



Valvira

Lausunto

17.01.2020

Asia: VN/12603/2019

Lausuntopyyntö luonnoksesta hallituksen esitykseksi eduskunnalle laiksi sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä sekä eräksi siihen liittyviksi laeiksi

1. Asiakas- ja potilastietojen käsittely ja luovuttaminen

Onko asiakas- ja potilastietojen käsittelystä ja luovuttamisesta säädetty riittävän selkeästi ja tarkasti? Jos ei ole, miten säännöstä pitäisi muuttaa?

Asiakas- ja potilastietojen käsittelystä on säädetty riittävän selkeästi ja tarkasti.

2. Tahdonilmaukset

Tiedonhallintapalvelua koskevaan 11 §:ään on lisätty uusi kohta liittyen muihin asiakkaan sosiaali- ja terveydenhuoltoon kytkeytyviin palveluihin ja asiakastietojen käsittelyyn liittyvistä tahdonilmauksista. Tiedonhallintapalveluun voisi tallentaa esimerkiksi henkilön vastustuksen hänen tietojensa käytöstä biopankkitoiminnassa. Onko tahdonilmauksista käsittelystä ja luovuttamisesta säädetty riittävän selkeästi ja tarkasti? Jos ei ole, miten säännöstä pitäisi muuttaa?

Tahdonilmauksien kirjaamisesta järjestelmään on pääasiassa säädetty riittävän selkeästi ja tarkasti.

Lakiehdotuksen 11 §:n säännös on muotoiltu siten, että 2 momentin kohdissa 1-5 luetellut tiedot on tallennettava tiedonhallintapalveluun. Kohdassa 3 todetaan, että tiedonhallintapalveluun on tallennettava tiedot muista asiakkaan terveyden- ja sairaanhoitoon tai sosiaalipalveluihin liittyvistä tahdonilmauksista. Tämä vaatimus on ilmaistu melko epätarkasti ja saattaa aiheuttaa epäselvyyttä sen suhteen, mitä kaikkia tahdonilmauksia tulee tallentaa tiedonhallintapalveluun. Sääntelyn joustava muotoilu mahdollistaa tapauskohtaista harkintaa, mutta on kuitenkin tärkeätä, että tästä lain säännöksestä on hallituksen esityksen lisäksi myös muuta ohjeistusta saatavilla.

3. Erityissuojattavat asiakirjat

Lain 9 §:stä poistettaisiin sosiaali- ja terveysministeriön asetuksenantovaltuus siitä, mitkä asiakasasiakirjat on luokiteltava erityistä suojausta edellyttäviksi. Lain mukaan Terveiden ja hyvinvoinnin laitos antaisi määräykset valtakunnallisten tietojärjestelmäpalvelujen toteutuksen edellyttämistä tietojärjestelmien olennaisista vaatimuksista ja määrittää asiakasasiakirjojen tietosisällöt ja tietorakenteet sekä tietorakenteissa valtakunnallisesti hyödynnettävät koodistot. Pitäisikö erityissuojattavista asiakirjoista säätää asiakastietolaissa ja potilasasiakirja-asetuksessa? Onko erityissuojattavista asiakirjoista säädetty riittävän selkeästi ja tarkasti? Jos ei ole, miten säännöstä pitäisi muuttaa?

Lain säännöksissä ei ole suoraan ilmaistu mitään erityissuojattavista asiakirjoista. Huomioon ottaen, että tietosuojasäännöksissä on säännökset erityisistä henkilötiedoista ja niiden käsittelystä, niin tulisi välttää mahdollista sekaannusta tietojen luokittelussa. Tietosuoja-asetuksen mukaan kaikki asiakirjat, jotka sisältävät henkilön terveystietoja ovat erityisasemassa. Vaikuttaisi näin ollen hieman ongelmalliselta antaa viranomaisen laitokselle valtuudet määrittellä mitkä asiakirjat ovat erityissuojattuja ja mitä tämä käytännössä tarkoittaa.

4. Omätietovaranto

Lain 12 §:ssä säädettäisiin, että henkilö voi antaa suostumuksensa siihen, että palvelunantajalle voidaan luovuttaa omätietovarannossa olevia hyvinvointitietoja sosiaali- ja terveyspalvelujen toteuttamiseksi. Onko hyvinvointitietojen luovuttamisesta säädetty riittävän selkeästi ja tarkasti? Jos ei ole, miten säännöstä pitäisi muuttaa?

Valvira katsoo, että hyvinvointitietojen luovuttamisesta on säädetty riittävän selkeästi ja tarkasti. Säännös itsessään ei ole erityisen yksityiskohtainen, mutta siitä ilmenee kuitenkin tärkeimmät asiat.

