SUOMEN SÄÄDÖSKOKOELMA

Julkaistu Helsingissä 31 päivänä maaliskuuta 2014

250/2014

Laki

sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetun lain muuttamisesta

Annettu Helsingissä 28 päivänä maaliskuuta 2014

Eduskunnan päätöksen mukaisesti

muutetaan sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetun lain (159/2007) 2 §:n 3 momentti, 3 §:n 7 ja 8 kohta, 5 §:n 2 momentti, 14 §:n 1 momentti, 14 a §:n 3 ja 4 momentti, 17—19 §, 20 §:n 4 ja 5 momentti ja 22 §,

sellaisina kuin niistä ovat 2 §:n 3 momentti, 20 §:n 4 ja 5 momentti ja 22 § laissa 981/2010, 3 §:n 8 kohta laissa 928/2011 sekä 14 §:n 1 momentti, 14 a §:n 3 ja 4 momentti sekä 17 ja 19 § laissa 1227/2010, sekä

lisätään 3 §:ään, sellaisena kuin se on osaksi laeissa 1227/2010 ja 928/2011, siitä lailla 1227/2010 kumotun 6 kohdan tilalle uusi 6 kohta, sekä uusi 9 ja 10 kohta, 16 §:ään, sellaisena kuin se on osaksi laeissa 981/2010 ja 1227/2010, siitä lailla 981/2010 kumotun 5 momentin tilalle uusi 5 momentti sekä lakiin uusi 5 a—5 c luku ja 20 a—20 h § seuraavasti:

2 §

Soveltamisala

— — — — — — — — — — — — — —

Jollei tästä tai muusta laista muuta johdu, asiakastietojen käsittelyyn sovelletaan, mitä potilaan asemasta ja oikeuksista annetussa laissa (785/1992), jäljempänä *potilaslaki*, sosiaalihuollon asiakkaan asemasta ja oikeuksista annetussa laissa (812/2000), jäljempänä *asiakaslaki*, henkilötietolaissa (523/1999), viranomaisten toiminnan julkisuudesta annetussa laissa (621/1999), sähköisestä asioinnista viranomaistoiminnassa annetussa laissa (13/2003), vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetussa laissa (617/2009), väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista annetussa laissa (661/2009) sekä arkistolaissa (831/1994) tai näiden nojalla säädetään. Lisäksi asiakastietojen käsittelyssä ja tämän lain mukaisia palveluja ja toimintoja järjestettäessä on noudatettava, mitä kielilaissa (423/2003) ja sen nojalla säädetään. Jos terveydenhuollon asiakas- ja potilastietoja käsittelevä tietojärjestelmä on terveydenhuollon laitteista ja tarvikkeista annetussa laissa (629/2010) tarkoitettu terveydenhuollon laite, tietojärjestelmään sovelletaan myös mainittua lakia ja sen mukaisia vaatimuksia.

3 §

Määritelmät

Tässä laissa tarkoitetaan:

— — — — — — — — — — — — — —

6) *tietojärjestelmällä* sosiaali- tai terveydenhuollon asiakastietojen sähköistä käsittelyä varten toteutettua ohjelmistoa tai järjestelmää, jonka avulla tallennetaan ja ylläpidetään

HE 219/2013
StVM 1/2014
EV 10/2014

asiakas- tai potilasasiakirjoja ja niissä olevia tietoja sekä kerätyistä tiedoista muodostettua automaattisen tietojenkäsittelyn avulla ylläpidettävää tiedostoa tai tietovarantoa, jonka valmistaja on erityisesti suunnitellut sosiaali- tai terveydenhuollon asiakas- tai potilasasiakirjojen ja niissä olevien tietojen käsittelyyn; lisäksi tietojärjestelmällä tarkoitetaan välityspalvelua, jolla sosiaali- tai terveydenhuollon asiakastietoja välitetään jäljempänä 14 §:n 1 momentissa tarkoitettuihin Kansaneläkelaitoksen ylläpitämiin valtakunnallisiin tietojärjestelmäpalveluihin;

7) *terveydenhuollon palvelujen antajalla* potilaslain 2 §:n 4 kohdassa tarkoitettua terveydenhuollon toimintayksikköä, työterveyshuoltolain (1383/2001) 7 §:n 2 kohdassa tarkoitettua työnantajaa sekä itsenäisenä ammatinharjoittajana toimivaa terveydenhuollon ammattihenkilöä;

8) *sosiaalihuollon palvelujen antajalla* asiakaslain 3 §:n 2 kohdassa tarkoitettua sosiaalihuoltoa järjestävää viranomaista, julkista sosiaalipalvelujen tuottajaa sekä yksityisistä sosiaalipalveluista annetussa laissa (922/2011) tarkoitettua palvelujen tuottajaa;

9) *tietoturvallisuuden arviointilaitoksella* sellaista yritystä, yhteisöä ja viranomaista, jonka Viestintävirasto on hyväksynyt tietoturvallisuuden arviointilaitoksista annetun lain (1405/2011) perusteella suorittamaan tietojärjestelmien vaatimustenmukaisuuden arviointeja; sekä

10) *yhteentoimivuudella* tietojärjestelmien teknistä ja tietosisällöllistä yhteentoimivuutta muiden tietojärjestelmien kanssa silloin, kun järjestelmät käyttävät samoja tietoja.

5 §

Käytön ja luovutuksen seuranta

— — — — — — — — — — — — —

Palvelujen antajan tulee kerätä asiakasrekisterikohtaisesti kaikesta asiakastietojen käytöstä ja jokaisesta asiakastietojen luovutuksesta seurantaa varten lokitiedot lokirekisteriin. Käyttölokirekisteriin tallennetaan tieto käytetyistä asiakastiedoista, siitä palvelujen antajasta, jonka asiakastietoja käytetään, asiakastietojen käyttäjästä, tietojen käyttötarkoituksesta ja käyttöajankohdasta. Luovutuslokirekisteriin tallennetaan tieto luovutetuista asiakastiedoista, siitä palvelujen antajasta, jonka asiakastietoja luovutetaan, asiakastietojen luovuttajasta, tietojen luovutustarkoituksesta, luovutuksensaajasta ja luovutusajankohdasta. Kansaneläkelaitoksen tulee kerätä vastaavat tiedot 14 a §:ssä tarkoitettuun potilaan tiedonhallintapalveluun tallennettujen ja sen kautta näytettyjen tietojen luovuttamisesta.

