksen mukaan kyseessä on todella laaja uusi prosessi, jossa on monia toimijoita ja työkaluja (Findata, tutkijat, uusi tutkijoiden käyttöliittymä, kansalaiset, Kanta-palvelut, terveydenhuolto, potilastietojärjestelmät). Terveidenhuoltoon ja valtakunnallisiin tietojärjestelmäpalveluihin kohdistuu seuraavana kahtena vuonna lukuisia muita lainsäädännön toimeenpanovaatimuksia mm. asiakastietolain muutosten toimeenpano, henkilötunnusuudistus 1.1.2023 mennessä sekä sote-uudistuksen edellyttämä toimeenpano. Edellä mainitun takia he pohtivat, voisiko toimeenpanon siirtymäaika olla jopa 1.1.2025.

Sosiaali- ja terveysministeriö järjesti 12.4.2021 kuulemistilaisuuden keskeisille toisiolain rekisterinpitäjille ja viranomaisille, jossa esiteltiin toisiolain 60 §:n 1 momentin siirtymäsääntöön esitettävät muutokset. Kuulemistilaisuuteen osallistui XX henkilöä. Kuulemistilaisuuden lisäksi luonnoksesta hallituksen esitykseksi on voinut antaa kirjallisen lausunnon 13.4.2021 mennessä. Lausuntoja esitykseen saapui määräaikaan mennessä yhteensä XX kappaletta.

Hallituksen esityksen valmisteluasiakirjat ovat julkisessa palvelussa osoitteessa [https://stm.fi/hankkeet/tunnuksella STM047:00/2021](https://stm.fi/hankkeet/tunnuksella_STM047:00/2021).

2 Nykytila ja sen arviointi

Yleisen tietosuoja-asetuksen 42 artiklan mukaisia hyväksytyjä tietosuojasertifiointimekanismeja ei vielä ole käytössä. Auditointia voidaan kuitenkin pitää esiasteena tietoturva- tai tietosuojaa koskevan sertifikaatin hankkimiseksi. Sertifikaatti toimii todistuksena sekä sovellettavien standardien että auditoinnissa käytettyjen kriteerien ja vaatimusten täyttämistä. Näiden käyttöä olisi syytä kannustaa eri toimialoilla täydentämään rekisterinpitäjän sisäistä valvontaa ja viranomaisvalvontaa vastaavalla tavalla kuin nyt käytetään tietoturva-auditointeja.³

Suomessa hyödynnetään muun muassa kansallista turvallisuusauditointikriteeristöä Katakria. Katakri-kriteeristö itsessään ei aseta tietoturvallisuudelle ehdottomia vaatimuksia, vaan siihen kootut vaatimukset perustuvat voimassa olevaan lainsäädäntöön ja Suomea sitoviin kansainvälisiin tietoturvavelvoitteisiin. Vaikka Katakri-kriteeristöä käytetään ensisijaisesti turvallisuusluokitellun tiedon käsittelyn arviointien yhteydessä, kriteeristöä voidaan hyödyntää myös yksityisen ja julkisen sektorin muussa turvallisuustyössä ja sen kehittämisessä. Lisäksi Kyberturvallisuuskeskus on laatinut pilvipalveluiden turvallisuuden arviointikriteeristön (PiTuKri), jonka tavoitteena on edistää viranomaisten salassa pidettävän tiedon turvallisuutta tilanteissa, joissa tietoja käsitellään pilvipalveluissa.

Myös terveydenhuollon B-luokan järjestelmien auditointi on vähäistä. Auditointien vähäinen käyttöaste osalla toimialoista on vaikuttanut siihen, että prosessien, toimintojen ja tietojärjestelmien tietoturvallisuuden taso voi vaihdella merkittävästi eri toimialoilla. Prosessien ja toimintojen auditoinnin pitäisi olla luonnollinen osa kriittisten toimialojen riskinhallintaa. Auditointien määrän lisääminen edellyttää sääntelyn tarkastelun ohella toimintakulttuurin muutosta niin julkisella kuin yksityisellä sektorilla. Kaikki auditointitoiminta edellyttää toiminnan kohteelta rahallisia panostuksia. Tämän osalta tulee kuitenkin huomioida, että audi-

³ Tietoturvan ja tietosuojan parantaminen yhteiskunnan kriittisillä toimialoilla työryhmän loppuraportti https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/162783/LVM_2021_1.pdf?sequence=1&isAllowed=y. Työryhmässä on arvioitu, että myös tietosuojaa koskevien arviointien osalta erityisesti yleisen tietosuoja-asetuksen mukaisten tietosuojan sertifiointimekanismien käyttöä olisi mahdollista lisätä. Loppuraportissa todetaan, että ”ulkopuolisten sertifiointielinten myöntämät tietosuojasertifiointit olisivat yksi tietosuoja-asetuksen mukainen keino rekisterinpitäjän osoittaa, että tietosuoja-asetusta ja erityisesti käsittelyn turvallisuuteen liittyviä vaatimuksia noudatetaan. Ulkopuolisten riippumattomien sertifiointielinten tekemät arviot lisäisivät toiminnan uskottavuutta, laajentaisivat merkittävästi kyvykkyyksiä arvioida säännösten mukaisuutta (valvontaa) ja samalla se toisi rekisterinpitäjille tärkeää osaamista tietosuojan kehittämiseen. Tämä edellyttäisi sertifiointielinten akkreditointia, joka on tietosuojavaltuutetun tehtävä, sekä tietosuojan sertifiointin liiketoiminnan käynnistämistä.”

toinnin yksityiskohtaisuus ja tarkistettavan kohteen laajuus vaikuttavat suoraan kyseessä olevan auditoinnin kustannuksiin. Näin ollen yksittäisten, kriittisiksi tunnistettujen, tietojärjestelmien tai prosessien auditoinnit ovat kokoluokaltaan moninkertaisesti pienempiä panostuksia kuin suuryrityksen tai kunnan digitaalisen palveluympäristön laajamittainen auditointi.

Tietoturvaa koskevia auditointeja tekevät Suomessa Liikenne- ja viestintäviraston Kyberturvallisuuskeskus, erikseen hyväksytyt arviointilaitokset (mm. KPMG ja Nixu), eräät tietoturvayritykset ja organisaatioiden sisäiset riippumattomat toimijat. Korkeimmasta tarkastustasosta vastaavat Kyberturvallisuuskeskus ja erikseen hyväksytyt arviointilaitokset, joita on Suomessa tällä hetkellä vain muutamia. Toimijoiden omavalvonta ja sisäiset riippumattomat auditoinnit ja tarkastukset eivät vastaa ulkopuolisen arviointilaitoksen tekemää tarkastusta, mutta ne voidaan nähdä yhtenä lisäkeinona tietoturvan ja tietosuojan parantamiseksi. Lisäksi yksityisen sektorin toimijoilta on mahdollista hankkia erilaisia koulutus- ja konsultointipalveluita tietoturvan ja tietosuojan parantamiseksi.

Toisiolain 24 §:n mukaan tietoturvallisten käyttöympäristön on täytettävä tietoturvaa ja tiedon siirron yhteentoimivuutta koskevat vaatimukset, jotka perustuvat viranomaisten antamiin määräyksiin, suosituksiin ja näiden osoittamiin, tietoturvalliseen käyttöympäristöön soveltuviin standardeihin. Tietolupaviranomainen antaa tarkemmat määräykset muiden palveluntarjoajien tietoturvallisille käyttöympäristöille asetettavista vaatimuksista. Vaatimuksissa on edellytettävä vastaavaa tietoturvan tasoa kuin Tietolupaviranomaisen omassa käyttöympäristössä vaaditaan. Toisiolain 25 §:n mukaan käyttöympäristön tietoturvallisuus on osoitettava toisiolain 26 §:n mukaisella tietoturvallisuuden arviointilaitoksen antamalla todistuksella. Tietolupaviranomainen voi antaa tarkempia määräyksiä tietoturvallisuuden osoittamisesta noudatettavista menettelyistä.

Tietolupaviranomainen antoi toisiolain mukaisen määräyksen tietoturvallisista käyttöympäristöistä 5.10.2020. Tietolupaviranomaiselta saadun tiedon mukaan tämän jälkeen määräystä ja sen toimeenpanoon liittyviä toisiolain edellyttämiä toimia on käyty loppuvuoden 2020 aikana läpi Liikenne- ja viestintäviraston (Traficom) ja Sosiaali- ja terveystieteiden valvontavirasto (Valvira) kanssa. Tietolupaviranomaisen mukaan tämä yhteinen läpikäynti on ollut tarpeen, jotta Traficom on pystynyt muokkaamaan omaa ohjeistustaan arviointilaitoksille ja ottamaan huomioon ohjeistuksessa uuden määräyksen. Valvira on tarvinnut tiedon määräyksen sisällöstä, jotta se on pystynyt viemään eteenpäin tietoturvallisten käyttöympäristöjen julkista rekisteriä. Tietolupaviranomaisen mukaan on tarvittu yhteistä läpikäyntiä ja yhteydenpitoa arviointilaitoksiin. Arviointilaitosten kanssa on ollut tarve käydä uutta määräystä läpi, jotta syntyy käsitys siitä, mitä määräyksen sisältämät vaatimukset tarkoittavat auditoinnille.

Tämä kuvattu läpikäynti on kestänyt noin 4 kuukautta. Se on ollut välttämätöntä määräyksen täytäntöönpanoon kannalta. Sitä ei myöskään olisi voitu aloittaa ennen kuin Tietolupaviranomainen olisi antanut määräyksen ja ennen kuin olisi ollut tiedossa, minkälaisia vaatimuksia määräys sisältäisi. Valmistelun aikana syntyi myös perustellumpi käsitys, minkälainen työ määrä vaaditaan sekä kuinka kauan auditointi uuden määräyksen perusteella ennakoitavan. Ainakin osa vaatimuksista ovat uusia auditointilaitoksille, koska määräys sisältää sellaisia vaatimuksia, joita ei esimerkiksi ole sisällytetty nykyisiin sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetun lain (159/2007, jäljempänä *asiakastietolaki*) mukaisiin terveydenhuollon A-luokan tietojärjestelmien vaatimuksiin. Tietolupaviranomaiselta saadun tiedon arviointilaitokset ovat arvioineet, että määräyksen mukainen auditointi kestää noin kaksi kalenterikuukautta. Auditointi edellyttää myös valmistautumista ennen kuin varsinaiseen auditointiin voidaan ryhtyä. Muun muassa tekniset kuvaukset ja dokumentaatiot tulee olla laadittuna, riittävän kattavia ja ne tulee arkistoida. Auditoidun toimijan

tulee myös itse käydä läpi määräyksen vaatimukset ja varmistaa, että sen toimintatavat ovat määräyksen mukaisia. Vasta tämän jälkeen voidaan ryhtyä varsinaiseen auditointiin.

Tietolupaviranomainen on myöntänyt tietolupia 1.4.2020 alkaen yksilötasoiseen aineistoon. Lupaharkinnassa on otettu huomioon, että Tietolupaviranomaisen oma käyttöympäristö on ensisijainen ympäristö, jonne tietoaineistoja voi luovuttaa. Siirtymäajan aikana on kuitenkin mahdollista luovuttaa tietoaineisto myös muuhun kuin Tietolupaviranomaisen ympäristöön. Laissa ei ole erityisiä säännöksiä siitä, missä tilanteissa tai millä perusteella tietoaineisto voidaan siirtymäajan voimassa ollen luovuttaa muualle kuin Tietolupaviranomaisen ympäristöön. Toisiolain mukaan ennen 1.5.2021 tietoja voidaan luovuttaa luvansaajan käsiteltäväksi, vaikka tietolupahakemuksessa ei osoitettaisi lain 20 §:n 3 momentissa ja 21–34 §:ssä tietoturvaliseltä käyttöympäristöltä edellytettäviä vaatimuksista tietojen käsittelylle. Toisiolain 43 §:n 4 momentin mukaan lupa voidaan antaa, jos on ilmeistä, ettei tiedon antaminen loukkaa niitä etuja, joiden suojaus salassapitovelvollisuus on säädetty. Lupa on lisäksi liitettävä tietojen käsittelyn suojaustoimenpiteitä koskevat riskien mukaiset vaatimukset ja muut yksityisen edun suojaamiseksi tarpeelliset määräykset. Toisiolain 18 § sisältää yleiset tietoturva-vaatimukset, jotka ovat olleet voimassa jo heti lain voimaantulua. Sen mukaan, kun henkilötietoja käsitellään tämän lain nojalla, käsittelyn riittävä tietoturvalisuus on varmistettava riskienhallinnalla, pääsynhallinnalla, aktiivisella valvonnalla sekä noudattamalla tietoturvalisuuden ja tietosuojan toteutuksesta ja valvonnasta vastaavan viranomaisen määräyksiä ja ohjeita. Erityistä huomiota on kiinnitettävä käyttörajoitusten sekä salassapitovelvoitteen toteuttamiseen.

Lainsäädäntö sisältää siten vaatimuksia tietoturva- ja suoja- ja näiden varmentamisesta myös siirtymäajalle. Samanaikaisesti Tietolupaviranomaisen on otettava huomioon lain toinen tavoite, joka on ollut tutkimustoiminnan turvaaminen ja lupakäytäntöjen nopeuttaminen. Tietolupaviranomainen on luovuttanut tietoaineistoja muuhun kuin sen omaan käyttöympäristöön seuraavissa tilanteissa:

- Jos kyseessä on ollut jo käynnissä oleva tutkimushanke, jossa on haettu Tietolupaviranomaiselta esimerkiksi jatkoaikaa. Tietolupaviranomainen myöntää jatkoajan tilanteessa, joissa alkuperäinen tutkimuslupa on koskenut useiden rekisterinpitäjien aineistoja. Näissä tilanteissa aineisto sijaitsee jo jossakin, sen mukaan kuin mitä alkuperäinen lupa tai luvat ovat määritelleet.
- Tietolupaviranomainen ei ole edellyttänyt, että jatkoajan vuoksi tutkimusaineisto tulisi siirtää toiseen paikkaan, siis tietolupaviranomaisen ympäristöön. Myös sensitiivisten tietoaineistojen siirto tai liikuttelu muodostaa itsessään riskiä tietoturvalle - ja suojaalle. Tutkimusaineistot voivat olla hvvinkin laajoja, ja osa aineistoista voi olla myös paperisia muodoltaan. Tietolupaviranomainen ei käsittele paperia, vaan sen käsittely pohjautuu täysin sähköiseen käsittelyyn ja siihen, että aineistot ovat sähköisiä. Esimerkiksi tällaisissa tilanteissa
- Tietolupaviranomainen on antanut luvan tietoaineistojen käsittelyyn myös silloin, kun luvansaajana on toiminut ja tietojen sijaintipaikkana on ollut terveydenhuollon toiminnanharjoittaja. Tällaisella toimijalla on jo itsellään hallinnassa merkittäviä määriä sensitiivistä tietoa, ja sitä koskevat myös muun lainsäädännön vaatimukset tietojen tietoturvalisesta käsittelystä. Lisäksi on voinut olla kyse kuvantamisaineistoista, joita ei voida käsitellä tietolupaviranomaisen omassa käyttöympäristössä.

