Valvira
Sosiaali- ja terveysalan lupa- ja valvontavirasto

Dnro V/30653/2022

26.9.2022

Eduskunnan sosiaali- ja terveysvaliokunta

Asiantuntijalausuntopyyntönne valtioneuvoston kirjelmästä U 61/2022 vp, 21.9.2022

Asia

Eduskunnan sosiaali- ja terveysvaliokunta on pyytänyt Sosiaali- ja terveysalan lupa- ja valvontavirastolta (Valvira) asiantuntijalausuntoa valtioneuvoston kirjelmästä eduskunnalle komission ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi eurooppalaisesta terveysdata-avaruudesta (COM (2022) 197 final, jäljempänä EHDS-asetusehdotus, annettu 5.3.2022)

Lausunto

EDHS-asetusehdotuksen tarkoituksena on luoda eurooppalainen terveysdata-avaruus (EHDS) asettamalla sääntöjä, yhteisiä standardeja ja käytänteitä, rakenteita ja hallintamallin sähköisten terveystietojen ensiö- ja toisiokäytölle.

Valviran näkemyksen mukaan 5.3.2022 annettu EHDS-asetusehdotus sisältää merkittäviä riskejä muun muassa kansallisen tietoturvan, potilasturvallisuuden ja markkinoille tulevien tietojärjestelmien valvonnan näkökulmasta. Lisäksi asetusehdotus loisi epätasapainoa sosiaalihuollon asiakastietojen ja terveydenhuollon potilastietojen sähköistä käyttöä koskevan kansallisen sääntelyn välille.

Asetuksen soveltamisalasta

Suomessa asiakas- ja potilastietojen käsittelystä on säädetty kansallisesti uudistetulla sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetulla lailla (784/2021, jäljempänä asiakastietolaki). Asiakastietolain keskeisimpänä tarkoituksena on edistää ja mahdollistaa sosiaali- ja terveydenhuollon tuottamien asiakastietojen ja asiakkaan itsensä tuottamien hyvinvointitietojen tietoturvallista käsittelyä kansallisesti terveydenhuollon ja sosiaalipalveluiden järjestämisen ja tuottamisen käyttötarkoituksissa.

Asetusehdotus koskisi potilastietojärjestelmiä ja hyvinvointisovelluksia (1 artikla). Asetus ei koskisi sosiaalihuollossa käytettäviä asiakastietojärjestelmiä. Asetuksessa ehdotetun soveltamisalan rajoituksen seurauksena voi Valviran näkemyksen mukaan syntyä tilanne, jossa potilastietojärjestelmien ja hyvinvointisovellusten sääntely tehdään EHDS:n säännösten perusteella, mutta sosiaalihuollon asiakastietojärjestelmien sääntely tehtäisiin edelleen sellaisten

kirjaamo@valvira.fi Puhelin 0295 209 111 www.valvira.fi

PL 43, 00521 Helsinki
Ratapihantie 9, 00520 Helsinki
Faksi 0295 209 700

Koskenranta 3, 96100 Rovaniemi
Faksi 0295 209 704

asiakastietolain säännösten perusteella, joita ei enää sovellettaisi terveydenhuollon potilastietojärjestelmiin.

Koska Suomessa sosiaali- ja terveydenhuollon integraation myötä niiden välistä raja-aitaa on madallettu ja tietojen välitystä haluttu mahdollistaa (asiakastietolain 20 § ja 21 §), on tietojärjestelmien valmistajat alkaneet kehittää järjestelmiä, joissa on sekä sosiaalihuollon asiakastietojärjestelmän että terveydenhuollon potilastietojärjestelmän käyttötarkoitus. Lisäksi tyypillistä on, että Suomessa tietojärjestelmän valmistajalla on kummankin käyttötarkoituksen tietojärjestelmät markkinoilla. EHDS astuessaan voimaan voisi tarkoittaa sitä, että samaa tietojärjestelmän valmistajaa ja mahdollisesti myös saman järjestelmän eri käyttötarkoituksia koskisivat eri säännökset siitä, miten järjestelmän saisi ottaa tuotantokäyttöön.