— — — — — — — — — — — — —

14 §

Valtakunnalliset tietojärjestelmäpalvelut

Kansaneläkelaitos hoitaa terveydenhuollon palvelujen antajien lukuun potilasasiakirjojen säilytystä ja käyttöä varten olevaa arkistointipalvelua sekä sen osana potilasasiakirjojen luovutusta varten hakemistopalvelua ja potilaan tiedonhallintapalvelua. Arkistointipalveluun voidaan tallentaa potilasasiakirjojen lisäksi myös muita terveydenhuollon järjestämiseen ja tiedonhallintaan liittyviä asiakirjoja. Lisäksi Kansaneläkelaitos hoitaa valtakunnallisiin tietojärjestelmäpalveluihin kuuluvina tehtävinä luovutuslokirekisterien säilytyksen osana arkistointipalvelua, 19 §:ssä tarkoitetun kansalaisen käyttöliittymän sekä palvelun, jonka avulla valtakunnallisia tietojärjestelmäpalveluja voi käyttää Internetin välityksellä sekä tietoliikenneverkkoja käyttävillä liikutettavilla laitteilla. Kansaneläkelaitos voi hoitaa myös muita sosiaali- ja terveydenhuollon tiedonhallintaan liittyviä valtakunnallisia palveluja siten kuin niistä erikseen muualla säädetään sekä huolehtia käyttölokirekisterien säilytyksestä. Kansaneläkelaitos voi tarvittaessa antaa ohjeita edellä mainittujen valtakunnallisten tietojärjestelmäpalveluiden toteuttamisen edellyttämistä teknisistä ja sanomaliikennemäärityksistä.

— — — — — — — — — — — — —

14 a §

Potilaan tiedonhallintapalvelu

— — — — — — — — — — — — —

Potilaan tiedonhallintapalvelun kautta voidaan lisäksi näyttää potilaan terveyden- ja sairaanhoidon tai niihin liittyvien palvelujen

kannalta keskeiset tiedot. Sosiaali- ja terveysministeriön asetuksella voidaan säätää siitä, mitkä ovat tiedonhallintapalvelun kautta näytettäviä keskeisiä tietoja. Tiedonhallintapalvelun välityksellä ei saa kuitenkaan näyttää sellaisia tietoja, joiden luovutuksen potilas on kieltänyt 10—12 §:n perusteella.

Kansaneläkelaitos on potilaan tiedonhallintapalvelun rekisterinpitäjä. Kansaneläkelaitos vastaa tiedonhallintapalvelussa olevien tietojen käytettävyydestä ja eheydestä, tietosisältöjen muuttumattomuudesta sekä tietojen säilyttämisestä ja hävittämisestä. Tiedon tallentaja vastaa potilaan tiedonhallintapalveluun tallennettujen tietojen oikeellisuudesta ja palvelussa olevan virheellisen tiedon korjaamisesta. Tiedonhallintapalvelussa olevien virheellisten tietojen korjaamiseen sovelletaan, mitä henkilötietolain 29 §:ssä säädetään. Jos virheellinen tieto perustuu terveydenhuollon palvelujen antajan tekemään merkintään, on korjausvaatimus osoitettava virheellisen merkinnän tehneelle palvelujen antajalle.

16 §

Vastuut tietojärjestelmäpalvelujen hoidossa

— — — — — — — — — — — — — —

Kansaneläkelaitos voi laatia ja luovuttaa arkistointipalvelussa olevien asiakirjojen kuvailutiedoista yhteenvetoja, joilla voi olla merkitystä valtakunnallisten tietojärjestelmäpalvelujen kehittämisessä, seurannassa tai raportoinnissa. Lisäksi Kansaneläkelaitos voi luovuttaa potilaan tiedonhallintapalvelussa olevia 14 a §:n 2 momentin mukaisia tietoja potilaan tahdonilmaisuista potilaslain 13 §:n 2—5 momentissa säädetyillä perusteilla.

17 §

Potilaan informointi

Valtakunnallisiin tietojärjestelmäpalveluihin liittyneen terveydenhuollon palvelujen antajan on annettava tiedot potilaalle valtakunnallisista tietojärjestelmäpalveluista, niiden yleisistä toimintaperiaatteista ja niihin liittyvistä potilaan oikeuksista. Tiedot tulee antaa ennen ensimmäistä palvelutapahtumaa tai sen yhteydessä. Lisäksi potilaalle tulee antaa tiedot tietojärjestelmäpalvelujen järjestäjästä, potilastietojen luovutuksen edellytyksistä, tietojen suojaamisesta sekä muista potilaan kannalta merkityksellisistä tietojen käsittelyyn liittyvistä seikoista.

Terveydenhuollon palvelujen antajan tulee antaa tiedot potilaalle henkilökohtaisesti kirjallisesti tai suullisesti. Tiedot voidaan antaa myös potilaan yksilöivän sähköisen palvelun välityksellä. Jos tiedot annetaan muulla tavalla kuin kirjallisesti, on potilaalla oltava mahdollisuus saada tiedot myös kirjallisena. Annetuista tiedoista tulee tehdä merkintä edellä 14 a §:ssä todettuun potilaan tiedonhallintapalveluun. Jos potilas on jo saanut edellä tarkoitetut tiedot, voidaan tiedonantovelvollisuudesta poikkeamiseen soveltaa, mitä henkilötietolain 24 §:ssä säädetään.

Tietojen antamisen menettelytavoista ja sisällöstä voidaan tarvittaessa antaa tarkempia säännöksiä sosiaali- ja terveysministeriön asetuksella.

18 §

Asiakkaan tiedonsaantioikeus

Asiakkaan oikeudesta tarkastaa asiakasrekisterin tietoja ja oikeuden toteuttamisesta säädetään henkilötietolain 26—28 §:ssä.