Tietolupaviranomainen ei ole antanut tietolupaa tietojen käyttöön, jos se on harkinnut saamiensa tietojen pohjalta, että tietojen käsittely ehdotetussa paikassa aiheuttaisi liian suurta ris-

kiä tietoturvalle- tai suojalle. Tällaisia tapauksia on voinut olla esimerkiksi silloin, jos luvan- hakija on ilmoittanut, että aineistoa pidetään usb-muistitikuilla tutkimuksen harjoittajan työ- huoneessa. Tilanteissa, joissa tietoaineistoa on haluttu siirtää ulkomaille, on Tietolupaviran- omainen harkinnut tapaus kerrallaan, miltä tilanne näyttää tietosuojan- ja tietoturvan kannalta.

Lain valmistelun yhteydessä arvioitiin, että tietoturvallisten käyttöympäristöjen rakentaminen veisi hyväksymisen jälkeen noin kaksi vuotta ja siirtymäajaksi esitettiin 1.5.2021. Tietolupavi- ranomainen saadun tiedon mukaan 1.5.2021 mennessä ei kenelläkään toimijalla, Tietolupavi- ranomaista itseään lukuun ottamatta, ole toisiolain 20 §:n edellyttämää tietoturvallista käyt- töympäristöä, jonne tietoaineistoa voisi luovuttaa luvansaajan käsiteltäväksi. Nykyinen ti- lanne johtaa siihen, että 1.5.2021 alkaen usea tutkimus uhkaa loppua tai muuttua mahdotto- maksi, koska ei ole tietoturvallisia käyttöympäristöjä, jonne tietoaineiston voisi tietoluvan pe- rusteella luovuttaa. Tietolupaviranomaisen käyttöympäristö ei kuitenkaan vielä pysty käsitte- lemään kaikkea sellaista tietoaineistoa, joita erityisesti lääketieteen tutkimuksessa olisi tarve käsitellä. Esimerkkinä voi mainita terveydenhuollon kuvantamisaineistot (esimerkiksi rönt- genkuvat), jotka kuuluvat aineistona toisiolain soveltamisalan piiriin. Kuvantamisaineistot edellyttävät käytännössä laitteistoja ja ohjelmistoja, joita on vain terveydenhuollon toimijoilla. Kuvantamisaineiston käsittely edellyttää myös lähes aina sitä, että käsittelyn tekee tai siihen osallistuu kyseiseen alaan erikoistunut lääkäri. Tämänkin vuoksi on tärkeää, että muun muassa merkittävimmät terveydenhuollon toimijat Suomessa ehtivät auditoida omat käyttöympäristöt vaatimuksia vastaaviksi ja siten pystyvät käsittelemään näitä erityisiä tietoaineistoja myös omilla ympäristöissään. Asiantuntija-arvioiden mukaan tämä voisi tapahtua 1.5.2022 men- nessä. Lisäksi erityisesti kansainvälisten tutkimusten turvaamista ja tietoturvaa koskevat haas- teet on tuotu esille hallituksen esityksen kohdassa toimeenpano ja seuranta.

Toisiolain 55 §:n mukaan tietoluvan saajalla on oikeus ilmoittaa Tietolupaviranomaisen ni- meämälle vastuuhenkilölle kliinisesti merkittävästä löydöksestä, jonka perusteella olisi mahdol- lista ehkäistä tietyn potilaan terveyteen liittyvää riskiä tai parantaa merkittävästi hoidon laatua.

Potilaalla on oikeus kieltää kliinisesti merkittävän löydöksen perusteella tehtävät yhteyden- otot. Kielto kirjataan asiakastietolain 14 a §:ssä tarkoitettuun potilaan tiedonhallintapalveluun. Potilas voi tehdä kiellon kirjallisesti missä tahansa julkista terveydenhuoltoa tuottavassa toi- mintayksikössä taikka sähköisesti asiakastietolain 19 §:ssä tarkoitettua kansalaisen käyttöliitty- män välityksellä.

Kansaneläkelaitokselta ja Terveyden ja hyvinvoinnin laitokselta saadun tiedon mukaan, koska toisiolain 55 §:n vaatimat muutokset edellyttävät muutoksia potilastietojärjestelmiin, valtakun- nallisiin tietojärjestelmäpalveluihin ja tutkijoiden käyttämiin tietoturvallisiin käyttöympäris- töihin, lain edellyttämät muutokset eivät ole valmiita 1.5.2021 mennessä vaan edellyttävät pal- jon enemmän työtä ja aikaa. Muutokset olisi lisäksi perusteltua yhdistää uuden asiakastietolain hallituksen esityksessä (HE 212/2020 vp) esitettyyn tahdonilmaisupalvelua ja kieltoja, koske- viin muutosehdotuksiin. Kansaneläkelaitokselta ja Terveyden ja hyvinvoinnin laitokselta saa- dun tiedon mukaan muutokset olisi toteutettavissa aikaisintaan siten, että toisiolain 55 § voisi astua voimaan 1. päivänä tammikuuta 2024.

3 Tavoitteet

Esityksen tavoitteena on, että toisiolain 60 §:n 1 momentin siirtymäsäännöstä muutetaan siten, että toisiolain 20 §:n 3 momenttia ja 21–34 §:ää tietoturvaliselta käyttöympäristöltä edellytet-

tävistä vaatimuksista sovellettaisiin vasta, kun alan keskeiset toimijat ovat voineet ilman aiheutonta viivytystä auditoida tietoturvalliset käyttöympäristönsä. Hallituksen näkemyksen mukaan tämä tulee tapahtua etupainotteisesti ilman aiheutonta viivytystä, mutta kuitenkin viimeistään 1 päivästä toukokuuta 2022. On oletettava, että viimeistään silloin alan toimijoiden tietoturvalliset käyttöympäristöt on auditoitu toisiolain edellyttämällä tavalla siten, että luvansaajan auditoituun tietoturvalliiseen käyttöympäristöön tietoaineistoja voisi luovuttaa toisiolain mukaisesti. Ennen mainittua ajankohtaa tietoja voitaisiin kuitenkin luovuttaa luvansaajan käsiteltäväksi toisiolain 51 §:n 1 ja 2 momentin nojalla, vaikka tietolupahakemuksessa ei osoitettaisi toisiolain 51 §:n 3 momentissa tarkoitettua tietoturvallista käyttöympäristöä tietojen käsittelylle.

Sen sijaan toisiolain 60 §:n 1 momentissa olevaa siirtymäaika koskien lain 19 §:ää lokitiedoista ei tässä yhteydessä esitetä muutettavaksi. Lokitietoja koskeva vaatimus on keskeinen keino, joilla rekisteröity, rekisterinpitäjä ja viranomaiset voivat seurata ja valvoa henkilötietojen käsittelyä. Lisäksi vastaava velvoite koskee viranomaisia jo tiedonhallintalain (906/2019) perusteella.⁴ Tietolupaviranomainen itse kerää edellä mainittua lokitietoa.

Koska toisiolain 55 §:n merkittäviin kliinisiin löydöksiin perustuvien oikeuksien, velvoitteiden ja toimenpiteiden täytäntöönpano edellyttää muutoksia myös potilastietojärjestelmiin, valtakunnallisiin tietojärjestelmäpalveluihin ja tietoturvalliisiin käyttöympäristöihin, lain edellyttämiä muutoksia ei ole mahdollista toteuttaa 1.5.2021 mennessä. Muutokset olisivat lisäksi perusteltua yhdistää uuden asiakastietolain hallituksen esityksessä (HE 212/2020 vp) esitettyyn tahdonilmaisupalvelua ja kieltoja, koskeviin muutosehdotuksiin. Kansaneläkelaitokselta ja Terveystieteiden ja hyvinvoinnin laitokselta saadun tiedon mukaan muutokset olisi tehtävissä siten, että toisiolain 55 § voisi astua voimaan aikaisintaan 1. päivänä tammikuuta 2024.

4 Ehdotukset ja niiden vaikutukset

4.1 Keskeiset ehdotukset

Keskeisenä ehdotuksena on, että toisiolain 60 §:n 1 momentin siirtymäsäännöstä muutetaan siten, että toisiolain 20 §:n 3 momenttia ja 21–34 §:ää tietoturvalliselta käyttöympäristöltä edellytettävistä vaatimuksista sovellettaisiin vasta, kun alan keskeiset toimijat ovat voineet ilman aiheutonta viivytystä auditoida tietoturvalliset käyttöympäristönsä.

Tietoturvallinen käyttöympäristö on toisiolain hallituksen esitykseen kirjoitettu keskeinen toimi, joka turvaa yksilön henkilötietojen suojaa. Tietoturvallisella käyttöympäristöllä on merkittävä rooli väärinkäytösten estämisessä ja kyberturvallisuuden toteuttamisessa. Se on myös kilpailuetu Suomelle, koska voimme siten osoittaa, että täällä huolehditaan vahvasti arkaluonteisten henkilötietojen suojasta. Myös yleisessä tietosuojasetuksessa edellytetään riittäviä suojatoimia, kun käsitellään arkaluonteisia henkilötietoja.

⁴ Ko. hallituksen esityksen (HE 284/2018 vp) valmistelussa tuotiin kuitenkin lokitietojen keräämisen osalta lausunnoissa esille, että ehdotettu vaatimus lokitietojen keräämisestä, jos tietojärjestelmässä käsitellään henkilötietoja tai salassa pidettäviä tietoja, on kohtuuttoman raskas ja kallis vaatimus toteuttaa nykyisiin tietojärjestelmiin.

Hallituksen näkemyksen mukaan tämä tulee tapahtua etupainotteisesti ilman aiheetonta viivytystä, mutta kuitenkin viimeistään 1 päivästä toukokuuta 2022. On oletettava, että viimeistään silloin alan keskeisten toimijoiden tietoturvalliset käyttöympäristöt on auditoitu toisiolain edellyttämällä tavalla siten, että luvansaajan auditoituun tietoturvalliseen käyttöympäristöön tietoaaineistoja voisi luovuttaa toisiolain mukaisesti. Ennen mainittua ajankohtaa tietoja voitaisiin kuitenkin luovuttaa luvansaajan käsiteltäväksi toisiolain 51 §:n 1 ja 2 momentin nojalla, vaikka tietolupahakemuksessa ei osoitettaisi toisiolain 51 §:n 3 momentissa tarkoitettua tietoturvallista käyttöympäristöä tietojen käsittelylle.

Kansaneläkelaitokselta ja Terveiden ja hyvinvoinnin laitokselta saadun tiedon mukaan, koska toisiolain 55 §:n sekä 21-29 §:n vaatimat muutokset edellyttävät muutoksia potilastietojärjestelmiin, valtakunnallisiin tietojärjestelmäpalveluihin ja tietoturvallisiin käyttöympäristöihin, lain edellyttämiä muutokset edellyttävät paljon enemmän aikaa kuin lain valmistelun yhteydessä on arvioitu ja toiminnallisuutta ei ole mahdollista toteuttaa 1.5.2021 mennessä.

Lain 55 §:n edellyttämät muutokset olisi perusteltua yhdistää asiakastietolain hallituksen esityksessä (HE 212/2020 vp) esitettyyn tahdonilmaisupalvelua ja kieltoja, koskeviin muutosehdotuksiin. Kansaneläkelaitokselta ja Terveiden ja hyvinvoinnin laitokselta saadun tiedon mukaan muutokset olisi toteutettavissa siten, että toisiolain 55 § voisi astua voimaan aikaisintaan 1. päivänä tammikuuta 2024. Tämän takia esitetään, että lain 55 §:ää kliinisistä löydöksistä sovellettaisiin 1 päivästä tammikuuta 2024.

Sen sijaan toisiolain 60 §:n 1 momentissa olevaa siirtymäaikaa koskien lain 19 §:ää lokitiedoista ei tässä yhteydessä esitetä muutettavaksi. Lokitietoja koskeva vaatimus on keskeinen keino, joilla rekisteröity, rekisterinpitäjä ja viranomaiset voivat seurata ja valvoa henkilötietojen käsittelyä. Lisäksi vastaava velvoite koskee viranomaisia jo tiedonhallintalain (906/2019) perusteella.⁵ Tietolupaviranomainen itse kerää edellä mainittua lokitietoa.

4.2 Pääasialliset vaikutukset

Tietoturva-vaikutukset

Esitys mahdollistaa sen, että useampi toimija saa oman käyttöympäristönsä auditoiduksi. Tämä parantaa mahdollisuuksia sille, että toisiolaissa tarkoitettuja turvallisia käyttöympäristöjä syntyisi useita. Uusissa auditoitavissa käyttöympäristöissä voidaan räätälöidä myös sellaisia tietojen käsittelymahdollisuuksia tai erikoistua johonkin tiettyyn käsittelyyn, joka ei välttämättä olisi tällä hetkellä mahdollista Tietolupaviranomaisen omassa käyttöympäristössä.

Suurin tietoturvaa koskeva vaikutus olisi, että kaikki toisiolain perusteella luvitettavat tietoaaineistot luovutettaisiin vain toisiolain tarkoittamiin auditoituihin tietoturvallisiin käyttöympäristöihin, siirtyisi vuodella eteenpäin. Vuoden siirtymäaika mahdollistaa siis sen, että tietoja voitaisiin käsitellä vuoden ajan lisää myös sellaisissa käyttöympäristöissä, joita ei ole auditoitu.

