Määräys A-luokkaan kuuluvien sosiaali- ja terveydenhuollon tietojärjestelmien olennaisista tietoturvavaatimuksista

Valtuutussäännökset

Sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetun lain (159/2007) 19 a § - 19 g §, sellaisena kuin ne ovat 1.4.2014 voimaan tulleessa lakimuutoksessa[1].

Kohderyhmät

Sosiaalihuollon asiakastietojärjestelmien valmistajat
Terveydenhuollon potilastietojärjestelmien valmistajat
Apteekkien tietojärjestelmien valmistajat
Sosiaali- ja terveydenhuollon tietojärjestelmäpalvelujen tuottajat
Kanta-välityspalveluiden tuottajat
Sosiaalihuollon palvelujen antajat
Terveydenhuollon palvelujen antajat
Apteekit
Kansaneläkelaitos

Voimassaoloaika

Määräys tulee voimaan 1. päivänä helmikuuta 2015 ja se on voimassa toistaiseksi.

[1]Laki asiakastietojen sähköisestä käsittelystä http://www.finlex.fi/fi/laki/ajantasa/2007/20070159

Sisällys

1. Määräyksen soveltamisala

Määräys koskee sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetussa laissa (159/2007)[2] säädettyjä tietojärjestelmien olennaisten vaatimusten sisältöä (19 a §).

Tämä määräys koskee Kanta-palveluihin liittyviä järjestelmiä ja Kanta-välityspalveluita, jotka kuuluvat käyttötarkoituksensa ja ominaisuuksiensa perusteella asiakastietolain 19 b § mukaiseen luokkaan A. Määräys liitteineen sisältää sosiaali- ja terveydenhuollon asiakas- ja potilastietojen käsittelyssä käytettävien tietojärjestelmien olennaiset **tietoturvavaatimukset**. Tietoturvavaatimusten täyttyminen on todennettava auditoinnilla, joka kohdistuu tietojärjestelmään tai tietojärjestelmäpalveluun ja jonka suorittaa hyväksytty tietoturvallisuuden arviointilaitos.

Vaatimukset koskevat esimerkiksi apteekki- ja potilastietojärjestelmiä, niiden osajärjestelmiä tai niissä käytettäviä tietojärjestelmäpalveluita tuotteena luokan A kriteerien täyttyessä. Vaatimukset koskevat myös Kanta-välityspalveluita sekä sellaisia verkkopalveluita ja sosiaalihuollon asiakastietojärjestelmiä, jotka täyttävät luokkaan A kuulumisen kriteerit. Siltä osin kuin tietojärjestelmän valmistaja tai tietojärjestelmäpalvelun tuottaja vastaa tietojärjestelmän tai jonkin tietojärjestelmän moduulin käyttöympäristöstä on sertifioinnissa todennettava myös tietojärjestelmän käyttöympäristöä koskevat vaatimukset.

Vaatimustenmukaisuuden osoittamisesta ja tietojärjestelmän luokittelusta vastaa (asiakastietolaki 19 c ja d §) tietojärjestelmän valmistajana tai tietojärjestelmäpalvelun tuottajana toimiva taho.

2. Määritelmät

Tässä määräyksessä tarkoitetaan:

- **Asiakastietolailla** ajantasaista sosiaali- ja terveydenhuollon asiakastietojen sähköi-sestä käsittelystä annettua lakia (159/2007);
- **Auditoinnilla** sertifiointiprosessin osaa, jossa hyväksytty arviointilaitos suorittaa vaatimusten osa-alueen (kuten tietoturvavaatimukset) läpikäynnin tuottaen auditointiraportin ja auditointitodistuksen;
- **Lääkemääräyslailla** ajantasaista sähköisestä lääkemääräyksestä annettua lakia (61/2007)[3];
- **Kanta-palveluilla** ja **valtakunnallisilla tietojärjestelmäpalveluilla** sähköisen lääkemääräyksen, Reseptikeskuksen, Lääketietokannan, Potilastiedon arkiston ja tiedonhallintapalvelun sekä Omakanta-palvelun muodostamaa kokonaisuutta;