Asiakkaalla on oikeus saada asiakastietojensa käsittelyyn liittyvien oikeuksiensa selvittämistä tai toteuttamista varten sosiaalihuollon ja terveydenhuollon palvelujen antajalta kirjallisesta pyynnöstä viivytyksettä lokirekisterin perusteella maksutta tieto siitä, kuka on käyttänyt tai kenelle on luovutettu häntä koskevia tietoja sekä mikä on ollut käytön tai luovutuksen peruste. Asiakkaalla on vastaava oikeus saada Kansaneläkelaitokselta tieto 14 a §:ssä tarkoitettuun potilaan tiedonhallintapalveluun tallennettujen ja sen kautta näytettävien tietojen luovuttamisesta. Asiakkaalla ei kuitenkaan ole oikeutta saada lokitietoja, jos lokitietojen luovuttajan tiedossa on, että lokitietojen antamisesta saattaisi aiheutua vakavaa vaaraa asiakkaan terveydelle tai hoidolle taikka jonkun muun oikeuksille. Myöskään kahta vuotta vanhempia lokitietoja ei ole oikeutta saada, jollei siihen ole erityistä syytä. Asiakas ei saa käyttää tai luovuttaa saamiaan lokitietoja edelleen muuhun tarkoitukseen.

Jos asiakas pyytää toistamiseen saman ajanjakson lokitietoja, palvelujen antaja tai Kansaneläkelaitos voi periä lokitietojen antamisesta kohtuullisen korvauksen, joka ei saa ylittää tiedon antamisesta aiheutuvia välittömiä kustannuksia. Pääsystä lokitietoihin 19 §:ssä tarkoitetun katseluyhteyden avulla ei kuitenkaan saa periä erillistä maksua.

Jos asiakas katsoo, että hänen asiakastietojaan on käytetty tai luovutettu ilman riittäviä perusteita, tietoja käyttäneen tai tietoja saaneen palvelujen antajan tai Kansaneläkelaitoksen tulee antaa asiakkaalle pyynnöstä selvitys tietojen käytön tai luovuttamisen perusteista.

19 §

Kansalaisen käyttöliittymä

Potilaalle annetaan kansalaisen käyttöliittymän avulla valtakunnalliseen arkistointipalveluun hänestä tallennetut seuraavat tiedot:

1) tiedot suostumuksesta ja kielloista sekä luovutuslokitiedot lukuun ottamatta luovuttajan ja luovutuksensaajan henkilötietoja sekä niitä luovutuslokitietoja, joita potilaalla ei henkilötietolain 27 §:n 1 momentin 1—4 kohdan mukaan ole oikeutta saada;

2) tieto potilaan tiedonhallintapalveluun merkitystä elinluovutuskiellosta, hoitotahdosta ja muusta potilaan terveyden- ja sairaanhoitoa tai elinluovutusta koskevasta tahdonilmaisusta;

3) tiedot palvelutapahtumien paikoista ja ajoista, hoidon kannalta keskeiset tiedot, lääkemääräystiedot ja hoito-ohjeet; sekä

4) lähetteet, yhteenvedot annetuista hoidoista, hoitojen loppulausunnot sekä lääkärintodistukset ja -lausunnot.

Potilaalle voidaan antaa kansalaisen käyttöliittymän avulla myös ajanvaraustiedot sekä laboratoriotulokset, kuvantamistulokset ja muut vastaavat tutkimustulokset. Käyttöliittymään voidaan 1 momentissa mainittujen toimintojen lisäksi liittää muita potilaan tiedonsaantia sekä hoidon ja terveydenhuoltoon muutoin liittyvien tehtävien toteuttamista ja seuraamista mahdollistavia toimintoja.

Sen estämättä, mitä 1 ja 2 momentissa säädetään, käyttöliittymä on toteutettava siten, ettei potilaalla ole pääsyä niihin tietoihin, joiden luovuttamisesta voi terveydenhuollon ammattihenkilön harkinnan mukaan aiheutua vakavaa vaaraa potilaan terveydelle tai hoidolle taikka jonkun muun oikeuksille.

Käyttöliittymä tulee toteuttaa siten, että potilas voi antaa 11 §:ssä tarkoitetun suostumuksen ja tehdä 12 §:ssä tarkoitetun kiellon sekä tehdä elinluovutuskiellon, hoitotahdon ja muun terveyden- ja sairaanhoitoa koskevan tahdonilmaisun käyttöliittymän välityksellä. Lisäksi käyttöliittymää toteutettaessa tulee varmistaa, että potilaan yksityisyyden suoja ei vaarannu. Alaikäisen potilaan tiedot saa luovuttaa käyttöliittymän kautta potilaan lisäksi hänen huoltajalleen tai muulle lailliselle edustajalleen. Tietojen luovutuksessa on tällöin otettava huomioon, mitä potilaan asemasta ja oikeuksista annetun lain 9 §:n 2 momentissa säädetään alaikäisen potilaan oikeudesta kieltää terveydentilaansa koskevien tietojen antaminen potilaan huoltajalle tai muulle laillliselle edustajalle. Tietojen saanti käyttöliittymän avulla ei vaikuta potilaan henkilötietolain mukaiseen tarkastusoikeuteen.

Sosiaali- ja terveysministeriön asetuksella voidaan antaa tarkempia säännöksiä tiedonsaantia, hoidon toteuttamista ja seurantaa koskevien tietojen sisällöstä ja niiden liittämisestä käyttöliittymään sekä siitä, miten tiedot annetaan käyttöliittymän kautta ja miten alaikäisen potilaan huoltajan tai laillisen edustajan oikeus saada tietoja toteutetaan.

5 a luku

Tietojärjestelmien olennaiset vaatimukset ja niiden osoittaminen

19 a §

Olennaiset vaatimukset

Sosiaali- tai terveydenhuollon asiakastietojen käsittelyssä käytettävän tietojärjestelmän tulee täyttää yhteentoimivuutta, tietoturvaa ja tietosuojaa sekä toiminnallisuutta koskevat olennaiset vaatimukset.

Tietojärjestelmä täyttää olennaiset vaatimukset silloin, kun se on suunniteltu, valmistettu ja toimii tietoturvaa ja tietosuojaa koskevien lakien ja niiden nojalla annettujen säännösten sekä yhteentoimivuutta koskevien kansallisten määritysten mukaisesti. Toimin-

nallisuutta koskevat olennaiset vaatimukset täyttyvät, jos tietojärjestelmä on käyttötarkoitukseensa sopiva ja sillä pystytään suorittamaan käyttötarkoituksen mukaisessa asiakas- ja potilastietojen käsittelyssä lakien ja niiden nojalla annettujen säännösten edellyttämät toiminnot ja sen suorituskyky on valmistajan ilmoittama. Vaatimusten on täytyttävä käytettäessä tietojärjestelmää sekä itsenäisesti että yhdessä muiden siihen liitettäväksi tarkoitettujen tietojärjestelmien kanssa.