⁵ Kyseisen hallituksen esityksen (HE 284/2018 vp) valmistelussa tuotiin kuitenkin lokitietojen keräämisen osalta lausunnoissa esille, että ehdotettu vaatimus lokitietojen keräämisestä, jos tietojärjestelmässä käsitellään henkilötietoja tai salassa pidettäviä tietoja, on kohtuuttoman raskas ja kallis vaatimus toteuttaa nykyisiin tietojärjestelmiin.

Vaikka toisiolaissa säädetty tietoturvallinen käyttöympäristö on keskeinen asia tietoturvaa ja tietosuojaa varmistamassa, ei se kuitenkaan ole ainoa keino varmistaa tietoturva- ja tietosuojaa.

Ensinnäkin siirtymäajan siirrosta huolimatta tietoaineisto luovutetaan ensisijaisesti aina Tietolupaviranomaisen omaan tietoturvalliseen käyttöympäristöön.

Tietolupaviranomainen on tehnyt ajalla 1.4.2020-21.3.2021 yhteensä 88 tietolupapäätöstä, jotka koskevat uuden tutkimuksen aloittamista ja niihin tarvittavia toisilain alaisia tietoja. Näistä yhteensä 47:ssä on päätetty, että tieto sijoitetaan Tietolupaviranomaisen tietoturvalliseen käyttöympäristöön. Muualle luovutuksista on tehty yhteensä 41 päätöstä. Muualle luovutuksista hyvin suuressa osassa on ollut kyse joko Terveystietokeskuksen (THL) omista tutkimushankkeista tai siitä, että tieto on luovutettu Tilastokeskuksen vastaavaan tietoturvalliseen ympäristöön ("Fiona"). Lisäksi tieto-aineistoa on luovutettu yliopistosairaaloiden omiin tietoympäristöihin, tai suomalaisten yliopistojen hallinnoimiin sijainteihin. Vain muutamissa, yksittäisissä tilanteissa tieto on luovutettu joko yksityisen toimijan hallintaan tai ulkomaille. Valtaosa muualle luovutettujen tietojen hallinnoijista ovat joko kotimaisia viranomaisia tai kotimaisia yliopistosairaloita. Yliopistosairaalat hallinnoivat jo perustehtävänsä vuoksi suurta määrää terveystietoa ja ne kuuluvat asiakastietolain perusteella A-luokan järjestelmien piiriin.

Kliinisesti merkittävän löydöksen perusteella tehtävät muutokset mahdollistuvat siirtymäajan jälkeen toteutettavan tietoturvallisesti.

Tietosuojavaikutukset

Esityksellä katsotaan olevan rajoitettu vaikutus tietosuojaan, koska kyse on vain siirtymäsääntöjen muuttamisesta.

Tietolupaviranomainen on ottanut käyttöön omassa lupatoiminnassa jo nyt useita tietosuojaa parantavia toimenpiteitä, joita ei aikaisemmin ole ollut käytössä. Tietolupaviranomainen vaikuttaa siten jo nyt toiminnallaan tietoturvaa - ja suojaa parantavasti.

Tietolupaviranomainen käy luvanhakijan kanssa hyvin tarkasti läpi, mitä tietoja ja kuinka paljon haettavaan käyttötarkoitukseen tarvitaan. On tavanomaista, että hakemusprosessin aikana tietoaineisto tarkentuu merkittävästi siitä, mitä on alun perin haettu. Tietolupaviranomainen arvioi, tarvitaanko haettuun käyttötarkoitukseen niin paljoa tietoa kuin on haettu, ja onko haettava tieto käyttötarkoitukseensa sopivaa.

Tietolupapäätöksessä Tietolupaviranomainen yksilöi muuttujakohtaisesti ne tiedot, joiden käyttöön se antaa luvan. Tämäkin parantaa tietosuojaa. Luvat myönnetään vain määräaikaikaisina, keskimäärin korkeintaan viiden vuoden määräajaksi. Lupaun liitetään erilliset lupaehdot, jotka sisältävät määräyksiä tietosuojan ja turvan suojaamisen näkökulmasta. Jos ehtoja ei noudateta, on Tietolupaviranomaisella oikeus perua myöntämänsä lupa. Tietoluvan peruuttamisia ei ole ollut, mutta muutamissa tilanteissa Tietolupaviranomainen on huomauttanut hakijaa lupaehtojen noudattamisen tärkeydestä. Tietolupaviranomaisen näkemyksen mukaan sen laatimat lupapäätökset ja niihin liitettävät lupaehdot ovat tarkemmalla tasolla kuin mitä on ollut tilanne lupapäätösten suhteen ennen toisiolakia.

Tiedot kerätään ja luovutetaan luvanhakijalle ensisijaisesti siten, että aineisto tulee ensin Tietolupaviranomaiselle, joka yhdistää tietoaineistot sekä pseudonymisoi ne. Aineiston lähettäminen tapahtuu toisilaisa säädettyä sähköistä tietoturvallista käyttöpalvelua pitkin. Vain pseudonymisoitu tietoaineisto luovutetaan luvansaaajalle.

Tietolupaviranomaisen tekemässä lupapäätöksessä yksilöidään ne henkilöt, jotka saavat pääsyn tietoaineistoon. Kun tämä tietoaineisto sitten luovutetaan luvansaaajalle, on edellytyksenä se, että käyttöoikeuden saaneet henkilöt tunnistetaan vahvasti.

Yleisessä tietosuoja-asetuksessa säädetään rekisteröityjen oikeuksista. Tietolupaviranomainen on ottanut käyttöön tammikuussa 2020 menettelyitä rekisteröityjen oikeuksien toteuttamiseksi. Asiasta on tuolloin keskusteltu Tietosuojavaltuutetun toimiston kanssa, joka on pitänyt tärkeänä, että rekisteröityjen oikeuksia ryhdytään toteuttamaan tehokkaasti. Tietolupaviranomainen on luonut internet-sivuilleen oman sivuston koskien rekisteröityjen oikeuksien toteuttamista. Tietolupaviranomainen on vastaanottanut tähän saakka yhteensä 201 vastustamisilmoitusta. Osa vastustamisilmoituksista on koskenut huoltajien tekemiä vastustamisia alaikäisistä lapsistaan.

Tietolupaviranomainen merkitsee vastustamisen tiedoksi ja suodattaa muilta rekisterinpitäjiltä saaduista aineistoista ne henkilöt pois, jotka ovat tehneet vastustamisilmoituksen. Sen sijaan tämä vastustamistieto ei välity muille rekisterinpitäjille, jotka tekevät itse päätöksiä omista aineistoistaan. Vastaavasti muille rekisterinpitäjille tehdyt mahdolliset vastustamisilmoitukset eivät tule Tietolupaviranomaisen tietoon. Tämä johtuu siitä, että toisilaisa ei ole säädetty oikeutta muille rekisterinpitäjille eikä Tietolupaviranomaiselle saada rekisteröityjen oikeuksien toteuttamistarkoituksessa salassa pidettävää tietoa.

Pyyntöjä saada pääsy omiin tietoihin on tehty yhteensä 20 kappaletta.

Tietolupaviranomaiselta saadun näkemyksen mukaan muille rekisterinpitäjille ei ole kuitenkaan vastaavia ilmoituksia tai pyyntöjä juurikaan tehty. Tietolupaviranomainen on kannustanut muita rekisterinpitäjiä tähän sekä tarjonnut myös omaa toimintamallia asiassa hyödynnettäväksi. Terveys- ja hyvinvoinnin laitos on ottanut myös rekisteröityjen oikeuksien toteuttamisen käyttöönsä.

Tietolupaviranomainen on ottanut rekisteröityjen oikeuksien toteuttamisessa kaikki ne keinot käyttöönsä, joihin sillä on laillinen oikeus ja velvollisuus. Tietolupaviranomaisen näkemyksen mukaan rekisteröityjen oikeuksia toteutetaan Tietolupaviranomaisen toimesta toisilain voimaantultua aktiivisemmin kuin mikä tilanne oli ennen toisilain voimaatuloa.

Potilaalla on oikeus kieltää kliinisesti merkittävän löydöksen perusteella tehtävät yhteydenotot siirtymäajan jälkeen. Potilas voi tehdä kiellon kirjallisesti missä tahansa julkista terveydenhuoltoa tuottavassa toimintayksikössä taikka sähköisesti asiakastietolain tarkoitetun kansallisen käyttöliittymän välityksellä.

Taloudelliset vaikutukset

Siirtymäajan pidentämisellä arvioidaan olevan pääosin myönteisiä vaikutuksia tietoturvallisia käyttöympäristöjä kehittävien organisaatioiden kustannuksiin. Nykyisten järjestelmien kehittäminen entistä paremmiksi huomioiden Tietolupaviranomaisen määräys tietoturvallisten käyttöympäristöjen vaatimuksista voidaan tehdä tarkoituksenmukaisella aikataululla, mikä merkitsee kustannussäästöjä verrattuna tilanteeseen, jossa joudutaan tekemään suuria kertainvestoin-

teja kiireessä. Myös käyttöympäristöjen auditointien kustannusten arvioidaan pysyvän kohtuullisempina siirtymäajan pidentymisen vuoksi. Arviointilaitosten perimien kustannusten on tällä hetkellä kuitenkin raportoitu kasvaneen jopa kolminkertaiseksi alkuperäisiin kustannusarvioihin verrattuna. Tämän arvioidaan ainakin osittain johtuvan arviointipalveluiden kovasta kysynnästä ja arviointilaitosten resurssien niukkuudesta.

Arviointilaitosten alustavien arvioiden mukaan yksi auditointi maksaisi toimijalle useita kymmeniä tuhansia euroja. Alustavien arvioiden mukaan auditointi edellyttäisi vähimmillään noin 40 henkilötyöpäivän työajan asiaan perehtyneeltä tietoturvan auditoijalta. Helsingin ja Uudenmaan sairaanhoitopiiri on esittänyt arvioita, jonka mukaan sen oman tietoaltaan auditointi tarkoittaa miljoonien eurojen kustannuksia. Suurin kustannuserä ei ole varsinainen auditointi, vaan se, jos tai kun auditoitavaa järjestelmää joudutaan muokkaamaan määräysten kriteerien mukaiseksi. Tästä kustannustasosta ei ole vielä kattavia arvioita, koska auditointeja vasta aloitetaan. Lisäksi käyttöympäristöjen palveluntarjoajille aiheutuisi kustannuksia maksuista, joita perittäisiin Valviralle tehtävistä ilmoituksista, joiden perusteella tiedot käyttöympäristöistä tallennettaisiin Valviran ylläpitämään julkiseen rekisteriin. Maksut olisivat 300 eurosta 1200 euroon.

Toisiolain 55 §:n toteuttamisesta aiheutuu kustannuksia sekä palvelunantajille, valtakunnallisten tietojärjestelmäpalveluiden kehittämiseen että tutkijoiden käyttämiin järjestelmiin. Muutokset on kuitenkin perustelua kustannustehokkaasti yhdistää asiakastietolain (HE 212/2020) tahdonilmaisupalvelua ja kieltoja koskeviin muutoksiin. Mikäli asian vaatimat tekniset muutokset tehtäisiin vain valtakunnallisiin tietojärjestelmäpalveluihin ja muusta Kanta -kehittämisestä erillään, siitä aiheutuisi vähintään 500 000 euron kustannukset. Toisiolain 55 §:n toimeenpano aiheuttaa myös merkittäviä kustannuksia sosiaali- ja terveydenhuollon palveluntuottajille, tutkijoiden käyttämien tietojärjestelmien muutoksiin sekä vähäisiä kustannuksia Tietolupaviranomaiselle ja Terveyden ja hyvinvoinnin laitokselle. Sinällään pelkän siirtymäajan muuttamisesta ei kuitenkaan aiheudu kustannuksia.

Viranomaisvaikutukset

Esityksellä ei lisittäisi viranomaisten hallinnollista taakkaa. Tietoturvallisten käyttöympäristöjen palveluntarjoajille aiheutuisi kuitenkin tietoturvallisten käyttöympäristöjen auditoinnista kustannuksia.

Tietolupia myöntävillä viranomaisilla säilvisi edelleen harkintavalta siitä, sijoitetaanko luvittava tietoaineisto Tietolupaviranomaisen omaan käyttöympäristöön vai muualle. Tältä osin voimassa ollut tilanne jatkuisi vielä vuoden. Harkintavallan jatkaminen vuodella helpottaa lupaharkintaa, tilanteessa, jossa tietoturvallisia käyttöympäristöjä ei vielä ole ehtinyt syntyä.

Toisiolain 6 §:n 1-8 kohdassa mainituilla organisaatioilla ja viranomaisilla on kuitenkin toisiolain 10 §:n perusteella mahdollisuus käyttää Tietolupaviranomaisen tietoturvallista käyttöympäristöä. Tietolupaviranomaisen tietoturvallinen käyttöympäristö ei kuitenkaan esimerkiksi vielä pysty käsittelemään tietäntyyppistä tietoaineistoa, esimerkiksi geenitietoa, joka on voimiltaan massiivista. Tietolupaviranomaisen ympäristössä ei myöskään voida käsitellä terveydenhuollon kuvantamisaineistoja, esimerkiksi röntgenkuvia. Kuvantamistiedon käsittelyyn tarvitaan omat, terveydenhuollon käytössä olevat laitteet. Tällaisia laitteistoja on vain sairaaloilla. Siten tietolupia myöntävä viranomainen on vaikeassa tilanteessa, jos ainoa mahdollinen ympäristö on Tietolupaviranomaisen käyttöympäristö, mikäli luvittava aineisto olisi sen laatuista, jota ei kyseisessä ympäristössä voida näistä syistä käsitellä.

Toisiolain 55 §:n voimaan tulon siirtämisellä ei ole viranomaisvaikutuksia. Vaikutukset aiheutuvat vasta, kun 55 §:n mukaisia oikeuksia, velvoitteita ja toimenpiteitä aletaan soveltaa.