5. Omätietovaranto

Lain 19 ja 21 §:ssä säädettäisiin, että henkilöllä on oikeus saada omat asiakas- ja potilastietonsa omätietovarantoon ja edelleen hyvinvointisovelluksiin hyödynnettäviksi. Onko asiakas- ja potilastietojen luovuttamisesta omätietovarantoon säädetty riittävän selkeästi ja tarkasti? Jos ei ole, miten säännöstä pitäisi muuttaa? Pitäisikö omätietovarantoon liittyvät hyvinvointisovellukset sertifioida?

Asiakas- ja potilastietojen luovuttamisesta omätietovarantoon on säädetty riittävän selkeästi ja tarkasti ehdotetun lain 19 §:ssä. Mikäli 21 § on tarkoitus koskea myös omätietovarantoa tulisi tämä olla selkeämmin muotoiltu pykälän tekstissä.

Omätietovarantoon liittyvät hyvinvointisovellukset tulisivat sisältämään paljon erityisiä henkilötietoja. Tällaisten tietojen käsittelystä ja tallentamisesta on varmistettava, että korkea tietosuojan ja tietoturvan taso toteutuu. Tästä näkökulmasta olisi tärkeätä, että sovelluksen käyttäjät voivat luottaa siihen, että sovellukset täyttävät tietyt vähimmäisvaatimukset. Näin ollen sertifiointi voisi olla hyvä vaihtoehto.

6. Valtakunnallisten tietojärjestelmäpalvelujen käytöstä perittävät maksut

Esityksen 47 §:ssä esitetään muutettavaksi valtakunnallisten tietojärjestelmäpalveluiden käytöstä perittävien maksujen perusteita siten, että Kansaneläkelaitoksen tulisi toimittaa arvio seuraavien neljän

vuoden kustannuksista yhden vuoden sijasta. Muutoksella tavoitellaan sitä, että merkittävien, valtakunnallisten tietojärjestelmäpalveluiden hoidon edellyttämien investointien kustannukset voidaan huomioida useamman vuoden jaksotuksella niin, etteivät kustannukset kasaannu yksittäiselle vuodelle. Onko maksuihin liittyvistä menettelyistä säädetty riittävän selkeästi ja tarkasti? Jos ei ole, miten säännöstä pitäisi muuttaa?

Valviralla ei tältä osin ole lausuttavaa asiassa.

7. Rekisteröidyn oikeus rajoittaa käsittelyä

Olisiko asiakastietolaissa säädettävä siitä, että rekisteröidyn oikeutta käsittelyn rajoittamiseen voitaisiin rajoittaa silloin, kun rekisteröity kiistää henkilötietojen paikkansapitävyyden (EU:n yleinen tietosuojasetus 18 art 1 kohta a alakohta)?

Valviralla ei tältä osin ole lausuttavaa asiassa.

8. Muut huomiot

Voitte kirjoittaa muut huomionne tähän

Asiakastietolain uudistus on ollut käynnissä jo useamman vuoden ajan ja Valvira on lausunut asiaan liittyen vuosina 2017 ja 2018. Valvira viittaa aikaisemmin lausuttuun ja haluaa lisäksi esittää alla olevan.

Valvira toistaa aikaisemmin lausunnoissaan esille tuomansa, että asiakastietolakiin on syytä lisätä selkeät säännökset siitä, että valvontaviranomaisella on oikeus saada tehtäviensä suorittamiseksi tarpeelliset tiedot teknistä käyttöyhteyttä käyttäen. Tällä hetkellä Valvira joutuu pyytämään muun muassa potilasasiakirjat manuaalisina suoraan kulloinkin kyseessä olevasta toimintayksiköstä. Joissakin tapauksissa toimintayksiköitä on samaan valvonta-asiaan liittyen useita. Digitalisaation edistäminen myös tässä toiminnassa olisi merkittävä parannus valvontaviranomaisen, mutta myös toimintayksiköiden toiminnassa.

Ehdotetun lain 29 §:n mukaan tietojärjestelmäpalvelun tuottajan on ilmoitettava A- tai B-luokkaan kuuluvasta tietojärjestelmästä Valviralle ennen sen ottamista tuotantokäyttöön. Lakiehdotuksen mukaan Valvira rekisteröisi tietojärjestelmän Valviran ylläpitämään julkiseen rekisteriin (29 §), jonka lisäksi Valvira myös valvoo ja edistää tietojärjestelmien vaatimustenmukaisuutta (40 §). Valviran tehtävänä on jo nykyisen sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetun lain (159/2007) mukaisesti valvoa ja edistää tietojärjestelmien vaatimustenmukaisuutta, mihin sisältyy muun muassa mahdollisuus tehdä tarkastuksia.

Valvira ehdottaa, että selvitetäisiin mahdollisuutta siirtää nyt lausunnolla olevan lain 29 §:ssä säädetyn rekisterin ylläpito ja rekisterimerkintöjen tekeminen Valviralta Kansaneläkelaitokselle. Kelalla olisi enemmän resursseja rekisterin tekniseen ylläpitoon kuin mitä Valviralla on.