Terveyden ja hyvinvoinnin laitos voi tarvittaessa antaa tarkempia määräyksiä olennaisten vaatimusten sisällöstä. Ennen määräyksen antamista Terveyden ja hyvinvoinnin laitoksen on kuultava sosiaali- ja terveydenhuollon sähköisen tietohallinnon neuvottelukuntaa. Lisäksi Kansaneläkelaitos voi antaa määräyksiä tässä laissa tai sähköisestä lääkemääräyksestä annetussa laissa tarkoitettuihin terveydenhuollon valtakunnallisiin tietojärjestelmäpalveluihin, jäljempänä *Kanta-palvelut*, liitettävien tietojärjestelmien yhteentoimivuuden todentamisessa noudatettavista menettelyistä.

19 b §

Luokitus

Sosiaali- ja terveydenhuollon tietojärjestelmät jaotellaan käyttötarkoitustensa ja ominaisuuksiensa perusteella luokkiin A ja B. Luokkaan A kuuluvat Kansaeläkelaitoksen ylläpitämät Kanta-palvelut sekä tietojärjestelmät, jotka on tarkoitettu liitettäväksi Kanta-palveluihin joko suoraan tai teknisen välityspalvelun kautta. Luokkaan A kuuluu myös 3 §:n 6 kohdassa tarkoitettu välityspalvelu. Muut tietojärjestelmät kuuluvat luokkaan B.

Jos on epäselvää, mihin luokkaan tietojärjestelmä kuuluu, Terveyden ja hyvinvoinnin laitos päättää kumpaan luokkaan tietojärjestelmä kuuluu.

Terveyden ja hyvinvoinnin laitos voi antaa tarkempia määräyksiä tietojärjestelmien luokkien määräytymisestä.

19 c §

Tietojärjestelmän valmistajan yleiset velvollisuudet

Valmistaja on vastuussa sosiaali- ja terveydenhuollon tietojärjestelmän suunnittelusta, valmistuksesta ja luokittelusta riippumatta siitä, suorittaako valmistaja nämä toimet itse vai tekeekö joku muu ne hänen lukuunsa.

Valmistajan on annettava tietojärjestelmän yhteydessä järjestelmän käyttäjälle yhteentoimivuuden, tietoturvallisuuden ja tietosuojan sekä toiminnallisuuden kannalta tarpeelliset tiedot ja ohjeet järjestelmän käyttöönotosta, tuotantokäytöstä ja ylläpidosta. Tietojärjestelmän mukana olevien tietojen ja ohjeiden on oltava suomen, ruotsin tai englannin kielellä. Tietojärjestelmää käyttävälle sosiaali- tai terveydenhuollon henkilöstölle tarkoitettujen tietojen ja ohjeiden on kuitenkin oltava suomen ja ruotsin kielellä.

Lisäksi valmistajalla on oltava laatujärjestelmä, jota sovelletaan tietojärjestelmän suunnitteluun ja valmistukseen.

19 d §

Vaatimustenmukaisuuden osoittaminen

Luokkaan A kuuluvan tietojärjestelmän vaatimustenmukaisuus on osoitettava tietojärjestelmän valmistajan antamalla selvityksellä siitä, että järjestelmä täyttää kaikki toiminnallisuutta koskevat vaatimukset, hyväksytyllä yhteistestauksella ja tietoturvallisuuden arviointilaitoksen antamalla vaatimustenmukaisuustodistuksella.

Luokkaan B kuuluvan tietojärjestelmän vaatimustenmukaisuus on osoitettava valmistajan antamalla kirjallisella selvityksellä siitä, että järjestelmä asianmukaisesti asennettuna, ylläpidettynä ja käyttötarkoituksensa mukaan käytettynä täyttää 19 a §:ssä säädetyt olennaiset vaatimukset.

Terveyden ja hyvinvoinnin laitos voi antaa tarkempia määräyksiä vaatimustenmukaisuuden osoittamisessa noudatettavista menettelyistä ja annettavan selvityksen sisällöstä.

19 e §

Yhteistestaus

Luokkaan A kuuluvan tietojärjestelmän on oltava yhteentoimiva valtakunnallisten tietojärjestelmäpalvelujen ja siihen liitettyjen muiden tietojärjestelmien kanssa. Yhteentoi-

mivuus on osoitettava Kansaneläkelaitoksen järjestämässä yhteistestauksessa. Yhteistestauksen toteuttamisen edellytyksenä on, että tietojärjestelmän valmistaja antaa Kansaneläkelaitokselle selvityksen siitä, miten tietojärjestelmän toiminnallisuutta koskevat vaatimukset on toteutettu ja testattu. Yhteistestauksen ajankohdasta ja toteuttamisesta on sovittava Kansaneläkelaitoksen kanssa.

Tuotantokäyttöön otetun luokkaan A kuuluvan tietojärjestelmän on oltava mukana valtakunnallisiin tietojärjestelmäpalveluihin liitettävien muiden tietojärjestelmien yhteistestauksissa tietojärjestelmien keskinäisen yhteentoimivuuden varmistamiseksi. Kansaneläkelaitos päättää niistä tietojärjestelmistä, joiden tulee osallistua yhteistestaukseen. Yhteistestaukseen osallistuvien tietojärjestelmien valmistajat vastaavat itse testauksen niille aiheuttamista kustannuksista.

Edellä 1 momentissa säädetystä poiketen Kansaneläkelaitoksen ylläpitämille keskitetyille tietojärjestelmille ei suoriteta erillistä yhteistestausta.

19 f §

Tietojärjestelmän käyttöönotto

Luokkaan A kuuluvan tietojärjestelmän saa ottaa tuotantokäyttöön ja liittää Kantapalveluihin, kun tietoturvallisuuden arviointilaitos on antanut sitä koskevan vaatimustenmukaisuustodistuksen. Luokkaan B kuuluvan tietojärjestelmän saa ottaa tuotantokäyttöön sen jälkeen, kun järjestelmän valmistaja on antanut 19 d §:ssä tarkoitetun kirjallisen selvityksen.