Potilastietojärjestelmien markkinoille tulosta

Asetusehdotuksen yhtenä tavoitteena on vapauttaa unionin sisäistä datataloutta mahdollistamalla aidot sisämarkkinat digitaalisille terveyspalveluille ja tuotteille. Asetusehdotuksen jaksossa 3 säädettäisiin, miten potilastietojärjestelmän voisi tuoda markkinoille. Asetuksen näkökulma eroaa asiakastietolain näkökulmasta, jossa korostetaan sitä, millaiset vaatimukset järjestelmän tulee täyttää, jotta sosiaali- tai terveydenhuollon palvelunantaja voi ottaa järjestelmän käyttöönsä.

Suomessa markkinoilla ja terveydenhuollon palveluntuottajien käytössä olevat potilastietojärjestelmät, jotka ovat tarkoitettu käytettäväksi terveydenhuollossa kirjattavien potilastietojen käsittelyyn, tallentamiseen ja ylläpitoon, tulee rekisteröidä asiakastietolain perusteella Valviran ylläpitämään julkiseen tietojärjestelmärekisteriin. Terveydenhuollossa käytettäväksi tarkoitetut potilastietoa käsittelevät tietojärjestelmät jaetaan kansallisesti luokkiin A ja B. Kansallisessa lainsäädännössä painotetaan sosiaali- ja terveydenhuollon palvelunantajan oikeutta saada käyttöönsä todennetusti vaatimuksenmukainen asiakas- tai potilastietojärjestelmä. Tietojärjestelmien sertifioinnissa on käytännössä kaksi ulkopuolista tarkastusta (yhteentoimivuuden testaus ja tietoturvallisuuden arviointi), joiden yhteydessä myös järjestelmän toiminnallisuudet tulevat tarkastetuksi. Luokitellessaan tietojärjestelmäänsä tietojärjestelmäpalvelun tuottajan on tehtävä järjestelmästään riskiarvio. Riskiarviossa on huomioitava muun muassa tietojärjestelmän käytön laajuus ja tietojärjestelmässä käsiteltävien tietojen sensitiivisyys.

A-luokan järjestelmältä edellytetään hyväksyttyä yhteentoimivuuden testausta, jonka jälkeen järjestelmä voi siirtyä tietoturvallisuuden arvioitiin. Tietoturvallisuuden arvioinnin suorittaa tietojärjestelmän tuottajasta erillinen toimija. Luokkaan B kuuluu sosiaali- ja terveydenhuollon asiakas- ja potilastietoja käsittelevät tietojärjestelmät, jotka eivät liity suoraan Kanta-palveluihin, jotka eivät tuota Kanta-palveluihin tallennettavia asiakirjoja ja joihin ei kohdistu esimerkiksi tehdyn riskiarvion perusteella luokan A1 mukaista vaatimusta tietoturvallisuuden arvioinnista.

Valvira
Sosiaali- ja terveysalan lupa- ja valvontavirasto

EHDS-asetusehdotuksessa potilastietojärjestelmän vaatimustenmukaisuuden todentaminen tapahtuisi tietojärjestelmän valmistajan itse tuottaman dokumentaation ja vakuutuksen kautta, eikä esimerkiksi tietoturvallisuuden arviointilaitos tarkastaisi tietojärjestelmän tietoturvallisuutta. Asetus mahdollistaisi Valviran näkemyksen mukaan toisessa jäsenvaltiossa rekisteröidyn potilastietojärjestelmän automaattisen ”hyväksymisen” muissa jäsenvaltiossa. Tämä synnyttäisi tilanteen, jossa Suomen markkinoille voisi tulla vapaammin tietojärjestelmiä, joille ei ole tehty nykyisin edellytettyä tietoturvan riskikartoitusta eikä tietoturvallisuuden arviointia. Tällaisten tietojärjestelmän tietoturva sekä tietoturvariskeihin ennalta varautuminen jäisi käytännössä tietojärjestelmän toimittajan oman ilmoituksen varaan.