Vaikutukset yritysten toimintaan

Esityksellä ei ole merkittäviä vaikutuksia yritysten toimintaan, koska kyse on vain siirtymäaikojen siirtämisestä. Esityksellä ei lisittäisi yritysten hallinnollista taakkaa, koska kyse on siirtymäajan siirtämisestä. Tietoturvallisten käyttöympäristöjen palveluntarjoajille aiheutuisi kuitenkin tietoturvallisten käyttöympäristöjen auditoinnista kustannuksia. Käytännössä nämä aiheutuvat lisäkustannukset siirrettäneen niiden käyttäjiltä perittäviin maksuihin. Lisäksi käyttöympäristöjen palveluntarjoajille aiheutuisi kustannuksia maksuista, joita perittäisiin Valviralle tehtävistä ilmoituksista, joiden perusteella tiedot käyttöympäristöistä tallennettaisiin Valviran ylläpitämään julkiseen rekisteriin. Maksut olisivat 300 eurosta 1200 euroon.

Toisiolain 55 §:n voimaantulon siirtämisellä ei ole vaikutuksia yritysten toimintaan.

Vaikutukset kansalaisten asemaan

Esityksellä olisi vaikutuksia kansalaisten asemaan lähinnä heidän henkilötietojensa suojan suhteen. Rekisteröityjen henkilöiden asema paranisi siirtymäajan jälkeen nykyisestä tässä toisiolaissa tarkoitetuilla tietoturvatoinenpiteillä, jotka ovat lähtökohtana kaikessa toisiolain mukaisessa henkilötietojen käsittelyssä.

Esityksessä ehdotettu tietojen käsittelyn lähtökohta on, että tietoja käsitellään siirtymäajan jälkeen tietoturvalisessa käyttöympäristössä, mikä merkitsee, että tietojen käsittely toteutetaan teknisessä ja fyysisessä ympäristössä, jossa tietoturva on varmistettu asianmukaisin hallinnollisin ja teknisin toimin sekä tietojärjestelmien asianmukaisin standardein. Tämä merkitsee tietojen käsittelyä tietoturvalisessa ympäristössä, johon käyttäjille annetaan käyttöoikeuksia.

Tietolupahakemusten ja niiden perusteella luovutettavien tietojen keskitetty hallinnointi ja käsittely tietoturvalisista käyttöyhteyksien välityksellä tietoturvalisessa käyttöympäristössä vähentää olennaisesti tietojen käsittelyyn liittyviä riskejä rekisteröityjen kannalta. Lisäksi tietojen käsittelyn valvonnasta on säädetty aiempaa tarkemmalla tasolla. Tarkemmat säännökset mahdollistaisivat sen, että rekisteröityjen oikeusturva toteutuu aiempaa paremmin. Rekisterinpitäjät on velvoitettu kuvaamaan tietoaineistonsa. Kun tietoaineistot on kuvattu nykyistä paremmin, myös rekistereiden yleiset tietosisällöt ovat avoimemmin kaikkien tarkasteltavissa.

Se, että ihmisille on järjestetty kanava Tietolupaviranomaisen kautta vastustaa tietojensa käsittelyä toisiotarkoituksessa, turvaa osaltaan sitä, että henkilöt, jotka eivät luota tietojensa olevan turvassa tai eivät ylipääntään halua tietojensa käytettävän toisiolaissa säädettyihin tarkoituksiin, voivat tällaisen vastustamisilmoituksen tehdä.

Toisiolain 55 §:n voimaantulon siirtämisellä ei ole suoranaisia vaikutuksia kansalaisiin. Mahdollisuus kliinisten löydösten perusteella ottaa yhteyttä kansalaisiin ja kansalaisen oikeus kieltää nämä yhteydennotot siirtyvät esitettävän siirtymäajan verran.

Vaikutukset sosiaaliset ja terveystalvuljärjestelmään

Vaikutuksia on arvioitu toisiolain hallituksen esityksessä (HE 159/2017). Sosiaali- ja terveydenhuollon palvelujärjestelmä on suurien muutosten edessä sote-uudistuksen tullessa voimaan

vuoden 2023 alussa. Palvelujärjestelmän muutoksen suunnittelun ja seurannan kannalta on tärkeää, että tietojen käyttöprosesseja saadaan muutettua ehdotetun lakiesityksen mukaiseen tietoturvaan korottavaan suuntaan.

Toisiolaki mahdollistaa tutkimusedellytysten lisääntymisen ja luo siten pohjaa korkeatasoisille tieteellisille tutkimusympäristöille ja niistä syntyville uusille innovaatioille. Uudet palveluinnovaatiot luovat edellytyksiä palvelujärjestelmän kehittymiselle asiakaslähtöisempään suuntaan ja luovat pohjaa yksilöllisemmän hoito- ja palvelukulttuurin syntymiselle.

Palvelurakenteen kehittämisen kannalta on tärkeää saada tutkimustietoa vaikuttavista hyvinvointiin ja terveyteen liittyvistä teknologioista, jotka voivat korvata esimerkiksi laitoshoidon ja siten siirtää palvelurakenteen painopistettä laitoksista ihmisten koteihin. Tällä painopisteen muutoksella on iso merkitys siinä, miltä tulevaisuuden palvelurakenne näyttää ja millaiseksi sitä pitäisi rakentaa. Lakiesitys mahdollistaa myös tutkimuksen ja tuotekehityksen ympärille rakentuvan tietoturvallisten ympäristöjen ekosysteemin syntymisen, mistä erikokoiset yksityiset ja julkiset toimijat voisivat hyötyä. Ekosysteemin syntymisen edellytyksenä on se, että laadukkaita rekisteriaineistojamme voidaan hyödyntää nopeasti ja siten, että tietojen käyttöönotosta syntyvät kustannukset ovat kohtuullisia.

Sote-uudistus painottaa sosiaali- ja terveydenhuollon integraatiota. Se hyödyttää palvelujärjestelmän näkökulmasta kaikkia asiakkaita, jotka käyttävät enemmän kuin yhtä palvelua. Kaikkein eniten se auttaa paljon palveluja käyttäviä asiakkaita ja potilaita. Vaikka järjestämislakiesitys helpottaa näiden asiakas- ja potilasryhmien saamien palveluiden seuraamista ja myös palveluketjujen seuraamista, se ei sinällään ratkaise kaikkia tiedonkeruuseen ja tietoturvaan liittyviä haasteita, vaan tarvitsee pohjakeseen ehdotetun kaltaiset tietoturvalliset käyttöympäristöt.

Toisiolain 55 §:n voimaantulon siirtämisellä ei ole suoranaisia vaikutuksia sosiaaliset ja terveyspalvelujärjestelmään. Mahdollisuus kliinisten löydösten perusteella ottaa yhteyttä kansalaisiin ja kansalaisen oikeus kieltää nämä yhteydenotot siirtyy. Siirtymäajan jälkeen toisiolain 55 §:n muutoksilla on toisiolain hallituksen esityksessä (HE 159/2017) todettuja vaikutuksia.

Vaikutukset lapsiin ja sukupuolten tasa-arvoon

Esityksellä ei arvioida olevan erityisiä lapsiin tai sukupuolten tasa-arvoon kohdistuvia vaikutuksia.

Vaikutukset työllisyyteen ja työelämään

Esityksellä on työllisyyttä lisäävä vaikutus, sillä luvanhakijoiden tulee rakentaa ja auditoida siirtymäajan aikana toisiolain mukaiset tietoturvalliset käyttöympäristöt tai hankkia vastaava palvelu Tietolupaviranomaiselta tai muilta toimijoilta. Tällä on sekä alan toimijoita, luvan hakijoita ja arviointilaitosten työmäärää lisäävä ja siten välillisesti työllisyyttä lisäävä vaatimus. Tietoturvallista käyttöympäristöä ei auditoida vain kerran vaan teknologian ja toimintakentän muutosten myötä auditointi on uusittava.

Toisiolain 55 §:n voimaantulon siirtämisellä on työllisyyttä lisäävä vaikutus, koska sen mukaiset oikeudet, velvoitteet ja toimenpiteet on toteutettava sosiaali- ja terveysalan tietojärjestelmiin, valtakunnallisiin tietojärjestelmäpalveluihin ja tutkijoiden käyttämiin järjestelmiin.

Vaikutukset rikosentorjuntaan ja turvallisuuteen

Siirtymäajan siirrolla ei sinällään ole rikosentorjuntaan lisäävä vaikutusta. Tietoturvallisilla ympäristöjä koskevilla vaatimuksilla, auditoinnilla ja lokitusvaatimuksella on kuitenkin sinällään jo rikosten torjuntaa edesauttava vaikutus. Tietoturvalliset ympäristöt ovat yksi monista keinoista turvallisuuden korottamiseen ja varmistamiseen. Täytäntöönpanossa tulee kuitenkin huolehtia, että on olemassa toimivia tietoturvaa varmistavia ratkaisuja ennen kuin laissa esitetty siirtymäsäännös astuu voimaan.

Toisiolain 55 §:n voimaantulon siirtämisellä on rikosentorjuntaan ja turvallisuutta lisäävä vaikutus, koska sen toisiolain 55 §:n mukaiset oikeudet, velvoitteet ja toimenpiteet toteutetaan tietoturvallisesti ja tietosuoja huomioon ottaen ja turvaavat kansalaisen itsemääräämisoikeuden.

Vaikutukset tietoyhteiskuntaan

Vaikutuksia on arvioitu jo toisiolain hallituksen esityksessä (HE 159/2017). Sinällään siirtymäajan muuttamisella ei ole merkittäviä vaikutuksia tietoyhteiskuntaan. Sinällään toisiolailla turvataan sosiaali- ja terveysalan tutkimus- ja innovaatiotyön jatkuminen kansallisesti sekä suomalaisten mahdollisuus osallistua kansainväliseen kehitykseen samalla kun rekisteritiedon hyödyntämisen tietosuojan ja –turvan pitkäjänteistä parantamistyötä jatketaan.

Tutkimus- ja innovaatiotoiminta tuottaa uusia hoitoja, lääkkeitä, terveysteknologian ratkaisuja, parempia toimintamalleja ja prosesseja sosiaali- ja terveydenhuoltoon. Samalla alan osaaminen kehittyy ja syntyy uutta ja kasvavaa kansainvälistä vientiä. Lääkeyritysten tutkimusinvestoinnit Suomeen olivat vuonna 2019 186 miljoonaa euroa. Terveysteknologian viennin arvo vuonna 2019 oli 2,4 miljardia euroa. Kasvua edelliseen vuoteen verrattuna 5,7 prosenttia. Terveysteknologian vienti on vahvasti ylijäämäistä. Tutkivan lääke- ja terveysteknologian työllisyysvaikutus vuonna 2018 oli noin 14 000 työllistä. Suoran rekisteritutkimuksen osuus kokonaisvaikutuksista on suhteellisen pieni. Sosiaali- ja terveystietojen hyödyntämisellä muun tutkimuksen osana on kuitenkin merkittävä vaikutus tutkimus- ja innovaatiomahdollisuuksiin.

Tutkimus- ja innovaatiotoiminnan osittainen pysähtyminen siirtymäajaksi sekä siitä seuraavat kerrannaisvaikutukset tuleville vuosille olisivat merkittävät, vaikka euromääräisiä vaikutuksia ei osata arvioida. Hoitojen, lääkkeiden, terveysteknologian laitteiden ja alan toimintamallien kehitys vaikeutuisi merkittävästi. Asiakassuhteet tutkimuskonsortioihin ja alan suurasiakkaisiin vaarantuisivat, työllisyys ja vientitulot laskisivat sekä alan myönteinen kehityssuunta vaarantuisi.

Tutkimus ja innovaatiot kasvattavat välillisesti ihmisten hyvinvointia ja terveyttä. Tutkimusyhteistyön avulla suomalaisten käyttöön saadaan alan uusinta osaamista ja hoitoja, joiden saapuminen Suomeen voisi muuten viedä vuosia. Rekisteritiedon hyödyntämisessä tapahtuva katkos haittaa siten mahdollisuuksia hyödyntää uusia, parhaita keinoja ja työkaluja vaikuttaa ihmisten hyvinvointiin ja terveyteen.

Toisiolailla on ollut selkeä myönteinen vaikutus tietosuojaan ja –turvaan sosiaali- ja terveystietojen käytössä tutkimus- ja innovaatiotoiminnassa. Siirtymäajan jatkamisella varmistetaan tämän myönteisen kehityksen jatkuminen. Alan toimijat, kuten rekisterinpitäjät ja tutkijat, ovat ryhtyneet kiinnittämään entistä enemmän huomiota tietosuojaan ja –turvaan omassa toiminnas-

saan. Lain edellytysten mukainen tietojärjestelmien kehittäminen on käynnissä ja keskeiset toimijat ovat käynnistäneet tietoturvallisten käyttöympäristöjen auditointiprosesseja. Tietosuojaan ja –turvan kehittäminen on pitkäjänteistä, jatkuvaa toimintaa.

Merkittäviin klinisiin löydöksiin perustuvat oikeudet, velvoitteet ja toimenpiteet toteutettaisiin tietoyhteiskunnan palveluita hyväksikäyttäen. Kiellon voisi siirtymäajan jälkeen tehdä sekä palvelunantajan luona mutta myös asiakastietolain mukaisen kansalaisen käyttöliittymän (Omakanta) kautta.

5 Muut toteuttamisvaihtoehdot

5.1 Vaihtoehdot ja niiden vaikutukset

Vaihtoehto 1: Palataan entisiin käytäntöihin

Tietoturvallinen käyttöympäristö on toisiolain hallituksen esitykseen kirjoitettu keskeinen toimi, joka turvaa yksilön henkilötietojen suojaa. Jos vaatimuksesta luovuttaisiin, putoaisi koko toisiolain keskeinen pohja. Tietoturvallisella käyttöympäristöllä on merkittävä rooli väärinkäytösten estämisessä ja kyberturvallisuuden toteuttamisessa. Se on myös kilpailuetu Suomelle, koska voimme siten osoittaa, että täällä huolehditaan vahvasti arkaluonteisten henkilötietojen suojasta. Myös yleisessä tietosuoja-asetuksessa edellytetään riittäviä suojoitoimia, kun käsitellään arkaluonteisia henkilötietoja.

Vaikka toisiolain tietoturvan taso on korkea, ei toisiolain tarkoituksena ole ollut vaikeuttaa tieteilistä tutkimusta vaan päinvastoin edistää sitä. Toisiolaissa on samanaikaisesti mahdollistettu tietojen käyttö toisiolaissa todettuun moneen eri käyttötarkoitukseen ja huolehdittu siitä, että rekisteröityjen henkilötietojen suoja ja luottamus sosiaali- ja terveydenhuoltopalveluihin sekä toisaalta toissijaista käyttöä kohtaan voidaan turvata. Tämä on ehdoton edellytys sille, että arkaluonteisia tietoja voidaan käsitellä toisiolain käyttötarkoituksiin.