Valmistajan on ilmoitettava tuotantokäyttöön otettavasta tietojärjestelmästä Sosiaali- ja terveysalan lupa ja valvontavirastolle. Ilmoituksessa on oltava tieto tietojärjestelmän valmistajasta ja käyttötarkoituksesta. Lisäksi valmistajan on ilmoitettava tietojärjestelmän tuotantokäytön päättymisestä. Lupa- ja valvontavirasto ylläpitää julkista rekisteriä sille ilmoitetuista sosiaali- ja terveydenhuollon tietojärjestelmistä.

Sosiaali- ja terveysalan lupa ja valvontavirasto voi antaa tarkempia määräyksiä ilmoituksen sisällöstä ja rekisteriin merkittävistä tiedoista.

19 g §

Käyttöönoton jälkeinen seuranta

Valmistajan on seurattava ja arvioitava ajantasaisella järjestelmällisellä menettelyllä tietojärjestelmästä sen tuotantokäytön aikana saatavia kokemuksia. Tietojärjestelmän olennaisten vaatimusten merkittävistä poikkeamista on ilmoitettava kaikille järjestelmää käyttäville palvelujen antajille. Lisäksi luokkaan A kuuluvien tietojärjestelmien merkittävistä poikkeamista on ilmoitettava tietoturvallisuuden arviointilaitokselle ja Sosiaali- ja terveysalan lupa- ja valvontavirastolle.

Tietojärjestelmän valmistajan on lisäksi seurattava tietojärjestelmien olennaisten vaatimusten muutoksia ja tehtävä tietojärjestelmiin muutosten edellyttämät korjaukset. Luokkaan A kuuluvan tietojärjestelmän muutoksista on ilmoitettava tietoturvallisuuden arviointilaitokselle. Vaatimustenmukaisuustodistus on uudistettava, jos tietojärjestelmään tehdään merkittäviä muutoksia tai olennaisia vaatimuksia on muutettu.

Valmistajan on säilytettävä vaatimustenmukaisuutta koskevat ja muut valvonnan edellyttämät tiedot vähintään viiden vuoden ajan tietojärjestelmän tuotantokäytön päättymisestä.

Terveyden ja hyvinvoinnin laitos voi antaa tarkempia määräyksiä siitä, mitkä ovat 1 momentissa tarkoitettuja merkittäviä poikkeamia ja miten niitä koskevat ilmoitukset tehdään.

5 b luku

Palvelujen antajan omavalvonta

19 h §

Omavalvontasuunnitelma

Sosiaalihuollon ja terveydenhuollon palvelujen antajan on laadittava tietoturvaan ja tietosuojaan sekä tietojärjestelmien käyttöön liittyvä omavalvontasuunnitelma. Siinä on selvitettävä, miten seuraavat järjestelmien käyttöön liittyvät asiat varmistetaan:

1) henkilöillä, jotka käyttävät tietojärjestelmiä, on niiden käytön vaatima koulutus ja kokemus;

2) tietojärjestelmien yhteydessä on saata-

villa niiden asianmukaisen käytön kannalta tarpeelliset käyttöohjeet;

3) tietojärjestelmiä käytetään valmistajan antaman ohjeistuksen mukaisesti;

4) tietojärjestelmiä ylläpidetään ja päivitetään valmistajan ohjeistuksen mukaisesti;

5) käyttöympäristö soveltuu tietojärjestelmien asianmukaiseen sekä tietoturvan ja tietosuojan varmistavaan käyttöön;

6) tietojärjestelmiin liitetyt muut tietojärjestelmät tai muut järjestelmät eivät vaaranna tietojärjestelmien suorituskykyä eivätkä niiden tietoturva- tai tietosuojaominaisuuksia; sekä

7) tietojärjestelmiä asentaa, ylläpitää ja päivittää vain henkilö, jolla on siihen tarvittava ammattitaito ja asiantuntemus.

Jos palvelujen antaja on liittynyt Kanta-palvelujen käyttäjäksi, on omavalvontasuunnitelmassa selvitettävä myös, miten näiden valtakunnallisten palvelujen tietoturvallisen käytön edellyttämät vaatimukset on varmistettu. Lisäksi 3 §:n 6 kohdassa tarkoitetun välityspalvelun tuottajan on laadittava omavalvontasuunnitelma välityspalvelusta ja Kansaneläkelaitoksen on laadittava suunnitelma ylläpitämistään Kanta-palveluista.

Palvelujen antajan, välityspalvelun tuottajan ja Kansaneläkelaitoksen on seurattava omavalvontasuunnitelman toteutumista.

Terveyden ja hyvinvoinnin laitos voi tarvittaessa antaa tarkempia määräyksiä 1 ja 2 momentissa tarkoitetuista omavalvontasuunnitelmaan sisällytettävistä selvityksistä ja vaatimuksista.

19 i §

Poikkeamista ilmoittaminen

Jos sosiaali- tai terveydenhuollon palvelujen antaja havaitsee, että tietojärjestelmän olennaisten vaatimusten täyttymisessä on merkittäviä poikkeamia, on palvelujen antajan ilmoitettava siitä tietojärjestelmän valmistajalle. Jos poikkeama voi aiheuttaa merkittävän riskin potilasturvallisuudelle, tietoturvalle tai tietosuojalle, on siitä ilmoitettava myös Sosiaali- ja terveysalan lupa- ja valvontavirastolle.

5 c luku

Tietojärjestelmien vaatimustenmukaisuuden arviointi

19 j §

Tietoturvallisuuden arviointilaitoksen hyväksyminen

Tietoturvallisuuden arviointilaitoksen hyväksymiseen ja toimintaan sovelletaan muutoin, mitä tietoturvallisuuden arviointilaitoksista annetussa laissa säädetään.

