HUS/1158/2021-1 **9.4.2021**
VN/8786/2021

Sosiaali- ja terveysministeriön kutsu 31.3.2021 kuulemistilaisuuteen 12.4.2021 koskien sosiaali- ja terveystietojen toissijaisesta käytöstä annetun lain 60 §:n muuttamista

Helsingin ja Uudenmaan sairaanhoitopiiri (HUS) kiittää mahdollisuudesta antaa asiantuntijalausuntonsa Sosiaali- ja terveysministeriölle toisiolain 60 §:n 1 momentin siirtymäsäännökseen esitettävistä muutoksista.

”Sosiaali- ja terveysministeriössä on valmisteltu hallituksen esitysluonnos sosiaali- ja terveystietojen toissijaisesta käytöstä annetun lain 60 §:n muuttamisesta. Esityksessä ehdotetaan muutettavaksi sosiaali- ja terveystietojen toissijaisesta käytöstä annetun lain (toisiolaki) 60 §:n 1 momentin siirtymäsäännöstä siten, että toisiolain tietoturvalliselta käyttöympäristöltä edellytettävistä vaatimuksista 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.”

Toisiolain tietoturvalliselta käyttöympäristöltä edellytettävistä vaatimuksista on annettu Findatan määräys 5.10.2020. Määräyksen voimaantulopäiväksi on asetettu 1.5.2021. Määräyksessä esitetään yksityiskohtaisia vaatimuksia tietoturvalliselle käyttöympäristölle ja osa vaatimuksista on jopa tiukempia kuin ensisijaiseen käyttöön tarkoitetuille käyttöympäristöille annetut vaatimukset. Yliopistosairaalan ja terveydenhuollon viranomaisrekisterinpitäjän näkökulmasta onkin epäjohdonmukaista, että tietoturvavaatimukset toisiokäytölle ovat vaativammat kuin potilastietojen ensisijaiselle käyttötarkoitukselle. Jo määräystä annettaessa 10/2020 on ollut ilmeistä, että toimijoille ei ole annettu riittävästi aikaa muokata käytössä olevia ratkaisuja sekä saada vaadittua sertifiointia tietoturvalliselle käyttöympäristölle.

Findatan määräyksen mukaisesti kohdassa 3.1.2 *Tietolupaviranomaisen asettamat vaatimukset* mainitaan, että ”Palveluntarjoajan on osoitettava luotettavuus turvallisuuden hallintajärjestelmällä, esimerkiksi ISO/IEC 27001 -standardin mukaisesti.".

HUS on työstänyt toisiolain vaatimukset täyttävää ISO 27001-standardin mukaista tietoturvallista analytiikkaympäristöä noin kahden vuoden ajan. HUS on jo toteuttanut ISO 27001-standardin mukaisen ulkoisen auditoinnin 5.2.2021 palveluntuottajan turvallisuuden hallintajärjestelmästä. Auditoinnissa ilmeni 4 lievää poikkeamaa, jotka korjataan huhtikuun 2021 kuluessa. Lopulliseen arviointiin varautuminen on kuitenkin hyvin haasteellista, koska sertifioinnin tarkat kriteerit ja tulkintaohjeet puuttuvat. Lisäksi Findatan määräyksessä jää epäselväksi, mitä ISO 27001 sertifioinnin tulee kattaa; koskeeko sertifiointi koko organisaation toimintaa vai vain palvelua (tietoturvallinen käyttäjäympäristö) tuottavaa osaa organisaatiossa.

Findatan määräyksen mukaisesti "Arvioinnin toteuttava ja todistuksen myöntävä tietoturvallisuuden arviointilaitos arvioi omalla ammattitaidollaan, soveltuvatko tietoturvallista käyttöympäristöä koskevat, voimassa olevat tietoturvallisuuteen liittyvät sertifikaatit määräyksessä esitettyjen vaatimusten täyttämisessä." Teknisen ympäristön osalta keskusteluissa HUSin Tietohallinnon ja Traficomin hyväksymien auditoijien (KPMG ja NIXU) kesken on tullut esiin, että auditointi kestää 6–8 viikkoa. Vaatimukset on asetettu siten, että mahdollisten auditoinnissa ilmenevien korjaustoimenpiteiden tulee olla tehtyjä toimintaluvan myöntämiseksi. Auditoinnin pitkän keston lisäksi Findatan määräyksessä asetettu aikatauluvaade muodostuu hyvin haastavaksi myös siksi, etteivät tekniset ja toiminnalliset arviointikriteerit ole yksiselitteisesti määritettyinä palveluntuottajille eikä arvioijille, joten toiminnallisuuksien viimeistely ei voi jatkua eikä arviointi käynnistyä ennen lopullisia määrityksiä. HUS näkee ongelmana myös sen, ettei Traficomin hyväksymillä arviointilaitoksilla ole yhdenmukaisia kriteerejä, joten tietoturvallisen käyttöympäristön tulkinnat ja sertifioinnin sisältö saattavat erota eri puolilla Suomea.