Oppivan tekoälyn ja re-identifikaatiotekniikoiden kehityksen myötä edes anonymisointi anonymisointitehokkällä tunnettuja anonymisointitekniikoita käyttäen ei enää automaattisesti takaa, etteikö henkilöitä tai heihin liitettäviä tietoja kyettäisi jälkikäteen selvittämään useita eri anonymisoituja tietoaaineistoja yhdistelemällä.

Turvallisten käyttöympäristöjen etuna on muun muassa se, että tietoaaineistoja ei käytetä eikä säilytetä niitä käsittelevien omassa tietokoneessa, vaan käsittelykapasiteetiltaan huomattavasti tehokkaammassa käyttöympäristössä, jossa tutkijoilla ja muilla tietoja käsittelevillä on käytettävissään parhaat tekniset välineet. Luonnollisesti turvallisen käyttöympäristön hankkimisesta aiheutuu rakentamiskustannuksia, mutta käyttökustannukset ovat kohtuullisia riittävällä tietoturvan tasollakin. Kyse on yhteiskunnan infrastruktuurin rakentamisesta digitaalitaloutta varten. Olisikin tärkeää, että eri tutkimuslaitoksille ja yliopistoille turvattaisiin taloudelliset edellytykset hankkia käyttöönsä ajanmukaiset, tietoturvalliset käyttöympäristöt edistämään kansallisen tutkimusinfrastruktuurin houkuttelevuutta sekä parantamaan sen tietoturvallisuutta ja samalla tutkimuksen teknisesti toteutettavia edellytyksiä.

Turvalliset käyttöympäristöt ovat kilpailutekijä. Niitä tarjoavat tahot voivat profiloitua kansainvälisestikin ja muun muassa kilpailla osaavista tutkijoista, koska hankkeet toteutetaan laadukkailla tietoaaineistoilla ja aineistot käsitellään tietoturvallisessa ympäristössä, mikä säästää niitä hyödyntävien tahojen laite- ja muita kustannuksia. Muun muassa Turussa Auria-biopan-

killä on hyviä kokemuksia tietoturvallisista ”hauskoista, hienoista ja työtä säästävistä” käyttöympäristöistä, joilla on säästetty ylimääräistä työtä, käytettävissä on viimeisimmät työvälineet ja toiminta on tietoturvallista.

Mikään ei myöskään estä yliopistotutkijaa käyttämästä esimerkiksi yliopistollisen sairaalan tarjoamaa auditoitua tietoturvallista käyttöympäristöä. Laissa ei veloiteta muita kuin Tietolupaviranomaista perustamaan tietoturvallisten käyttöympäristön. Jokainen toimija ei siis tarvitse omaa järjestelmäänsä tietojen turvalliseen käsittelyyn.

Kansaneläkelaitokselta ja Tietolupaviranomaiselta saadun tiedon mukaan, koska toisiolain 55 §:n vaatimat muutokset edellyttävät muutoksia potilastietojärjestelmiin, valtakunnallisiin tietojärjestelmäpalveluihin ja tietoturvalisiin käyttöympäristöihin, lain edellyttämät muutoksia ei ole mahdollista toteuttaa 1.5.2021 mennessä. Toisiolain 55 §:n mukaiset yhteydenotot ja kielto-oikeus eivät olisi mahdollista, mikäli palattaisiin vanhoihin käytänteisiin.

Mikäli palattaisiin vanhoihin käytänteisiin, niin siitä huolimatta olisi edelleen rekisteröityjen oikeuksia ja erityisesti tietosuojaa ja tietoturvaa suojaamassa yleinen tietosuoja-asetus, tiedonhallintalaki ja toisiolain perusteella jo nyt toteutetut tietosuojaa ja tietoturvaa lisäävät toimenpiteet. Käyttöympäristöjen tietoturvaa voisi korottaa vapaaehtoisilla auditoinneilla ja sertifiikaateilla.

Mikäli palattaisiin vanhoihin käytänteisiin on riskinä, että kliinisten merkittävien löydösten perusteella potilaisiin otettaisiin yhteyttä ilman lakiperustaa ja potilaiden perustuslaillista tiedollista itsemääräämisoikeutta loukaten.

Vaihtoehto 2: Siirretään siirtymäaikaa esityksen sijaan vain kuudella kuukaudella

Mikäli siirtymäaikaa siirretään vain kuudella kuukaudella, tilanne olisi tietoturvan tason nostamisen osalta sinällään osin parempi kuin tällä hetkellä, mutta on kuitenkin oletettavaa, etteivät edes alan keskeiset toimijat olisi vielä auditoineet heidän ympäristöjään. Sen sijaan myös siirtymäajan aikana tietosuojaa ja tietoturvaa turvaisivat useat Tietolupaviranomaisen toisiolain perusteella käyttöön ottamatta toimenpiteet.

Kansaneläkelaitokselta ja Terveystieteiden ja hyvinvoinnin laitokselta saadun tiedon mukaan, koska toisiolain 55 §:n vaatimat muutokset edellyttävät muutoksia potilastietojärjestelmiin, valtakunnallisiin tietojärjestelmäpalveluihin ja tietoturvalisiin käyttöympäristöihin, lain edellyttämät muutokset edellyttämät muutoksia ei ole mahdollista tehdä 1.5.2021, eikä 1.5.2022. Kansaneläkelaitokselta saadun tiedon mukaan muutokset olisi toteutettavissa siten, että toisiolain 55 § voisi astua voimaan aikaisintaan 1. päivänä tammikuuta 2024

Vaihtoehto 3: Sidotaan siirtymäaikaa sote-uudistuksen voimaantuloon 1.1.2023.

Useassa sote-uudistusta koskevassa lausunnossa on todettu, että mitään muita suuria muutoksia ei tulisi asettaa sosiaali- ja terveysalan toimijoille samaan aikaan sote-uudistuksen määräaikojen kanssa, koska suurin osa resursseista menee sote-uudistuksen valmisteluun.

Kansaneläkelaitokselta ja Tietolupaviranomaiselta saadun tiedon mukaan, koska toisiolain 55 §:n vaatimat muutokset edellyttävät muutoksia potilastietojärjestelmiin, valtakunnallisiin tietojärjestelmäpalveluihin ja tietoturvalisiin käyttöympäristöihin, lain edellyttämät muutokset

edellyttämiä muutoksia ei ole mahdollista tehdä 1.5.2021, eikä 1.1.2023. Kansaneläkelaitok-
selta saadun tiedon mukaan muutokset olisi toteutettavissa siten, että toisiolain 55 § voisi as-
tua voimaan aikaisintaan 1. päivänä tammikuuta 2024. Itse asiassa muun muassa sote-uudis-
tuksen vuoksi Kansaneläkelaitos ja Terveysten ja hyvinvoinnin laitos suosittelee siirtymäajaksi
1.1.2025.

Vaihtoehto 4: Yhteiseurooppalaiset ratkaisut

Yleisen tietosuoja-asetuksen 42 artiklan mukaisia hyväksytyjä tietosuojasertifiointimekanis-
meja ei vielä ole käytössä. Näiden käyttöä olisi syytä kannustaa eri toimialoilla täydentämään
rekisterinpitäjän sisäistä valvontaa ja viranomaisvalvontaa vastaavalla tavalla kuin nyt käyte-
tään tietoturva-auditointeja.

Ulkopuolisten sertifiointielinten myöntämät tietosuojasertifiointit olisivat yksi yleisen tieto-
suoja-asetuksen mukainen keino rekisterinpitäjän osoittaa, että tietosuoja-asetusta ja erityisesti
käsitteilyn turvallisuuteen liittyviä vaatimuksia noudatetaan. Ulkopuolisten riippumattomien
sertifiointielinten tekemät arviot lisäisivät toiminnan uskottavuutta, laajentaisivat merkittävästi
kyvykkyyksiä arvioida säännösten mukaisuutta (valvontaa) ja samalla se toisi rekisterinpitä-
jille tärkeää osaamista tietosuojan kehittämiseen. Tämä edellyttäisi sertifiointielinten akkredi-
tointia, joka on tietosuojavaalutetun tehtävä, sekä tietosuojan sertifiointin liiketoiminnan
käynnistämistä.

Kansallisessa sote-tietojen toisiokäytössä ovat koko ajan olleet lähtökohtana yhteiset kansain-
väliset ja eurooppalaiset käytännöt ja ratkaisut. Kansainvälinen ja eurooppalainen kehitys on
kuitenkin vielä niin yleisellä tasolla ja käytännöt eri maissa vaihtelevat niin paljon, että tieto-
jen tietoturvallista luovuttamista käyttöympäristöihin ei voida varmentaa pelkästään niiden
avulla. Tietolupaviranomaisen määräys tietoturvallisen käyttöympäristön vaatimuksista kon-
kretisoi keskeiset ratkaisut, joita tietosuoja ja -turvan osalta tulee noudattaa. Määräys perustuu
muun muassa ISO 27001 Tietoturvaohjauksen standardiin ja kansalliseen tietoturvallisuuden
auditointityövälineeseen viranomaisille Katakriin.

Yleiseurooppalaisia toimintamalleja ja ratkaisuja henkilötason terveystietojen eurooppalaiseen
tiedonvaihtoon ja hyödyntämiseen toisiokäytössä selvitetään parhaillaan komission European
Health Data Space yhteishankkeessa. Komission on myös ilmoittanut käynnistävänsä Euro-
pan Health Data Space lainsäädäntöhankkeen vuoden 2021 aikana. Tämä lainsäädäntö luon
mahdollisesti tulevaisuudessa sellaiset yleiseurooppalaiset toimintamallit ja arviointikäytän-
nöt, joiden avulla myös käyttöympäristöjen tietoturvallisuus voidaan varmistaa koko Euroo-
pan Unioinin alueella. Toistaiseksi tällaisia yleiseurooppalaisia ratkaisuja ei kuitenkaan ole
olemassa.

Yleiseurooppalaiset ratkaisut eivät tuo ratkaisua merkittäviin kliinisiin löydöksiin perustuviin
oikeuksien, velvoitteiden ja toimenpiteiden kansalliseen toteuttamiseen.

Merkittäviin kliinisten löydöksiin liittyvää sääntelyä ei ole vastaavanlaisesti muissa maissa.
Alan yleiseurooppalaista sääntelyä tulee seurata, mutta lyhyellä aikavälillä olisi tarkoituksen-
mukaista seurata vastaavaa biopankkilakiin ja genomilakiin mahdollisesti ehdotettavia muutok-
sia.

5.2 Ulkomaiden lainsäädäntö ja muut ulkomailla käytetyt keinot

Ulkomaista lainsäädäntöä ja ulkomailla käytettyjä keinoja arviotiin toisiolain hallituksen esityksen (HE 159/2017 vp) yhteydessä sivuilla 32-58 ja edellä yhteiseurooppalaiset ratkaisut vaihtoehdossa. Vastaavia tietoturvallisia auditoituja käyttöympäristöjä kuin toisiolaissa on säädetty, ei kuitenkaan ole vielä muissa maissa.

Sen sijaan kuten työryhmäraportissa⁶ on todettu, ”tieto- ja kyberturvallisuuden ja tietosuojan kehittäminen edellyttävät ymmärrystä kybertoimintaympäristön muutoksista kansallisella ja kansainvälisellä tasolla. Kriittisillä toimialoilla tämä edellyttää, että eri toimijat jakavat ja ylläpitävät kybertoimintaympäristön tilannekuvaa koordinoitusti ja kohdennetuin tilannekatsauksin. Toimintaympäristön osalta on tärkeää huomata, että pahantahtoista kybertoimintaa ja -loukkauksia kohdistuu yksityisten yritysten lisäksi valtion instituutioihin. Tekijänä voivat tällöin olla yksityisen toimijan lisäksi valtiotoimija tai sen käyttämä bulvaani. Valtiolähtöisissä loukkauksissa korostuvat haavoittuvuuksien havaitsemisen ja korjaamisen ohella yhteisesti koordinoitujen poliittisten toimenpiteiden ja signaloimien. Suomi on osallistunut aktiivisesti yhteisen EU-politiikan ja välineiden kehittämiseen ja hyödyntämiseen, joiden avulla edistetään vastuullista valtiokäyttötymistä kybertoimintaympäristössä. Tällaisia välineitä pahantahtoisen kybertoiminnan torjuntaan EU:n tasolla ovat olleet esimerkiksi kyberdiplomatian työkalupakki ja kyberpakotteet.

Edellä mainittuihin tekijöihin voidaan kansallisen ja kansainvälisen sääntelyn ohella vaikuttaa toimialojen toimintakulttuureja kehittämällä, vapaaehtoisella yhteistyöllä viranomaisten ja palveluiden tarjoajien välillä sekä kehittämällä sekä hyödyntämällä EU-politiikkoja ja välineitä. Lisäksi on tärkeää osallistua aktiivisena osapuolena kansainväliseen yhteistyöhön, jossa edellytetään vastuullista valtiokäyttötymistä kybertoimintaympäristössä. On selvää, että hallinnonalojen välistä yhteistyötä EU- ja kansainvälisen tason vaikuttamisen tehostamiseksi kehitetään jatkuvasti. Kansainvälisen kybertoimintaympäristön kehitystä koskevaa tilannekuvaa jaetaan hallinnonalojen välillä ja tämä huomioidaan myös Suomen kansallisen toimintaympäristön arvioinnissa. Näitä laajempia kybertoimintaympäristöön liittyviä kysymyksiä ja kansainvälistä yhteistyötä kyberuhkien torjunnassa ei kuitenkaan käsitellä tämän raportin suosituk- sissa, vaan niihin liittyvää kehitystyötä tehdään jatkuvasti muun muassa kansallisen kybertur- vallisuuksstrategian toimeenpanon puitteissa.”