19 k §

Tietojärjestelmien arviointi

Luokkaan A kuuluvan sosiaali- ja terveydenhuollon tietojärjestelmän vaatimustenmukaisuuden arviointi suoritetaan tämän lain ja tietoturvallisuuden arviointilaitoksista annetun lain mukaisesti. Tämän lain mukaiseen tietoturvallisuuden arviointiin ei kuitenkaan sisälly tietojärjestelmän valmistajan eikä käyttäjän toimitilojen arviointi eikä tarkastaminen. Vaatimustenmukaisuuden arviointi tehdään tietojärjestelmän valmistajan hakemuksesta.

Jos luokkaan A kuuluva tietojärjestelmä täyttää vaatimustenmukaisuusedellytykset ja Kansaneläkelaitos on antanut yhteistestaukseen perustuvan puoltavan lausunnon yhteentoimivuutta koskevien vaatimusten täyttymisestä, tietoturvallisuuden arviointilaitoksen on annettava suorittamastaan vaatimustenmukaisuuden arvioinnista valmistajalle vaatimustenmukaisuustodistus sekä siihen liittyvä tarkastusraportti. Vaatimustenmukaisuustodistus on voimassa enintään viisi vuotta. Todistuksen voimassaoloa voidaan jatkaa enintään viideksi vuodeksi kerrallaan. Tietoturvallisuuden arviointilaitos voi vaatia valmistajalta kaikki arvioinnin edellyttämät tiedot vaatimustenmukaisuustodistuksen laatimiseksi ja ylläpitämiseksi. Todistuksen antamiseen sovelletaan muutoin, mitä tietoturvallisuuden arviointilaitoksista annetun lain 9 §:ssä säädetään.

Tietoturvallisuuden arviointilaitoksen on tarvittaessa, kotirauha huomioon ottaen, suoritettava tarkastuksia ja arviointeja varmis-

taakseen, että valmistaja ylläpitää kehitystyössään tietojärjestelmän vaatimustenmukaisuuden varmistavia menettelyjä, sekä annettava valmistajalle arviointikertomus. Tietoturvallisuuden arviointilaitoksen on otettava huomioon tietojärjestelmän tuotannon aikana suoritetuista arviointi- ja tarkastustoimista saadut tulokset.

19 l §

Vaatimustenmukaisuustodistuksen peruuttaminen

Jos tietoturvallisuuden arviointilaitos toteaa, ettei tietojärjestelmä ole täyttänyt tai enää täytä tässä laissa tai sen nojalla säädettyjä vaatimuksia tai että vaatimustenmukaisuustodistusta ei muutoin olisi tullut myöntää, laitoksen on kehotettava tietojärjestelmän valmistajaa korjaamaan puutteet. Arviointilaitos voi peruuttaa todistuksen määräajaksi tai kokonaan taikka myöntää sen rajoitettuna, jollei valmistaja korjaa puutteellisuuksia arviointilaitoksen asettamassa määräajassa. Määräajan pituutta määritettäessä on otettava huomioon tietojärjestelmän korjaamiseksi tarvittava kohtuullinen aika.

19 m §

Tietoturvallisuuden arviointilaitoksen ilmoittamisvelvollisuus

Tietoturvallisuuden arviointilaitoksen on ilmoitettava Sosiaali- ja terveysalan lupa- ja valvontavirastolle ja Kansaneläkelaitokselle tiedot kaikista myönnetyistä, muutetuista, täydennetyistä, määräajaksi tai kokonaan peruutetuista tai evätyistä vaatimustenmukaisuustodistuksista. Lisäksi tietotuvallisuuden arviointilaitoksen on pyydettäessä annettava lupa- ja valvontavirastolle kaikki tarvittavat lisätiedot.

20 §

Ohjaus, valvonta ja seuranta

— — — — — — — — — — — — —

Sosiaalihuollon ja terveydenhuollon palvelujen antajan, Kansaneläkelaitoksen, Sosiaali- ja terveysalan lupa- ja valvontaviraston ja Väestörekisterikeskuksen on omalta osaltaan seurattava ja valvottava, että sen antamaan palveluun liittyvä tietosuoja ja tietoturva toteutuvat. Jos joku on lainvastaisesti käsitellyt asiakastietoja, tulee asianomaisen palvelujen antajan sekä Kansaneläkelaitoksen oma-aloitteisesti ryhtyä tarvittaviin toimenpiteisiin. Seurannan ja valvonnan toteuttamiseksi palvelujen antajalla on oikeus saada Kansaneläkelaitokselta omien potilasrekisteriensä lokitiedot sekä 14 a §:ssä tarkoitetussa potilaan tiedonhallintapalvelussa olevien tietojen käsittelyyn liittyvät lokitiedot siltä osin kuin asianomaisen palvelujen antajan henkilökunta on katsellut ja käsitellyt potilaan tiedonhallintapalvelussa olevia tietoja.

Sosiaalihuollon ja terveydenhuollon toimintayksikön vastaavan johtajan tulee antaa kirjalliset ohjeet asiakastietojen käsittelystä ja noudatettavista menettelytavoista sekä huolehtia henkilökunnan riittävästä asiantuntemuksesta ja osaamisesta asiakastietojen käsittelyssä. Vastaavan johtajan tulee myös huolehtia 19 h §:ssä tarkoitetun omavalvontasuunnitelman laatimisesta ja noudattamisesta. Lisäksi jokaisella palvelujen antajalla ja Kansaneläkelaitoksella on oltava seuranta- ja valvontatehtävää varten tietosuojavastaava.

20 a §

Tietojärjestelmien valvonta ja tarkastukset

Sosiaali- ja terveysalan lupa- ja valvontaviraston tehtävänä on valvoa ja edistää tietojärjestelmien vaatimustenmukaisuutta.

Sosiaali- ja terveysalan lupa- ja valvontavirastolla on oikeus tehdä valvonnan edellyttämiä tarkastuksia. Tarkastuksen suorittamiseksi tarkastajalla on oikeus päästä kaikkiin tiloihin, joissa harjoitetaan tässä laissa tarkoitettua toimintaa tai säilytetään tämän lain noudattamisen valvonnan kannalta merkityksellisiä tietoja. Tarkastusta ei kuitenkaan saa tehdä pysyväisluonteiseen asumiseen käytettävissä tiloissa. Lisäksi tarkastusta toteutettaessa on noudatettava, mitä hallintolain (434/2003) 39 §:n 1 momentissa säädetään tarkastuksen toteuttamisesta.