Rekisterin ylläpidon siirtämistä Kelalle puoltaisi myös prosessin tehostuminen. Mikäli tehtävä ylläpitää rekisteriä siirtyisi Kelalle, rekisterimerkinnän tekeminen ja siten rekisterin päivitys voisi tapahtua heti kun vaatimukset rekisterimerkinnän tekemiselle täyttyvät. Nykytilanteessa rekisterin päivitys tapahtuu noin kerran kuukaudessa. Rekisteri olisi Kelan ylläpitämänä jatkossa paremmin ajan tasalla, mikä palvelisi myös valvontaa. Tämä mahdollistaisi myös sen, että Valvirassa olevat resurssit voitaisiin jatkossa keskittää tehokkaammin valvontatehtäviin, sillä rekisterin ja rekisteröityjen tietojärjestelmien valvonta säilyisi edelleen Valvirassa.

Tietojärjestelmien tietoturvallisuuden arvioinnista ja vaatimustenmukaisuustodistuksen voimassaolosta säädettäisiin lakiehdotuksen mukaan 36 §:ssä. Ehdotuksen mukaan tietoturvallisuuden arviointilaitos suorittaa tietoturvallisuusvaatimustenmukaisuuden arvioinnin sekä antaa tuottajalle vaatimustenmukaisuustodistuksen. Ennen vaatimustenmukaisuustodistuksen antamista Kelan on kuitenkin annettava yhteistestaukseen perustuvan puoltavan lausunnon. Valvira katsoo, että vaatimustenmukaisuustodistuksen tulisi antaa Kela. Tietoturvallisuuden arvioinnin suorittaisi kuitenkin tietoturvallisuuden arviointilaitos. Kela antaisi vaatimustenmukaisuustodistuksen sen jälkeen, kun tietoturvallisuuden arviointi ja yhteistestaus ovat suoritettuina.

Myös sellainen vaihtoehto on ollut esillä, että tehtävä antaa vaatimustenmukaisuustodistukset siirrettäisiin Valviraan. Valviralla ei ole ollut mahdollisuutta arvioida tätä vaihtoehtoa tarkemmin. On kuitenkin todettava, että Valviralla ei nykytilanteessa ole riittäviä resursseja tällaiset tehtävän hoitamiseen.

Vaatimustenmukaisuustodistuksen voimassaolon enimmäisajaksi tulisi säätää kolme vuotta ehdotetun viiden vuoden sijaan. Viiden vuoden aikana on todettu tapahtuvan muutoksia järjestelmien teknisessä toteutuksessa ja myös Kanta-määrittelyissä. Voimassaolon lyhentäminen ehkäisisi järjestelmien muutoksista aiheutuvien poikkeamatilanteiden riskien toteutumista. Vaatimustenmukaisuuden voimassaoloajan päättymisen ohjaisi tekemään yhteistestauksen uudelleenarvioinnin riittävän säännöllisesti.

Valviralle on asiakastietolain mukaisesti tehtäviin osoitettu määrärahat yhden henkilön palkkaamiseen. Tehtävät ovat kuitenkin niin laajat, että yksi henkilö ei voi tehdä kaikkia lakiehdotuksessa virastolle säädettävistä tehtävistä. Valviran ylläpitämässä rekisterissä on 75 A-luokan ja 229 B-luokan tietojärjestelmää (31.12.2019). Asiakastietolain perusteella tehtyjä poikkeamailmoituksia tehtiin vuoden 2019 aikana 60. Osa poikkeamailmoituksista on liittynyt laaja-alaisiin, hyvin vakavasti potilasturvallisuutta vaarantaviin julkisuudessaakin olleisiin tilanteisiin. Asiakastietolain mukaisessa tehtävässä Valvira on voinut aikaisemmin tukeutua virastossa olevaan terveydenhuollon laitteisiin liittyvään ohjelmistoasiantuntemukseen, joka on siirretty vuoden 2020 alusta Lääkealan turvallisuus- ja kehittämiskeskus Fimeaan. Valviran näkemyksen mukaan tehtävät muutokset ja tehtävään nykyisellään osoitetut resurssit ovat täysin riittämättömät ottamaan huomioon toimialalla tapahtuvat laajat tietojärjestelmien muutokset. Vaikka rekisterin ylläpito siirtyisi Kelalle, Valviran arvion mukaan asiakaslaissa Valviralle osoitettujen tehtävien hoitaminen

edellyttäisi aiemman yhden henkilön lisäksi toisen asiantuntijan viran perustamista asiakastietolain mukaisiin valvonnan tehtäviin.

Kujala Ritva
Valvira

Aaltonen Jonna
Valvira