6 Lausuntopalaute

Sosiaali- ja terveysministeriö järjesti kuulemistilaisuuden 12.4.2021. Kuulemistilaisuuden lisäksi luonnoksesta hallituksen esitykseksi on voinut antaa kirjallisen lausunnon 13.4.2021 mennessä. Lausuntoja esitykseen saapui määräaikaan mennessä yhteensä XX kappaletta. Selvä enemmistö kannatti/ei kannattanut esitettyjä muutoksia.

Lausuntojen ja kuulemistilaisuuden johdosta hallituksen esityksessä on...

⁶ Tietoturvan ja tietosuojan parantaminen yhteiskunnan kriittisillä toimialoilla. Työryhmän loppura- portti ks. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/162783/LVM_2021_1.pdf?sequence=1&isAllowed=y

7 Säännöskohtaiset perustelut

60 §. Siirtymäsäännökset. Ehdotetun pykälän *1 momenttia* ehdotetaan muutettavaksi siten, että toisiolain 20 §:n 3 momenttia ja 21–34 §:ää tietoturvaliselta käyttöympäristöltä edellytettävistä vaatimuksista sovellettaisiin 1 päivästä toukokuuta 2022.

Tietoturvallinen käyttöympäristö on toisiolain hallituksen esitykseen kirjoitettu keskeinen toimi, joka turvaa yksilön henkilötietojen suojaa. Tietoturvalisella käyttöympäristöllä on merkittävä rooli väärinkäytösten estämisessä ja kyberturvallisuuden toteuttamisessa. Se on myös kilpailuetu Suomelle, koska voimme siten osoittaa, että täällä huolehditaan vahvasti arkaluonteisten henkilötietojen suojasta. Myös yleisessä tietosuojasetuksessa edellytetään riittäviä suojatoimia, kun käsitellään arkaluonteisia henkilötietoja.

Tietolupaviranomainen saadun tiedon mukaan 1.5.2021 mennessä ei kenelläkään toimijalla, Tietolupaviranomaisesta lukuun ottamatta, ole toisiolain 20 §:n edellyttämää tietoturvalista käyttöympäristöä, jonne Tietolupaviranomainen voisi luovuttaa tietoaineiston luvansaajan käsiteltäväksi. Tietolupaviranomaisen käyttöympäristö ei kuitenkaan vielä pysty käsittelemään kaikkea sellaista tietoaineistoa, joita erityisesti lääketieteen tutkimuksessa olisi tarve käsitellä. Esimerkkinä voi mainita terveydenhuollon kuvantamisaineistot (esimerkiksi röntgenkuvat, ultraäänikuvat ja EKG-tallenteet), jotka kuuluvat aineistona toisiolain soveltamisalan piiriin. Kuvantamisaineistot edellyttävät käytännössä laitteistoja ja ohjelmistoja, joita on vain terveydenhuollon toimijoilla. Tämänkin vuoksi on tärkeää, että muun muassa merkittävimmät terveydenhuollon toimijat Suomessa ehtisivät auditoida omat käyttöympäristöt toisiolain ja Tietolupaviranomaisen vaatimuksia vastaaviksi ja siten pystyisivät käsittelemään näitä erityisiä tietoaineistoja myös omissa ympäristöissään. Hallituksen näkemyksen mukaan tämä tulisi tapahtua ilman aiheetonta viivytystä, mutta kuitenkin viimeistään 1 päivästä toukokuuta 2022. On oletettava, että viimeistään silloin alan toimijoiden tietoturvaliset käyttöympäristöt olisi auditoitu toisiolain edellyttämällä tavalla siten, että luvansaajan auditoituun tietoturvaliseen käyttöympäristöön tietoaineistoja voisi luovuttaa toisiolain mukaisesti. Ennen mainittua ajankohtaa tietoja voitaisiin kuitenkin luovuttaa luvansaajan käsiteltäväksi toisiolain 51 §:n 1 ja 2 momentin nojalla, vaikka tietolupahakemuksessa ei osoitettaisi toisiolain 51 §:n 3 momentissa tarkoitettua tietoturvalista käyttöympäristöä tietojen käsittelylle.

Koska toisiolain 55 §:n merkittävää kliinistä löydöstä koskevat tekniset muutokset edellyttävät muutoksia potilastietojärjestelmiin, valtakunnallisiin tietojärjestelmäpalveluihin ja tietoturvalisiin käyttöympäristöihin, lain edellyttämät muutokset eivät ole toteutettavissa 1.5.2021 mennessä. Muutokset olisit kustannustehokasta yhdistää asiakastietolain hallituksen esityksessä (HE 212/2020 vp) esitettyyn tahdonilmaisupalvelua ja kieltoja koskeviin muutosehdotuksiin. Muutokset olisi toteutettavissa siten, että toisiolain 55 § voisi astua voimaan 1. päivänä tammikuuta 2024. Tämän takia 1 momenttia ehdotetaan muutettavaksi siten, että toisiolain 55 §:ää kliinisistä löydöksistä sovellettaisiin 1 päivästä tammikuuta 2024.

Pykälän *1 momentissa* olevaa siirtymäaika toisiolain 19 §:ää lokitiedoista ei tässä yhteydessä ehdoteta muutettavaksi. Lokitietoja koskeva vaatimus on keskeinen keino, joilla rekisteröity, rekisterinpitäjä ja viranomaiset voivat seurata ja valvoa toisiolain soveltamisalaan kuuluvien korostetusti arkaluonteisten henkilötietojen käsittelyä. Lisäksi vastaava velvoite koskee viranomaisia jo tiedonhallintalaissa (906/2019) säädetyllä tavalla.

8 Voimaantulo

Koska toisiolain 60 §:n 1 momentin nykyinen siirtymäsäännös on 1.5.2021 alkaen, laki on tarkoitettu tulemaan voimaan mahdollisimman pian, kun se on vahvistettu, jotta toisiolain mukaisten tietolupien myöntäminen voisi keskeytyksettä jatkua.

9 Toimeenpano ja seuranta

Sosiaali- ja terveystieteiden valiokunta on toisiolain hallituksen esityksessä (HE 159/2017) antamassaan mietinnössään todennut, että valtioneuvoston on tarpeen seurata ja arvioida sääntelyn toimeenpanoa ja toimivuutta huolellisesti siten, että lainsäädäntö vastaa teknisen kehityksen muutosten mukanaan tuomiin tarpeisiin siten, että varmistetaan tietojen toissijaisen käytön sujuva toteutus, korkean tason tietoturva arkaluonteisten sosiaali- ja terveystietojen käsittelylle sekä tietojen toissijaisen käytön vaikuttavuus sosiaali- ja terveydenhuollon palvelujärjestelmälle. Valiokunta korosti, että ehdotetun järjestelmän kokonaisuuden sekä sitä sääntelevän lainsäädännön toimivuutta tulee seurata ja arvioida huolellisesti myös silloin, kun toiminta on jo käynnissä, jotta toiminnassa hyödynnetään asianmukaisella tavalla teknologian kehitystä turvaamaan henkilötietojen suoja. Tarvittaessa lainsäädäntöä tulee myös muuttaa.

Hallituksen näkemyksen mukaan toisiolain toimeenpanoa tulee edelleen seurata yhdessä valvojen viranomaisten ja toisiolain 8 § 4 momentin korkean tason asiantuntijaryhmän kanssa varmistuen, että toiminnassa hyödynnetään asianmukaisella tavalla teknologian kehitystä turvaamaan henkilötietojen suoja.

Pääministeri Sanna Marinin hallituksen ohjelman 2019 tavoitteena on, että Suomi on kansainvälisesti houkutteleva paikka opiskella, tutkia ja investoida. Hallitusohjelmassa todettu keino olisi muun muassa, että Suomeen laaditaan pitkän aikavälin suunnitelma, jonka avulla TKI-toimintaympäristö paranee, ja sitä kautta yksityisten ja julkisten investointien ja rahoituksen tasossa tavoitellaan neljän prosentin bruttokansantuoteosuutta. Lisäksi edistetään Suomen houkuttelevuutta kansainvälisten sekä kotimaisten yritysten tutkimus- ja kehitystoiminnan sijoitusmaana ja vahvistetaan suomalaisen tutkimus- ja tiedeyhteisön kansainvälistä kilpailukykyä ja vetovoimaa panostamalla tutkimusympäristöihin ja tutkimusinfrastruktuureihin.

Suomalaisen henkilötietojen käsittelyllä tulisi lähtökohtaisesti olla samat vaatimukset koko EU-alueella, riippumatta siitä, käsitelläänkö henkilötietoja Suomessa vai muualla EU-alueella. Kansainväliset tutkijat voivat käsitellä toisiolain mukaista henkilötason rekisteritietoja ainoastaan Tietolupaviranomaisen tietoturvalisessä käyttöympäristössä tai mahdollisesti muissa siihen mennessä auditoiduissa suomalaisissa käyttöympäristöissä. Aggregoituja aineistoja voidaan kuitenkin luovuttaa vapaasti käyttöön. Lääketieteen tutkimus on luonteeltaan kansainvälistä ja tutkimusta tehdään hyvin usein kansainvälisissä konsortioissa. Vaikeutta syntyy nyt siirtymäajan määrääjän jälkeenkin erityisesti kansainvälisten tutkimusten osalta, jossa Suomesta saatava tietoaaineisto on vain osa muista maista kerättävää tietoaaineistoa, jota tutkimuksessa käytetään. Toisiolaki edellyttää, että Suomesta saatava tietoaaineisto luovutetaan vain auditoituun tietoturvalisessä käyttöympäristöön, riippumatta siitä, missä tämä käyttöympäristö sijaitsee maantieteellisesti. Ulkomaisilla toimijoilla ei ole kattavaa tietoa tästä auditointivelvoitteesta, eikä kukaan ulkomainen toimija ole ryhtynyt auditoimaan omia järjestelmiä toisiolain perusteella. Kansainvälisten tutkimusten siirtymistä suuressa määrin Tietolupaviranomaisen tai muiden suomalaisten toimijoiden käyttöympäristöihin ei voida pitää todennäköisenä vaihtoehtona. Kansainvälisillä toimijoilla ei arvioida olevan kiinnostusta suomalaisten vaatimusten mukaiseen oman käyttöympäristönsä auditointiin kuin yksittäistapauksissa. Tilanne on johtamassa siihen, että suomalaisen datan hyödyntäminen kansainvälisessä tutkimuksessa ja siten suomalaisten

tutkijoiden mahdollisuus osallistua kansainvälisiin tutkimuksiin vaikeutuu. Tutkimuksissa yhdistyy nykyisin hyvin usein ns. rekisterityyppinen tutkimus, biopankista saatavat näytteet, ja kliininen tutkimus (joko lääketutkimus tai muu lääketieteellinen, kajoava tutkimus). Tutkimuksia ei siis yleensä tehdä per lainsäädäntö, vaan tutkimuksissa yhdistyvät nykyisin useat Suomessa voimassa olevat erilaiset tutkimuslainsäädännöt. Toisiolaki on sote-tietojen ja eräiden niihin liitettävien rekisteritietojen yleislainsäädäntö toisiokäyttöön.

Sosiaali- ja terveysministeriössä on tarkoitus perustaa työryhmä, jossa alan johtavat tieturva- ja tietosuojaja-asiantuntijat, toisiolakia ohjaavat ja valvovat viranomaiset ja alan keskeiset toimijat selvittävät, millaisia tietoturva koskevia lainsäädännöllisiä vaatimuksia toisioalassa voitaisiin jatkossa asettaa, mikäli tietoaineistoja halutaan luovuttaa muihin kuin Suomessa auditoituihin tietoturvallisiin käyttöympäristöihin. Tarkoituksena on, että työryhmän työn tuloksena valmistellaan hallituksen esitysluonnos viimeistään vuoden 2021 aikana kansainvälisiin luovutuksiin sovellettavista tietoturva koskevista toisioalain säännöksistä, jolla turvataan myös kansainvälinen tutkimus tietoturvallisesti ja tietosuoja kunnioittaen.

10 Suhde muihin esityksiin

10.1 Esityksen riippuvuus muista esityksistä

Esityksellä on toisioalain 55 §:n siirtymäajan muuttamisen osalta liittymä asiakastietolain hallituksen esitykseen (HE 212/2020), joka on eduskunnan sosiaali- ja terveysvaliokunnan käsittelyssä. Toisioalain 55 §:n mukaiset muutokset olisi kustannustehokkainta ajoittaa siten, että ne tehtäisiin samalla kuin esitettyyn tahdonilmaisupalveluun ja kieltoihin on esitetty tehtävän muutoksia 1. tammikuuta 2024 mennessä.

10.2 Suhde talousarvioesitykseen

Esityksellä ei katsota olevan merkittäviä talousarvioesitysvaikutuksia. Esityksen talousarviovaikutukset on arvioitu toisioalain hallituksen esityksessä (HE 159/2017) ja asiakastietolain hallituksen esityksessä (HE 212/2020 vp). Koska kyse on vain siirtymäajan siirtämisestä, tässä yhteydessä ei ole tarvetta arvioida erityisiä talousarviovaikutuksia.

11 Suhde perustuslakiin ja säätämisjärjestys

Yksityiselämän suoja

Toisioalain hallituksen esityksessä (HE 159/2017) on arvioitu erityisesti esityksen suhdetta yksityiselämän suojaan ja julkisuusperiaatteeseen ja julkisen vallan käyttöä.

Perustuslain 10 §:n 1 momentin mukaan jokaisen yksityiselämä, kunnia ja kotirauha on turvattu. Henkilötietojen suojasta säädetään tarkemmin lailla. Säännös viittaa tarpeeseen turvata yksilön yksityiselämän suoja henkilötietojen käsittelyssä eli henkilötietojen suoja sisältyy osittain yksityiselämän suojan piiriin. Henkilötietojen suojasta voidaan säätää tarkemmin lailla, mutta samalla on turvattava tietosuojaa sellaisella tavalla, jota voidaan pitää hyväksyttävänä perusoikeusjärjestelmän kokonaisuuden kannalta.