Tarkastuksessa on esitettävä kaikki tarkastajan pyytämät asiakirjat, jotka ovat tarpeellisia tarkastuksen toimittamiseksi. Lisäksi tar-

kastajalle on annettava maksutta hänen pyytämänsä jäljennökset tarkastuksen toimittamiseksi tarpeellisista asiakirjoista.

Tarkastuksesta on laadittava pöytäkirja, josta on toimitettava jäljennös 30 päivän kuluessa asianosaiselle. Tarkastus katsotaan päättyneeksi, kun tarkastuspöytäkirjan jäljennös on annettu tiedoksi asianosaiselle. Sosiaali- ja terveysalan lupa- ja valvontaviraston tulee säilyttää tarkastuspöytäkirja kymmenen vuoden ajan tarkastuksen suorittamisesta lukien.

20 b §

Oikeus ulkopuolisen asiantuntijan käyttöön

Sosiaali- ja terveysalan lupa- ja valvontavirastolla on oikeus käyttää ulkopuolisia asiantuntijoita arvioimaan tietojärjestelmän vaatimustenmukaisuutta. Ulkopuoliset asiantuntijat voivat osallistua tämän lain mukaisiin tarkastuksiin sekä tutkia ja testata tietojärjestelmiä. Ulkopuolisella asiantuntijalla tulee olla tehtävien edellyttämä asiantuntemus ja pätevyys.

Ulkopuoliset asiantuntijat eivät saa luvatta ilmaista, mitä he asemansa, tehtävänsä tai työnsä vuoksi ovat saaneet tietää toisen terveydentilasta, sairaudesta tai vammaisuudesta taikka häneen kohdistuvista sosiaali- ja terveydenhuollon toimenpiteistä tai muista vastaavista seikoista. Vaitiolovelvollisuus säilyy tehtävän päättymisen jälkeen. Ulkopuoliseen asiantuntijaan sovelletaan virkamiehen esteellisyyttä koskevia hallintolain säännöksiä sekä rikosoikeudellista virkavastuuta hänen suorittaessaan tässä laissa tarkoitettuja tehtäviä.

20 c §

Poliisin virka-apu

Poliisin antamasta virka-avusta säädetään poliisilaissa (872/2011).

20 d §

Määräys velvollisuuksien täyttämiseksi

Jos sosiaali- tai terveydenhuollon tietojärjestelmän valmistaja, sosiaalihuollon tai terveydenhuollon palvelujen antaja, välityspalvelun tuottaja taikka Kansaneläkelaitos on laiminlyönyt tässä laissa säädetyn velvollisuutensa, Sosiaali- ja terveysalan lupa- ja valvontavirasto voi määrätä velvollisuuden täytettäväksi määräajassa.

20 e §

Käytössä oleviin tietojärjestelmiin kohdistuvat velvollisuudet

Sosiaali- ja terveysalan lupa- ja valvontavirasto voi antaessaan 20 d §:n nojalla tietojärjestelmää koskevan päätöksen samalla määrätä valmistajan korjaamaan tuotantokäytössä olevia tietojärjestelmiä koskevat puutteet.

Jos tietojärjestelmä voi vaarantaa tietosuojan taikka asiakas- tai potilasturvallisuuden, eikä puutteita ole korjattu Sosiaali- ja terveysalan lupa- ja valvontaviraston asettamassa määräajassa, voi lupa- ja valvontavirasto kieltää tietojärjestelmän käytön, kunnes turvallisuuden vaarantava ominaisuus on korjattu. Lisäksi Kansaneläkelaitos voi sulkea yhteyden ylläpitämiinsä terveydenhuollon valtakunnallisiin tietojärjestelmäpalveluihin, jos niihin liitetty tietojärjestelmä tai sen käyttäjäorganisaatio vaarantaa valtakunnallisten tietojärjestelmäpalvelujen asianmukaisen toiminnan.

Sosiaali- ja terveysalan lupa- ja valvontavirasto voi velvoittaa valmistajan tai valtuutetun edustajan tiedottamaan tietojärjestelmän tuotantokäyttöä koskevasta päätöksestä lupa- ja valvontaviraston asettamassa määräajassa ja määräämällä tavalla.

20 f §

Uhkasakko

Sosiaali- ja terveysalan lupa- ja valvontaviraston tämän luvun nojalla antamaa määräystä tai tekemää päätöstä voidaan tehostaa uhkasakolla. Uhkasakosta säädetään uhkasakkolaissa (1113/1990).

20 g §

Tiedonsaantioikeus

Sosiaali- ja terveysalan lupa- ja valvontavirastolla on oikeus saada maksutta ja salassa-

pitosäännösten estämättä sosiaali- ja terveydenhuollon tietojärjestelmien valvontaa varten välttämättömät tiedot valtion ja kunnan viranomaisilta sekä luonnollisilta tai oikeushenkilöiltä, joita tämän lain tai sen nojalla annetut säännökset ja päätökset sosiaali- ja terveydenhuollon tietojärjestelmistä koskevat.

20 h §

Muutoksenhaku

Sosiaali- ja terveysalan lupa- ja valvontaviraston tämän lain nojalla tekemään päätökseen saa hakea muutosta hallinto-oikeudelta siten kuin hallintolainkäyttölaissa (586/1996) säädetään. Hallinto-oikeuden päätökseen saa hakea muutosta valittamalla korkeimpaan hallinto-oikeuteen, jos korkein hallinto-oikeus myöntää valitusluvan.

Sosiaali- ja terveysalan lupa- ja valvontaviraston tekemän tarkastuksen yhteydessä annettuun päätökseen ei saa hakea muutosta valittamalla. Päätökseen saa hakea oikaisua lupa- ja valvontavirastolta 30 päivän kuluessa tarkastuksen päättymisestä. Päätökseen on liitettävä ohjeet oikaisuvaatimuksen saattamiseksi lupa- ja valvontaviraston ratkaistavaksi. Päätöksen mukaisiin toimenpiteisiin on ryhdyttävä oikaisuvaatimuksesta huolimatta. Sosiaali- ja terveysalan lupa- ja valvontaviraston oikaisuvaatimuksen johdosta antamaan päätökseen saa hakea muutosta valittamalla siten kuin 1 momentissa säädetään.