Valvira suhtautuu varauksella siihen, että asetusehdotuksessa kuvattu menettelytapa turvaisi tarkoituksenmukaisella tavalla esimerkiksi kansalaisten potilastietojen tietoturvan ja tietosuojan. EU:n tietosuoja-asetuksen mukaan muun muassa potilastiedot ovat erityissuojattavia tietoja, ja on perusteltua edellyttää, että arkaluonteisia potilastietoja käsitteleviin ja tallentaviin tietojärjestelmiin ulotetaan vähintäänkin vaatimus ulkopuolisen toimijan tekemästä tietoturvallisuuden arvioinnista. Valvira katsoo lisäksi, että asetusehdotuksessa tulisi ottaa paremmin huomioon myös kyberturvallisuusuhat, jotka voivat kohdistua muun ohella kriittisiin potilastietojärjestelmiin. Tämä seikka on omiaan lisäämään vaatimusta siitä, että Suomessa käyttöön otettaviin ja käytössä oleviin kriittisiin ja laajoihin potilastietojärjestelmiin ulotettaisiin jatkossakin vaatimus ulkopuolisesta tietoturvallisuuden arvioinnista, joka suoritettaisiin kolmen vuoden välein, kuten voimassa olevassa asiakastietolaissa edellytetään.

Komission EHDS-asetusehdotukseen tekemän vaikutuksenarvioinnin perusteella on pidetty parhaimpana keskitasoisen intensiteetin puuttumista EU-sääntelyllä. Se tarkoittaisi ehdotuksen mukaan muun muassa pakollisia vaatimuksia ja sertifiointia, jotka varmistaisivat läpinäkyvyyden käyttäjille ja hankkijoille sekä vähentäisivät valmistajien rajat ylittäviä markkinaesteitä. Asetusehdotusta koskevan valtioneuvoston kirjelmän mukaan komissio tulee tekemään kohdistetun arvioinnin viiden vuoden kuluttua sääntelyn voimaantulosta keskittyen erityisesti asetusehdotuksen III lukuun ja mahdollisin muutosehdotuksin. Arviointiin kuuluu potilastietojärjestelmien itsearviointimenettelyn arviointi ja tarve asettaa vaatimuksenmukaisuuden arviointimenettely notifioiduille tahoille.

Valviran näkemyksen mukaan tämä käytännössä tarkoittaisi, että Suomessa nykyisin tietoturvallisuuden arviointilaitoksen tekemää työtä ja antamaa todistusta ei käytännössä enää olisi. Valviralla tai käytännössä muillakaan viranomaisilla ei ole sellaista tietoteknistä osaamista, joka voisi korvata tietoturvallisuuden arviointilaitosten tekemää käytännön työn ja tarkastuksen (muun muassa nykyisin kriittisiin potilastietojärjestelmiin tehdään tietoturvatestausta). Tietoturvallisuuden arviointilaitoksen antamalla todistuksella on keskeinen rooli asiakastietolain ja toisiolain mukaisessa tietojärjestelmän ja sen käyttöympäristön hyväksymisessä. Nykyinen Suomen lainsäädännössä kyseinen

kirjaamo@valvira.fi Puhelin 0295 209 111 www.valvira.fi

PL 43, 00521 Helsinki
Ratapihantie 9, 00520 Helsinki
Faksi 0295 209 700

Koskenranta 3, 96100 Rovaniemi
Faksi 0295 209 704

todistus on katsottu olevan välttämätön, koska lainsäädäntö kieltää A-luokan tietojärjestelmän käyttöönoton ilman hyväksyttyä ko. todistusta.

Uusien eurooppalaisten potilastietojärjestelmien markkinoille tulossa on tärkeää huomioida lisäksi potilastietojärjestelmien rakenteiden kansalliset erityispiirteet. Potilastietojärjestelmät, erityisesti potilaskertomusjärjestelmät, on kehitetty vastaamaan kunkin maan lainsäädäntöä, terveydenhuollon rakenteita ja työprosesseja. Esimerkiksi Suomessa julkisessa terveydenhuollossa käytössä oleva potilastietojärjestelmä ja potilasasiakirjojen tekninen rakenne kuvastavat julkisen terveydenhuollon rakennetta, ja järjestelmien kehittämisessä on huomioitu kansallinen substanssilainsäädäntö (muun muassa laki potilaan asemasta ja oikeuksista).