Eduskunnan perustuslakivaliokunta on lausunnoissaan (PeVL 8/1995 vp, PeVL 26/1996 vp sekä PeVL 7, 28 ja 29/1997 vp) ottanut kantaa hallitusmuodon 8 §:n 1 momentissa (nykyinen perustuslain 10 §:n 1 momentti) säädettyyn henkilötietojen käsittelyn lailla sääätämisen velvollisuuteen. Valiokunta on todennut, että henkilötietojen suoja koskevan perusoikeussäännöksen kannalta tärkeitä sääntelykohteita ovat ainakin rekisteröinnin tavoite, rekisteröitävien henkilötietojen sisältö, niiden sallitut käyttötarkoitukset mukaan luettuna tietojen luovutettavuus ja tietojen säilytysaika henkilörekisterissä sekä rekisteröidyn oikeusturva samoin kuin näiden seikkojen sääntelemisen kattavuus ja yksityiskohtaisuus lain tasolla. Myöhemmissä lausunnoissaan (PeVL 12/2002 vp, 14/2002 vp, 51/2002 vp ja 11/2008 vp) valiokunta on uudistanut näkemystään ja todennut, että lailla sääätämisen vaatimus koskee myös mahdollisuutta luovuttaa henkilötietoja teknisen käyttöyhteyden avulla.

Henkilötietojen käsittelyä koskevan lainsäädännön on oltava kattavaa, täsmällistä ja tarkkaraista. Perustuslakivaliokunta on lisäksi kiinnittänyt useissa lausunnoissaan huomiota siihen, mihin ja ketä koskeviin tietoihin tiedonsaantioikeus ulottuu ja miten tiedonsaantioikeus sidotaan tietojen välttämättömyyteen. Viranomaisen tietojensaantioikeus ja tietojenluovuttamismahdollisuus ovat valiokunnan mukaan voineet liittyä jonkin tarkoituksen kannalta "tarpeellisiin tietoihin", jos tarkoitetut tietosisällöt on pyritty luettelemaan laissa tyhjentävästi. Jos taas tietosisältöjä ei ole samalla tavoin luetteloitu, sääntelyyn on pitänyt sisällyttää vaatimus "tietojen välttämättömyydestä" jonkin tarkoituksen kannalta (esim. PeVL 10/2014 vp, s. 6/II, PeVL 17/2016 vp, s. 2—3, PeVL 38/2016 vp, s. 2). Lisäksi mahdollisuudesta yhdistää rekisteritietoja on säädetty lailla (PeVL 17/2007 vp ja PeVL 30/2005 vp).

Ehdotetulla lailla täsmennettäisiin ja täydennettäisiin asetusta niiltä osin kuin se on kansallisen liikkumavaran puitteissa mahdollista ja tarkoituksenmukaista.

Perustuslakivaliokunnan mukaan on lähtökohtaisesti riittävää perustuslain 10 §:n 1 momentin kannalta, että sääntely täyttää EU:n yleisessä tietosuoja-asetuksessa asetetut vaatimukset. Valiokunnan mukaan henkilötietojen suoja tulee turvata ensisijaisesti EU:n yleisen tietosuoja-asetuksen ja kansallisen yleislainsäädännön nojalla. Kansallisen erityislainsäädännön säätämiseen tulee siten suhtautua pidättyvästi ja rajata sellainen vain välttämättömään tietosuoja-asetuksen salliman kansallisen liikkumavaran puitteissa (ks. PeVL 14/2018 vp, s. 4—5).

Perustuslakivaliokunnan mukaan on kuitenkin selvää, että erityislainsäädännön tarpeellisuutta on arvioitava myös tietosuoja-asetuksenkin edellyttämän riskiperustaisen lähestymistavan mukaisesti kiinnittämällä huomiota tietojen käsittelyn aiheuttamiin uhkiin ja riskeihin. Mitä suurempi riski käsittelystä aiheutuu luonnollisen henkilön oikeuksille ja vapauksille, sitä perustellumpaa on yksityiskohtaisempi sääntely. Tällä seikalla on erityistä merkitystä arkaluonteisten tietojen käsittelyn osalta (ks. PeVL 14/2018 vp, s. 5).

Yleistä tietosuoja-asetusta yksityiskohtaisemman sääntelyn tarve tulee kuitenkin perustella myös tietosuoja-asetuksen puitteissa tapauskohtaisesti. Tällöin on syytä kiinnittää huomiota myös asetuksessa omaksuttuun riskiperusteiseen lähestymistapaan. Valiokunta on painottanut, että myös arkaluonteisten henkilötietojen käsittelyä koskevan sääntelyn kohdalla on syytä pyrkiä selkeään ja ymmärrettävään lainsäädäntöön (PeVL 14/2018 vp, s. 6).

Perustuslakivaliokunta on painottanut arkaluonteisten tietojen käsittelyn aiheuttamia uhkia. Valiokunnan mielestä arkaluonteisia tietoja sisältäviin laajoihin tietokantoihin liittyy tietoturvaan ja tietojen väärinkäyttöön liittyviä vakavia riskejä, jotka voivat viime kädessä muodostaa uhan henkilön identiteetille (ks. PeVL 13/2016 vp, s. 4, PeVL 14/2009 vp, s. 3/I). Myös EU:n yleisen tietosuoja-asetuksen 51 johdantokappaleen mukaan asetuksen 9 artiklassa tarkoitettuja

erityisiä henkilötietoja, jotka ovat erityisen arkaluonteisia perusoikeuksien ja -vapauksien kannalta, on suojeltava erityisen tarkasti, koska niiden käsittelyn asiayhteys voisi aiheuttaa huomattavia riskejä perusoikeuksille ja -vapauksille. Valiokunta on tämän johdosta kiinnittänyt erityistä huomiota siihen, että arkaluonteisten tietojen käsittely on rajattava täsmällisillä ja tarkkarajaisilla säännöksillä vain välttämättömään ja sääntelyn on oltava tietosuojasetuksen mahdollistamissa puitteissa yksityiskohtaista ja kattavaa (PeVL 65/2018 vp, s. 45, PeVL 15/2018 vp, s. 40).

Perustuslakivaliokunta on painottanut, että väärinkäytön estävät tietoturvajärjestelyt ovat toimivia ja käytettävissä heti, kun järjestelmä otetaan käyttöön. Valiokunnan mielestä käsittelyn välttämättömyyden ja muun lainmukaisuuden jälkikäteinen ja tehokas valvonta esimerkiksi lokitietojen avulla on sinänsä välttämätöntä, mutta ei kuitenkaan riittävä tae. Valiokunta on korostanut, että tietojen suojaamista oikeudettomalta käytöltä ei voi perustaa vain rekisterinpitäjää tai tietojen käsitteijää koskevan virkavastuun tai muun seuraamusjärjestelmän varaan (PeVL 65/2018 vp, s. 47, PeVL 51/2018 vp, s. 5, PeVL 52/2018 vp, s. 4).

Tämän hallituksen esityksen tietosuojaja- ja tietoturva vaikutuksia koskevissa kohdissa on kuvattu tietosuojaa ja tietoturvaa koskevasta järjestelystä, jotka ovat jo nyt kattavasti voimassa.

Toisio-laissa on säännökset, jotka koskevat sosiaali-, terveys- ja hyvinvointitietojen hyödyntämistä muuhun kuin siihen tarkoitukseen jossa henkilötiedot on alun perin tallennettu. Laki sisältää mahdollisimman tarkkarajaisesti ne käyttötarkoitukset, joihin sanottuja tietoja voidaan luovuttaa, sekä perusteet joilla luovutus päätös tulee ratkaista. Käyttötarkoituksista on säädetty yksityiskohtaisesti. Henkilötietoja voitaisiin luovuttaa näihin käyttötarkoituksiin salassapitovelvollisuuden estämättä. Henkilötietojen käsittely on lisäksi useissa kohdin sidottu välttämättömyysvaatimukseen.

Toisio-lakiin sisältyy merkittäviä määrä teknisiä ja muita turvatoimia, joiden avulla voitaisiin varmistua siitä, että luovutuksensaaja käsittelee tietoja rekisteröidyn yksityiselämän suojaa turvaten silloin, kun pyydetty tiedot olisi käyttötarkoituksen vuoksi välttämätöntä luovuttaa poikkeuksellisesti henkilötunnuksin tai siten, että rekisteröity voitaisiin muutoin tunnistaa väkivalloisesti.

Rekisteröidyn oikeuksia ja vapauksia suojataan muun muassa siten, että henkilötietoja voisi pääsääntöisesti käsitellä vain viranomaisen myöntämän tietoluvan perusteella ja luvansaajaa koskisi salassapitovelvollisuus. Salassapitovelvollisuus on merkittävä myös perustuslain 12 §:n 2 momentissa säädetyn julkisuusperiaatteen näkökulmasta. Eduskunta on korostanut, että viranomaisten tietojen salassapitoa koskevia säännöksiä tulisi erityislainsäädännön sijaan sisällyttää keskitetysti julkisuuslakiin (PeVL 25/2010 vp, s. 3, PeVL 2/2008 vp, s. 2). Mainitussa toisio-lain salassapitopykälässä on kysymys salassapitosäännösten laajentamisesta koskemaan myös muuta kuin viranomaistoimintaa. Lisäksi pykälässä kielletään pääsääntöisesti tietojen käyttö yksittäistä henkilöä koskevassa päätöksenteossa. Salassapitovelvollisuuden tarkoituksena on samalla turvata yksilöiden henkilötietojen suojaa perusoikeutena.

Henkilötiedot tulee anonymisoida tai pseudonymisoida aina, kun se on käyttötarkoituksen kannalta mahdollista, ja niiden käsittelylle luotaisiin lain 3 luvun mukaiset palvelut viimeistään 1. toukokuuta 2022. Palveluihin sisältyy tietoturvallinen käyttöympäristö. Henkilötiedot voisi luovuttaa vain tällaiseen käyttöympäristöön 1.5.2022 alkaen.

Tietoluvan myöntäneen viranomaisen olisi valvottava luvan ehtojen noudattamista. Lisäksi sen olisi raportoitava 53 §:n mukaisesti tietosuojavaltuutetulle tietojen käsittelystä.

Rekisteröityjen yhdenvertaisen kohtelun kannalta toisiolaki turvaa sen, että sosiaali- ja terveystietojen sekä muiden yksityiselämän suojan piiriin kuuluvien hyvinvointitietojen hyödyntämistä koskevat tulkintalinjaukset ja päätökset muodostuisivat mahdollisimman yhteneviksi. Keskitetty lupamenettely turvaa yksityiselämän suojaa myös siten, että henkilötietojen käsittelyä voitaisiin minimoida silloinkin, kun saman tiedonhyödyntämissuunnitelman perusteella tarvitaan useiden eri rekisterinpitäjien terveyteen ja hyvinvointiin liittyviä tietoja.

Vaikka toisiolaissa säädetty tietoturvallinen käyttöympäristö on keskeinen toimi tietoturvaa ja tietosuojaa varmistamassa, ei se kuitenkaan ole ainoa keino varmistaa tietoturva- ja tietosuoja. Siirtymäajan siirrosta huolimatta toisiolaissa olisi edelleen voimassa se vahva ja selkeä periaate, että tieto luovutetaan ensisijaisesti aina Tietolupaviranomaisen omaan tietoturvalliseen käyttöympäristöön.

Siltä osin kuin Tietolupaviranomainen on tietoa luovuttanut muuhun kuin Tietolupaviranomaisen omaan käyttöympäristöön, on suurimmassa osassa tilanteista ollut kyse joko Terveystietojen ja hyvinvoinnin laitoksen omista tutkimushankkeista tai siitä, että tieto on luovutettu Tilastokeskuksen vastaavaan tietoturvalliseen ympäristöön ("Fiona"). Lisäksi tietoa on luovutettu yliopistosairaaloiden omiin tietoympäristöihin, tai yliopistojen hallinnoimiin sijainteihin. Vain muutamissa, yksittäisissä tilanteissa tieto on luovutettu joko yksityisen toimijan hallintaan tai ulkomaille. Siten valtaosa muualle luovutettujen tietojen hallinnoijista ovat joko kotimaisia viranomaisia tai kotimaisia erikoissairaanhoidon toimijoita, joiden hallussa on jo muutoinkin merkittävä määrä terveystietoja ja jotka kuuluvat asiakastietolain (159/2007) perusteella A-luokan järjestelmien piiriin.

Tietolupaviranomainen vaikuttaa jo nyt toiminnallaan tietoturva- ja suojaa parantavasti. Tietolupaviranomainen harkitsee lupaprosessissa varsin tarkasti useita erilaisia, tietoturvaan - ja suojaan liittyviä seikkoja. Tietolupaviranomainen käy ensinnäkin luvanhakijan kanssa hyvin tarkasti läpi, mitä tietoja ja kuinka paljon haettavaan käyttötarkoitukseen tarvitaan. On hyvin tavallista, että hakemusprosessin aikana tietoa tarkentuu merkittävästi siitä, mitä on alun perin haettu. Tietolupaviranomainen ei arvioi tutkimuksen tai muunkaan haettavan käyttötarkoituksen tarpeellisuutta tai tarkoituksenmukaisuutta. Se arvioi kuitenkin, tarvitaanko sanottuun käyttötarkoitukseen niin paljon tietoa kuin on haettu, ja onko haettava tieto tarkoituksensa sopiva.

Tietolupapäätöksessä Tietolupaviranomainen yksilöi muuttujakohtaisesti ne tiedot, joiden käyttöön se antaa luvan. Tämäkin parantaa tietosuojaa. Luvat myönnetään määräaikaisena, keskimäärin korkeintaan viiden vuoden määräajaksi. Lupaa ei siis saa toistaiseksi. Lupaan liitetään erilliset lupaehdot, jotka sisältävät määräyksiä tietosuojan ja turvan suojaamisen näkökulmasta. Jos ehtoja ei noudateta, on Tietolupaviranomaisella oikeus perua myöntämänsä lupa. Tällaisia peruuttamistilanteita ei ole syntynyt, mutta muutamissa tilanteissa Tietolupaviranomainen on huomauttanut hakijaa lupaehtojen noudattamisen tärkeydestä. Tietolupaviranomaisen näkemyksen mukaan sen laatimat lupapäätökset ja niihin liitettävät lupaehdot ovat tarkemmalla tasolla kuin mitä on ollut tilanne lupapäätösten suhteen ennen toisiolakia.

Tiedot kerätään ja luovutetaan luvanhakijalle ensisijaisesti niin, että aineisto tulee ensin Tietolupaviranomaiselle, joka yhdistää aineistot keskenään sekä pseudonymisoi sen. Aineiston lähettäminen tapahtuu toisiolaissa säädettyä sähköistä, tietoturvallista sähköistä kanavaa pitkin. (koska henkilötiedot ovat tutkimusryhmällä tai osalla siitä tiedossa).