Nyt käsiteltävässä esityksessä ehdotetaan muutettavaksi sosiaali- ja terveystietojen toissijaisesta käytöstä annetun lain (toisiolaki) 60 §:n 1 momentin siirtymäsäännöstä siten, että toisiolain tietoturvalliselta käyttöympäristöltä edellytettävistä vaatimuksista sovellettaisiin vasta 1 päivästä toukokuuta 2022. Tällä pyritään varmistamaan se, että merkittävimmät terveydenhuollon toimijat ehtivät auditoida omat käyttöympäristönsä vaatimuksia vastaaviksi ja siten pystyvät käsittelemään tietoaineistoja myös omissa ympäristöissään. HUS esittää kantanaan, että tietoturvallisen käyttöympäristön käyttöönottoajankohtaa on perusteltua siirtää esityksen mukaisesti.

HUS toteaa myös, että Suomessa tehdyt kansalliset erityisratkaisut tietoturvallisista käyttöympäristöistä ja tulkinnat henkilötiedon ja sen anonymisoinnin osalta vaikeuttavat vakavasti kansainvälistä yhteistyötä. Suomalaisten tutkijoiden asema TKI-sektorilla suhteessa verrokkimaihin (mm. muut Pohjoismaat ja EU jäsenvaltiot) heikkenee ja kehitys on EU tavoitteiden vastainen ja Suomen pitäisikin ennemmin tukeutua eurooppalaisiin tai muihin kansainvälisiin standardeihin.

Lisäksi siirtymäsäännöstä esitetään muutettavaksi siten, että toisiolain 55 §:n merkittäviin kliinisiin löydöksiin perustuvia oikeuksia, velvoitteita ja toimenpiteitä sovellettaisiin vasta 1 päivästä tammikuuta 2024. Koska syytä tähän lykkäykseen ei ole kerrottu, on kannanottomme vajavainen. Findatalla on väestötasolla vaikeuksia mm. tietopyyntöjen hallinnassa. Lykkäys liittynee yleisen tietosuoja-asetuksen noudattamisen vaikeuteen väestötasolla, kuten tietojen toisiokäytön etukäteiskieltojen ja oikeuden tulla unohdetuksi pyyntöjen hallinnan osalta keskitetysti esimerkiksi Kanta-palvelussa.

Toisiolain 55 § on ongelmallinen työläytensä, mahdollisen hitautensa sekä Findatan asiantuntijan ja THL:n nimeämien asiantuntijoiden vastuukysymysten ja oikeusturvan osalta. Niinpä 55 §:ä pitäisikin päästä harjoittelemaan, jolloin 1. päivään tammikuuta 2024 mennessä 55 §:ä voitaisiin saatujen käyttökokemusten myötä myös tarvittaessa ennakoivasti muokata. Tämä voisi tulla kyseeseen käyttöympäristöissä, joissa valmiudet tietosuoja-asetuksen noudattamiselle tai vastaavalle ongelmalle ovat hallinnassa. HUS toteaa, että ainakin valikoiduissa, kansallisen tietolupaviranomaisen ongelmattomiksi arvioimissa tapauksissa toisiolain 55 § soveltaminen tulisi sallia jo aiemmin. Näin saataisiin aikaan kehitystyö toisiolain erään edistyksellisimmistä pykälistä muokkaamiseksi täysimääräisesti potilaan oikeudet ja potilasturvallisuus huomioivaksi. Äkillinen viivästäminen voi myös kohtuuttomasti hai-

tata jo käynnistettyjä, Findatan tietolupa-arvioinneissa olevia ja 55 §:ä käyttämään suunniteltuja projekteja. Tämä olisi myös tutkijoiden ja tutkittavien oikeusturvan kannalta ongelmallista, mikäli jo ilmaantuneet 55§:n ongelmat olisivat muuten ratkaistavissa kansallisen tietolupaviranomaisen selvityksen perusteella.

Kunnioittavasti,

Mikko Seppänen
Osastonylilääkäri
Toisiolakitoimikunnan varapuheenjohtaja

Anu Maksimow
vs. hallintoylilääkäri
Toisiolakitoimikunnan puheenjohtaja

Helsingin ja Uudenmaan sairaanhoitopiiri