EHDS-asetusehdotuksessa jää epäselväksi, miten varmistettaisiin jatkossa, että kansallisesta lainsäädännöstä nousevat, potilastietojärjestelmään toteutettavat toiminnallisuudet on toteutettu toisessa jäsenvaltiossa käyttöön otettuun potilaistietojärjestelmään, kun se otetaan tuotantokäyttöön suomalaisessa terveydenhuollossa. Tällä hetkellä terveydenhuollon palveluntuottaja voi luottaa siihen, että ottaessaan käyttöön asiakastietolain perusteella sertifioidun potilastietojärjestelmän, se toimii kansallisten, lakiin perustuvien minimivaatimusten mukaisesti. Jos tämä menettely poistuu ja potilastietojärjestelmä voidaan tuoda markkinoille ilman, että siihen kohdistetaan mitään ulkopuolisen tahon tekemää ennakkotestausta tai -tarkastusta, vastuu tietojärjestelmän vaatimustenmukaisuudesta jäisi yhä enemmän järjestelmää hankkivan terveydenhuollon yksikön vastuulle.

Yhteentoimivuudesta

EHDS-asetusehdotuksen liitteen II kohdassa 2 säädettäisiin potilastietojärjestelmien yhteentoimivuudesta. Valvira toteaa, että tietojärjestelmien yhteentoimivuus vaatii tyypillisesti (yleiseurooppalaista) standardia tarkempaa vaatimusten määrittelyä. Tulee myös huomioida, että yhteentoimivuuteen johtavat toimenpiteet yhdenmukaistavat väistämättä terveydenhuollon työprosesseja ja käytäntöjä.

Tietojärjestelmien yhteentoimivuus tarkoittaa standardien ja teknisten yksityiskohtien lisäksi ennen kaikkea sitä, että eri Euroopan maiden välillä välitettävät potilastiedot kirjataan ja ne ymmärretään samalla tavalla. Valviran näkemyksen mukaan jatkossa potilastietojen virheettömään ja potilasturvalliseen välittämiseen eri Euroopan maiden välillä ei riitä, että Euroopassa käytetään yhteisiä koodistoja esimerkiksi diagnoosien kirjaukseen. On arvioitava tarkkaan, mitkä potilastiedoista ovat sellaisia, että niiden kirjaamisessa ja niiden tulkitsemisessa käytännöt ovat niin yhdenmukaiset, että virhetulkinnan vaaraa ei synny eikä potilasturvallisuus vaarannu.

Suomessa asiakastietolain mukaiseen sertifiointiprosessiin kuuluu Kansaneläkelaitoksen suorittama yhteistestaus, jolla tarkistetaan, että tietojärjestelmä ovat yhteentoimiva Kanta-palvelujen ja muihin niihin liitettävien

tietojärjestelmien kanssa. Jotta terveydenhuollon ammattihenkilö voi toimia työssään lain edellyttämällä tavalla ja potilaan laissa säädetyt oikeudet toteutuvat, tietojärjestelmän toiminnallisuudet tulee olla toteutettu asianmukaisesti potilastietojärjestelmään. Valvira katsoo, että tietojärjestelmien yhteentoimivuuden testaus on edellytys sille, että tietojärjestelmät ovat keskenään yhteentoimivia. Tämä turvaa myös potilasturvallisuuden tietoja välitettäessä palvelunantajalta toiselle. Se takaa myös datan laadun ja siten tietojen toisiokäytön.

Potilastietojen yksilöinnistä

Asetusehdotuksesta ei käy ilmi, mikä olisi se potilaan yksilöivä tunniste, jota käytettäisiin Euroopan laajuisessa tietojenvälityksessä. Suomessa potilaan yksilöivä tunniste on tällä hetkellä henkilötunnus, joka toimii avaimena potilastietoihin Suomessa käytettävissä tietojärjestelmissä. Toisissa EU-maissa potilaan yksilölliset tunnisteet eroavat Suomessa käytetystä. Myös esimerkiksi potilaan terveystietojen luovuttamista koskevien kieltojen ja suostumisten antaminen perustuu henkilötunnuksen käyttämiseen.