Siirtymäajan aikana ala toimijat voivat auditoida ympäristönsä. Lisäksi rekisteröidyillä on käytettävissään myös siirtymäajan aikana kaikki yleisen tietosuoja-asetuksen mukaiset rekisteröidyn oikeudet.

Toisiolain 55 §:n 5 momentissa säädettäisiin potilaan mahdollisuudesta kieltää kliinisesti merkittävän löydöksen perusteella tehtävät yhteydenotot. Potilas voisi kieltää ne jo ennakolta sähköisesti asiakastietolaisissa (159/2007) tarkoitetun kansalaisen käyttöliittymän (Omakanta-palvelu) välityksellä taikka tekemällä kiellon kirjallisesti missä tahansa julkista terveydenhuoltoa tuottavassa toimintayksikössä, jolloin kiello kirjataan asiakastietolain 14 a §:ssä tarkoitettuun potilaan tiedonhallintapalveluun. Toisaalta potilas voisi kieltäytyä yksittäisen yhteydenoton perusteella ehdotetuista tiedoista, tutkimuksista ja hoidosta. Kielto-oikeudella ja toisiolain 55 §:n mukaisilla menettelyillä turvataan yksityisyyden suoja heti, kun 55 § astuisi voimaan, kuten myös merkittävistä kliinisistä löydöistä ilmoittaminen.

Julkisen vallan käyttö

Perustuslain 124 §:ssä säädetään hallintotehtävän antamisesta muulle kuin viranomaiselle. Sen mukaan julkinen hallintotehtävä voidaan antaa muulle kuin viranomaiselle vain lailla tai lain nojalla, jos se on tarpeen tehtävän tarkoituksenmukaiseksi hoitamiseksi eikä vaaranna perusoikeuksia, oikeusturvaa tai muita hyvän hallinnon vaatimuksia.

Perustuslain 124 §:n perustelujen sekä perustuslakivaliokunnan tulkintakäytännön mukaan ”julkisella hallintotehtävällä” viitataan ”julkisen vallan käyttöä” laajempaan kokonaisuuteen. Julkinen hallintotehtävä voi olla luonteeltaan myös palvelutehtävä, joka ei välttämättä sisällä julkisen vallan käyttöä tai julkisen vallan käytön osuus siinä voi olla vähäinen.

Lisäksi perustuslain 124 §:n mukaan merkittävää julkista valtaa sisältävää tehtävää voi hoitaa vain viranomainen. Tällaista merkittävää julkista valtaa saattaisi sisältyä muun muassa käyttö- lupaharkintaan ja tietojen luovuttamista tämän lain perusteella koskeviin muihin päätöksiin. Julkisen hallintotehtävän hoitaminen on pykälän perusteella pääsääntöisesti viranomaisen tehtävä ja se voidaan antaa muille kuin viranomaisille vain rajoitetusti.

Perustuslakivaliokunnan tulkintakäytännöstä ilmenee, että perustuslain 124 §:n mukaisella hallintotehtävän antamisella muulle kuin viranomaiselle voi etenkin yksityisen oikeusasemaan olennaisesti vaikuttavissa tilanteissa olla vain viranomaistoimintaa täydentävä ja avustava luonne. Perustuslakivaliokunnan käytännössä on arvioitu muun muassa lennonvarmistustehtävien jakamista (PeVL 47/2005 vp), passin antamista koskevan menettelyn ulkoistamista (PeVL 6/2013 vp), viranomaisten turvallisuusverkko toiminnan antamista valtionyhtiölle (PeVL 8/2014 vp), rautatieliikenteen vaatimuksenmukaisuuden teknisen arvioinnin ja tarkastustehtävien antamista yksityiselle oikeushenkilölle (PeVL 16/2002 vp). Kyse on ollut viranomaistoiminnalle edellytyksiä luovasta, teknisluontoisesta tai epäitsenäisestä toimintakokonaisuudesta.

Perustuslakivaliokunta on käytännössään jakanut 124 §:n mukaisen arvioinnin kolmeen osaan. Jako perustuu perustuslain esitöihin. Valiokunta on edellyttänyt, että:

Kyseessä ei ole merkittävän julkisen vallan siirto;

Tehtävän siirto on tarkoituksenmukainen mm. hallinnon tehokkuuden ja muiden hallinnon sisäisten tarpeiden sekä myös yksityisten henkilöiden ja yhteisöjen tarpeiden vuoksi; ja

Siirrettäessä huolehditaan perusoikeuksien, oikeusturvan ja muiden hyvän hallinnon vaatimusten turvaamisesta. Toisiolain 20 §:ssä tarkoitettua tietoturvallisen käyttöympäristön voisi pe-

rustaa muukin kuin viranomainen, myös yksityisoikeudellinen oikeushenkilö. Käyttöympäristössä käsiteltäisiin henkilötietoja. Säännös on arvioitava henkilötietojen suojaa koskevan perustuslain 10 §:n lisäksi myös perustuslain 124 §:n kannalta.

Siirtymäajan jälkeen Tietolupaviranomaisen tietoturvallinen käyttöympäristö olisi aina ensisijainen paikka, johon henkilötiedot luovutettaisiin. Tietolupaviranomaisen käyttöympäristö ei kuitenkaan välttämättä aina mahdollista tietojen käsittelyä luvansaajan tarpeisiin, koska tietoja voidaan käsitellä niin monella eri tavalla. Eri käyttötarkoituksissa saatetaan tarvita erilaisia työkaluja, joita Tietolupaviranomaisen ei ole aina mahdollista tarjota luvansaajalle. Esimerkiksi tieteellistä tutkimusta voidaan toteuttaa monin eri metodein ja niissä saatetaan tarvita erilaisia analyysityökaluja. Tietolupaviranomaisen käyttöympäristö ei tästä syystä aina käytännössä mahdollistaisi tietojen käsittelyä tietolupaahakemuksessa esitettyyn, sinänsä asialliseen henkilötietojen käyttötarkoitukseen.

Tietolupaviranomaisen käyttöympäristön ei pitäisi rajoittaa sinänsä perustuslainmukaisen käyttötarkoituksen toteutumista. Tämän vuoksi olisi tarkoituksenmukaista, että tietoja voisi käsitellä muussakin kuin Tietolupaviranomaisen käyttöympäristössä. Lisäksi nykysääntelyn valossa arkaluonteistenkin henkilötietojen käsittely on ollut mahdollista muussa kuin viranomaisen käyttöympäristössä. Käsittelijöiltä on luonnollisesti edellytetty salassapitovelvollisuutta.

Vaikka tietoja voitaisiin siirtää muuhun kuin Tietolupaviranomaisen käyttöympäristöön, rekisteröidyn perusoikeudet eivät saisi näissä tilanteissa vaarantua. Tietoturvallisen käyttöympäristön tietoturvallisuudelle asetettaisiin henkilötietojen suojaamiseksi lain 21—29 §:ssä vähimmäisvaatimukset, jotka sen olisi täytettävä. Tietoturvallisuuden arviointilaitos suorittaisi järjestelmille auditoinnin, millä varmistuttaisiin vähimmäisvaatimusten täyttymisestä. Sosiaali- ja terveysalan lupa- ja valvontaviranomaisen olisi valvottava järjestelmiä. Luvansaajaa sitoisi lisäksi salassapitovelvollisuus. Tietosuojavaltuutettu toimialallaan ja Sosiaali- ja terveysalan käyttöluovaviranomainen laissa säädetyn edellytyksin valvoisivat sitä, että henkilötietoja käsitellään lain ja lupaehtojen mukaisesti. Näin kyettäisiin nykytilannetta paremmin huolehtimaan siitä, että henkilötietoja käsitellään asianmukaisesti.

Perustuslain 10 §:ssä ei edellytetä, että henkilötietoja käsittelee viranomainen. Käytännössä yksityiset tahot käsittelevät henkilötietoja huomattavassa määrin ja myös arkaluonteisia henkilötietoja. Teknisiä viranomaisten henkilötietojen käsittelyyn liittyviä tehtäviä hoitavat yksityisoikeudellisetkin oikeushenkilöt esimerkiksi sopimuksen nojalla.

Toisiolain 55 §:ssä säädettäisiin oikeuksista ja velvollisuuksista, joita eri toimijoille syntyisi, jos terveydenhuollon asiakastietoja tai niitä sisältäviä rekisteritietoja toisiolain mukaisesti käsiteltäessä havaittaisiin kliinisesti merkittävä löydös. Pykälän 1 momentin mukaan tietoluvan saajalla, joka käsittelee terveydenhuollon asiakastietoja tai niitä sisältäviä rekisteritietoja ehdotetun lain perusteella, olisi oikeus ilmoittaa kliinisesti merkittävästä löydöksestä. Edellytyksenä olisi, että löydöksen perusteella olisi ilmoittajan ammatillisen käsityksen mukaan mahdollista ehkäistä tietyn potilaan terveyteen liittyvää riskiä tai parantaa merkittävästi hoidon laatua. Kuten edellä on todettu, perustuslain 10 §:ssä ei edellytetä, että henkilötietoja käsittelee viranomainen. Ilmoitus sen sijaan tehtäisiin asian merkittävyyden takia Tietolupaviranomaisen nimeämälle vastuuhenkilölle.

Tietolupaviranomaisen vastuuhenkilön olisi toisiolain 55 §:n 2 momentin mukaan ilmoituksen saatuaan koodattava mahdollisesti pseudonymisoidut tiedot auki ja selvitettävä, ketä tai keitä tieto koskee, sekä toimitettava tiedot ilman aiheutonta viivytystä Terveyden ja hyvinvoinnin

laitoksen nimeämälle asiantuntijalle. Tehtävä on esitetty säädettäväksi asian edellyttämän erityisasiantuntemuksen vuoksi, joka arvioidaan olevan toisiolain 55 §:n 3 momentin mukaan Terveyden ja hyvinvoinnin laitoksen asiantuntijalla, jonka olisi yhteistyössä laitoksen nimeämien muiden asiantuntijoiden kanssa arvioitava tiedon merkittävyys ja sen pohjalta toteutettavissa olevien toimenpiteiden odotettavissa oleva hyöty. Jos hyöty arvioidaan niin ilmeiseksi, että tutkittava olisi tärkeää saada hoidon piiriin, on edellä mainitun asiantuntijan ilmoitettava löydöksestä kunkin henkilön terveydenhuollosta alueellisesti terveydenhuoltolain nojalla vastuussa olevalle toimintayksikölle.

Terveydenhuollon toimintayksikön olisi 55 §:n 4 momentin mukaan tiedon saatuaan otettava yhteys potilaaseen ja selvitettävä, haluaako tämä tiedon kliinisesti merkittävästä löydöksestä ja sen mahdollisesti edellyttämistä tutkimus- ja hoitotoimenpiteistä sekä niistä odotettavissa olevasta hyödystä.

Edellä mainituilla perusteilla lakiehdotukset voidaan käsitellä tavallisessa lainsäätämisyksessä.

Ponsi

Edellä esitetyn perusteella annetaan eduskunnan hyväksyttäväksi seuraava lakiehdotus:

Laki

sosiaali- ja terveystietojen toissijaisesta käytöstä annetun lain 60 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti
muutetaan sosiaali- ja terveystietojen toissijaisesta käytöstä annetun lain (552/2019) 60 §:n
1 momentti seuraavasti:

60 §

Siirtymäsäännökset

Tämän lain 19 §:ää lokitiedoista sovelletaan 1 päivästä toukokuuta 2021. Tämän lain 20 §:n 3 momenttia ja 21–34 §:ää tietoturvaliselta käyttöympäristöltä edellytettävistä vaatimuksista sovelletaan 1 päivästä toukokuuta 2022. Ennen mainittua ajankohtaa tietoja voidaan luovuttaa luvansaajan käsiteltäväksi 51 §:n 1 ja 2 momentin nojalla, vaikka tietolupahakemuksessa ei osoitettaisi 51 §:n 3 momentissa tarkoitettua tietoturvaliselta käyttöympäristöä tietojen käsitte-lylle. Tämän lain 55 §:ää kliinisistä löydöksistä sovelletaan 1 päivästä tammikuuta 2024.

Tämä laki tulee voimaan päivänä kuuta 20 .

Helsingissä x.x.20xx

Pääministeri

Sanna Marin

Perhe- ja peruspalveluministeri Krista Kiuru

Laki

sosiaali- ja terveystietojen toissijaisesta käytöstä annetun lain 60 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti
muutetaan sosiaali- ja terveystietojen toissijaisesta käytöstä annetun lain (552/2019) 60 §:n
1 momentti seuraavasti:

Voimassa oleva laki

Ehdotus

60 §

60 §

Siirtymäsäännökset

Siirtymäsäännökset

Tämän lain 19 §:ää lokitiedoista, 20 §:n 3 momenttia ja 21–34 §:ää tietoturvaliselta käyttöympäristöltä edellytettävistä vaatimuksista sekä 55 §:ää kliinisistä löydöksistä sovelletaan 1 päivästä toukokuuta 2021. Ennen mainittua ajankohtaa tietoja voidaan luovuttaa luvansaajan käsiteltäväksi 51 §:n 1 ja 2 momentin nojalla, vaikka tietolupahakemuksessa ei osoitettaisi 51 §:n 3 momentissa tarkoitettua tietoturvaliselta käyttöympäristöä tietojen käsittelylle.

Tämän lain 19 §:ää lokitiedoista sovelletaan 1 päivästä toukokuuta 2021. *Tämän lain 20 §:n 3 momenttia ja 21–34 §:ää tietoturvaliselta käyttöympäristöltä edellytettävistä vaatimuksista sovelletaan 1 päivästä toukokuuta 2022.* Ennen mainittua ajankohtaa tietoja voidaan luovuttaa luvansaajan käsiteltäväksi 51 §:n 1 ja 2 momentin nojalla, vaikka tietolupahakemuksessa ei osoitettaisi 51 §:n 3 momentissa tarkoitettua tietoturvaliselta käyttöympäristöä tietojen käsittelylle. *Tämän lain 55 §:ää kliinisistä löydöksistä sovelletaan 1 päivästä tammikuuta 2024.*

Tämä laki tulee voimaan päivänä kuuta 20

..