Sosiaali- ja terveysalan lupa- ja valvontaviraston tämän lain nojalla tekemää päätöstä tai määräystä on muutoksenhausta huolimatta noudatettava, jollei muutoksenhakuviranomainen toisin määrää.

22 §

Maksut

Kansaneläkelaitoksen ja Väestörekisterikeskuksen hoitamien 14 §:ssä tarkoitettujen valtakunnallisten tietojärjestelmäpalvelujen käyttö on palvelujen antajille maksullista. Kunnallisen sosiaali- ja terveydenhuollon maksut peritään sairaanhoitopiireittäin sairaanhoitopiirin kuntayhtymältä. Kansaneläkelaitoksen perimät maksut säädetään valtion maksuperustelain (150/1992) 10 §:n estämättä sosiaali- ja terveysministeriön asetuksella sellaisiksi, että ne vastaavat palvelujen hoidosta aiheutuvien kustannusten määrää. Maksujen tulee lisäksi turvata Kansaneläkelaitoksen palvelurahaston maksuvalmius. Väestörekisterikeskuksen suoritteista perittävistä maksuista säädetään valtion maksuperustelaissa ja sen nojalla.

Kansaneläkelaitoksen ja Väestörekisterikeskuksen tulee toimittaa vuosittain sosiaali- ja terveysministeriölle selvitys edellisen vuoden kustannuksista ja kustannuksiin vaikuttaneista tekijöistä sekä arvio seuraavan vuoden käyttömaksujen perustana olevista kokonaiskustannuksista.

Tietojärjestelmän valmistaja vastaa vaatimustenmukaisuuden osoittamisen aiheuttamista kustannuksista. Kansaneläkelaitoksella on oikeus periä maksu 19 e §:ssä tarkoitetusta yhteistestauksesta valtion maksuperustelain 6 §:n 1 momentissa tarkoitetun omakustannusarvon mukaisesti. Sosiaali- ja terveysalan lupa- ja valvontavirastolle tämän lain 19 f §:n mukaan tehtävän ilmoituksen rekisteröinti ja merkintä julkiseen rekisteriin on maksullinen. Maksusta säädetään sosiaali- ja terveysministeriön asetuksella ottaen huomioon, mitä valtion maksuperustelaissa ja sen nojalla maksuista säädetään. Tietoturvallisuuden arviointilaitoksen hyväksymisestä perittävistä maksuista säädetään tietoturvallisuuden arviointilaitoksista annetun lain 11 §:ssä.

Tämä laki tulee voimaan 1 päivänä huhtikuuta 2014.

Ennen lain voimaantuloa voidaan ryhtyä lain täytäntöönpanon edellyttämiin toimiin.

Luokan A tietojärjestelmällä on oltava tämän lain mukainen vaatimustenmukaisuustodistus viimeistään 1 päivänä tammikuuta 2015. Ennen mainittua ajankohtaa tietojärjestelmä, jolla ei ole vaatimustenmukaisuustodistusta, voidaan liittää valtakunnallisiin tietojärjestelmäpalveluihin Kansaneläkelaitoksen päätöksellä enintään kahden vuoden ajaksi. Jos luokan A tietojärjestelmä on liitetty valtakunnallisiin tietojärjestelmäpalveluihin ennen tämän lain voimaantuloa, saa tietojärjestelmää käyttää ilman vaatimusten-

mukaisuustodistusta liittymisen yhteydessä todetun määräajan loppuun saakka. Jos määräaika päättyy vuoden 2014 aikana, tietojärjestelmää saa kuitenkin käyttää Kansaneläkelaitoksen antaman päätöksen perusteella enintään 2 vuoden ajan.

Luokkaan B kuuluvan tietojärjestelmän on täytettävä 19 a §:ssä säädetyt olennaiset vaatimukset, jos se otetaan käyttöön 1 päivänä tammikuuta 2017 tai sen jälkeen. Sitä ennen käyttöön otettu luokan B tietojärjestelmä on saatettava vastaamaan olennaisia vaatimuksia, jos tietojärjestelmää muutetaan olennaisesti ja muutettu tietojärjestelmä otetaan käyttöön 1 päivänä tammikuuta 2017 tai sen jälkeen. Jos ennen tämän lain voimaantuloa tehty luokan B tietojärjestelmää koskeva palvelusopimus päättyy 1 päivänä tammikuuta 2017 tai sen jälkeen, on tietojärjestelmä kuitenkin muutettava vastaamaan olennaisia vaatimuksia palvelusopimuksen päättymisestä lukien.

Kansaneläkelaitos toteuttaa 14 §:n 1 momentissa tarkoitetun palvelun, jolla valtakunnallisia tietojärjestelmäpalveluja voi käyttää Internetin välityksellä sekä tietoliikenneverkkoja käyttäen 1 päivään tammikuuta 2017 mennessä.

Lain 19 h §:n mukainen omavalvontasuunnitelma tulee olla:

1) Kansaneläkelaitoksella, palvelujen antajalla ja välityspalvelun tuottajalla, joka on liittynyt valtakunnallisiin tietojärjestelmäpalveluihin tämän lain voimaan tullessa, viimeistään 1 päivänä tammikuuta 2015;

2) terveydenhuollon valtakunnallisiin tietojärjestelmäpalveluihin tämän lain voimaantulon jälkeen liittyvällä liittymisestä lukien; jos liittyminen tapahtuu 1 päivään tammikuuta 2015 mennessä, suunnitelman on kuitenkin oltava viimeistään mainittuna ajankohtana; sekä

3) muilla sosiaalihuollon ja terveydenhuollon tietojärjestelmiä käyttävillä palvelujen antajilla viimeistään 1 päivänä huhtikuuta 2015.

Sosiaali- ja terveysalan lupa- ja valvontavirastolla tulee olla 19 f §:n 2 momentissa tarkoitettu julkinen rekisteri sosiaali- ja terveydenhuollon tietojärjestelmistä viimeistään 31 päivänä joulukuuta 2016.

Helsingissä 28 päivänä maaliskuuta 2014

Tasavallan Presidentti

SAULI NIINISTÖ

Peruspalveluministeri *Susanna Huovinen*

JULKAISIJA: OIKEUSMINISTERIÖ EDITA PRIMA OY / EDITA PUBLISHING OY ISSN 1455-8904 / 1237-3419 (painettu)