Valviran näkemyksen mukaan yhdessä jäsenvaltiossa käytössä olevaa potilastietojärjestelmää ei voi siirtää toiseen jäsenvaltioon ilman, että järjestelmään tehdään kansallisen lainsäädännön ja muiden kansallisten toimintatapojen edellyttämät muutokset. Unionintasoinen laaja potilastietojen vaihto edellyttänee minimissään yksilöidyn potilaskohtaisen tunnistetiedon käyttöön ottamista, joka tulisi toteuttaa myös jo käytössä oleviin potilastietojärjestelmiin.

Asetusehdotuksen vaikutukset terveydenhuollon etäpalveluihin

.

Asetusehdotuksella toteutuessaan on vaikutusta terveydenhuollon etäpalveluihin. Rajat ylittävistä terveydenhuollon palveluista ei ole tällä hetkellä niin sanotun EU-potilasdirektiivin lisäksi muuta EU-sääntelyä, mikä on aiheuttanut tulkintatilanteita ja vaikeuttanut osaltaan unionin sisäistä potilaiden ja palveluntuottajien vapaata liikkuvuutta. Jäsenvaltioilla on kansalliseen sääntelyynsä perustuvia erilaisia terveydenhuollon palveluiden tuottamista koskevia lupa- ja ilmoitusvaatimuksia, joita ei ole yhtenäistetty. EHDS-asetusehdotuksen toimeenpano edellyttää näiden käytänteiden yhtenäistämistä kansallisella ja unionin tasolla. Lisäksi rajat ylittävän terveydenhuollon palveluiden osalta on tärkeä huolehtia tulevassa sääntelyssä täsmällisistä vastuu-, korvaus- ja valvontasäännöksistä (esimerkiksi potilasvakuutuksen voimassaolo, terveydenhuollon valvontaviranomaisen toimivaltakysymykset ym.). Edellä todettujen ongelmakohtien lisäksi tulee pohtia, kuinka kehitetään tietoturvallista tekniikkaa, joka mahdollistaa ja helpottaa rajat ylittävän terveydenhuollon palveluiden antamista lääketieteellisesti asianmukaisella tavalla.

Valvira
Sosiaali- ja terveysalan lupa- ja valvontavirasto

Terveystietojen toisiokäytöstä

EHDS-asetusehdotuksessa säädettäisiin myös terveystietojen toisiokäytöstä. Sääntely muistuttaisi olennaisilta osiltaan kansallista sosiaali- ja terveystietojen toissijaisesta käytöstä annettua lakia (552/2019, toisiolaki).

Valviran näkemyksen mukaan asetusehdotuksen mukaisten tietoluokkien, jotka määrittävät terveystietojen toissijaisia käyttökohteita, tarkkuustaso kuitenkin muuttunee/laajenee toisiolakiin nähden (44 artikla). Asetus sallisi muun muassa ihmisen geneettisten, genomisten ja proteomisten tietojen käytön. Valviran näkemyksen esimerkiksi genomitietojen käsittely on erityisen haastavaa sen vaatiman suuren laskentaresurssin ja säilytystilan vuoksi. Näiden tietojen käsittely vaatisi hyvin erikoistuneen käsittely-ympäristön. Genomitietojen osalta myös tietosuojan ja -turvan toteutumisen varmistaminen on käytännössä erityisen haastavaa. Lähtökohtaisesti ihmisen perimää koskevien tietojen käsittely ”anonyymiksi” voi olla itsestään ristiriitainen prosessi.

Asetusehdotuksen mukaan toisiokäyttöä varten luovutettavat terveystiedot tulee ensisijaisesti anonymisoida (tietojen minimointi, 44 artikla). Asetusehdotuksen mukaan käyttäjän hakemuksesta kyseiset tiedot on myös mahdollista luovuttaa pseudonymisoituna, jos tietyt ehdot täyttyvät. Valviran näkemyksen mukaan tällaisen tietojen käsittely tapahtuisi turvatussa käsittely-ympäristössä tiedon luonteesta riippumatta (anonymisoitu/pseudonymisoitu), mikä merkitsee isoa kontrastia toisiolaissa omaksuttuun sääntelyyn. Koska anonyymit tiedot eivät ole enää henkilötietoja eivätkä ne siten ole turvatoimenpiteiden kohteena, niiden käsittely ei toisiolain mukaan rajoitu vain tietoturvalliseen käyttöympäristöön (turvattu käsittely-ympäristö).

Toisiolain mukainen tietoturvallinen käyttöympäristön hyväksyminen perustuu keskeisesti tietoturvallisuuden arviointilaitoksen tekemään arviointiin ja sen perusteella annettuun todistukseen. Nykyiseen Tietoturvallinen käyttöympäristö -rekisteriin on rekisteröity kahdeksan ympäristöä ja näille 50 %:lle käyttöympäristöjä on arviointilaitos antanut huomion sellaisesta tietotuvallisuuden poikkeamista, joka tulee korjata 6kk aikana ja korjauksen tulee osoittaa tehdyksi. Tämä puoltaa myös ennakollisen tietoturvallisuuden arvioinnin vaatimusta terveystietojen toissijaisessa käytössä.

Muita huomioita

EHDS:ä koskevassa komission vaikutustenarvioinnissa on käyty läpi asetusehdotuksen vaikutuksia erityisesti potilastietojärjestelmien valmistajiin nähden. Asetuksella olisi kuitenkin erittäin merkittäviä vaikutuksia Valviran tehtäviin, mutta valtioneuvoston U-kirjelmässä eikä asetusehdotuksessa ole mainintoja asetuksen vaikutuksesta terveydenhuollon valvontaan, ohjaukseen eikä terveydenhuollon viranomaislupiin ja hyväksyntöihin. Lisäksi asetusehdotuksesta koskevassa kirjelmässä mainitaan muun muassa, että potilaiden oikeuksien toteutumista valvoisi EU tietosuoja-asetuksen mukaiset valvontaviranomaiset ja jäsenmaiden terveysviranomaiset. Kirjelmässä ei ole avattu

tarkemmin ketkä ovat jäsenmaiden terveysviranomaiset (sisältyvätkö esimerkiksi Valvira ja aluehallintovirastot valvontaviranomaisina näihin). Tietosuoja-asetuksen mukainen valvova viranomainen Suomessa on Tietosuojavaltuutetun toimisto.

Asetusehdotuksen mukaan EHDS-asetusta sovellettaisiin 12 kuukauden kuluttua sen voimaantulosta (72 artikla). Asetusehdotuksessa eikä sitä koskevassa valtioneuvoston kirjelmässä ole tarkemmin määritelty EHDS-asetuksen voimaantuloajankohtaa. Valviran näkemyksen mukaan 12 kuukautta ei ole realistinen aika toimeenpanna asetuksessa ehdotettuja muutoksia, jotka ovat laajuudeltaan ja vaikutukseltaan merkittäviä.

Lopuksi

Valviran näkemyksen mukaan toimintamalliin, jossa terveydenhuollon toiminnan kannalta kriittinen tietojärjestelmä voitaisiin ottaa käyttöön käytännössä tietojärjestelmän valmistajan tekemien dokumenttien perusteella, sisältyy merkittäviä riskejä. Valvira katsoo, että sosiaali- ja terveydenhuollon erityisluonne huomioiden sosiaali- ja terveydenhuollon tietojärjestelmien markkinoille pääsyä on tarkoituksenmukaista kontrolloida ennakollisesti kuten nykyisin asiakastietolain nojalla tapahtuu.

Valvira katsoo kokonaisuudessaan, että sosiaali- ja terveydenhuollon toimialalla on perusteltua, että siellä käytettäviin kriittisiin tietojärjestelmiin kohdistetaan ennen tuotantokäytön aloittamista vähintään ulkopuolisen tekemä tietoturvallisuuden arviointi. Asiakastietojen tietoturvan ja salassapidon sekä asianmukaisen käsittelyn vaatimukset korostuvat entisestään, kun asiakastietoja tallennetaan hyvin erilaisiin tietojärjestelmiin ja tietoja siirretään unionin tasolla jäsenvaltiosta toiseen.

Ratkaisija: Henriksson Markus
Virka-asema: Ylijohtaja
Esittelijät:
Malava Arttu, Lakimies

Asiakirja on sähköisesti allekirjoitettu asiankäsittelyjärjestelmässä.
Allekirjoituksen oikeellisuuden voi todentaa kirjaamosta.

Lisätietoja

Asiasta antaa tarvittaessa lisätietoja lakimies Arttu Malava, puh. 0295 209 231