[2] Laki asiakastietojen sähköisestä käsittelystä http://www.finlex.fi/fi/laki/ajantasa/2007/20070159
[3] Laki sähköisestä lääkemääräyksestä https://www.finlex.fi/fi/laki/ajantasa/2007/20070061

- **Kanta-välityspalvelulla** terveydenhuollon organisaation tai apteekin Kanta-palveluihin liittymisessä hyödyntämää palvelua, jonka tuottajalla on tässä roolissa mahdollisuus nähdä salaamattomia potilas- tai asiakastietoja esimerkiksi ylläpito-toimien yhteydessä;
- **Kanta-välityspalveluiden tuottajalla** edellä kuvatun välityspalvelun tuottajaa;
- **Käyttöympäristöllä** teknistä, organisatorista ja fyysistä ympäristöä, jossa yksi tai useampi palvelun antaja käyttää tietojärjestelmää tai tietojärjestelmäpalvelua sosiaali- ja terveydenhuollon palvelujen tuottamisessa ja todellisten asiakas- tai potilastietojen käsittelyssä;
    - käyttöympäristö sisältää mm. päätelaitteet, palvelimet, työasemat, käyttö-järjestelmä- ja varusohjelmistot sekä hallinta- ja tietoturvakäytännöt, jotka eivät ole osa tietojärjestelmää tai tietojärjestelmäpalvelua;
- **Palvelun antajalla**
    - terveydenhuollon toimintayksikköä (potilaslaki 785/1992 2 §:n 4 mom)[4]
    - työantajaa (työterveyshuoltolaki 1383/2001 7 §:n 2 mom.)[5]
    - itsenäisenä ammatinharjoittajana toimivaa terveydenhuollon ammattihenki-löä (asiakastietolaki 3 §, 28.3.2014/250)
    - apteekkia;
- **Sertifioinnilla** vaatimustenmukaisuuden osoittamisen prosessia, jonka tuloksena täytetään ne edellytykset, joilla tietojärjestelmä tai tietojärjestelmäpalvelu voi saada vaatimustenmukaisuustodistuksen ja merkinnän valvontaviranomaisen rekisteriin vaatimukset täyttävästä tietojärjestelmästä tai tietojärjestelmäpalvelusta
    - luokkaan A kuuluvilta tietojärjestelmiltä tai tietojärjestelmäpalveluilta edelly-tetään selvitystä toiminnallisuutta koskevien vaatimusten täyttämisestä, hy-väksyttyä Kansaneläkelaitoksen yhteistestausta ja pakollisten tietoturvalli-suuden vaatimusten täyttämisen auditointia;
- **Tietojärjestelmällä** ohjelmistoa (mukaan lukien dokumentaatio, asennus- ja konfi-gurointiohjeet sekä ohjelmiston osat kuten asiakas- tai palvelinohjelmistot, sovel-luspalvelut tai sovelluspalvelimet ja tietokannat), jonka käyttötarkoituksena on asiakas- ja potilastietojen käsittely
    - tämä määräys koskee erityisesti luokkaan A kuuluvia tietojärjestelmiä riippu-matta siitä onko ohjelmistolla myös muita käyttötarkoituksia
- **Tietojärjestelmäpalvelulla** palvelua, jonka kautta palvelujen antaja käsittelee asiakas- ja potilastietoja, riippumatta siitä onko palveluun kuuluvat ohjelmistot asennettu kokonaan tai osittan palvelujen antajan tai tietojärjestelmäpalvelun tuottajan hallitsemaan käyttöympäristöön;
- **Tietojärjestelmän valmistajalla** tahoa, joka on vastuussa sosiaali- ja tervey-denhuollon tietojärjestelmän suunnittelusta ja valmistuksesta, riippumatta siitä toimiiko tämä taho myös tietojärjestelmäpalvelun tuottajana;
- **Tietojärjestelmäpalvelun tuottajalla** tahoa, joka tarjoaa palvelun antajalle tietojärjestelmäpalvelua, jossa käsitellään asiakas- ja potilastietoja; tietojärjestel-

[4] Laki potilaan asemasta ja oikeuksista https://www.finlex.fi/fi/laki/ajantasa/1992/19920785
[5] Työterveyshuoltolaki https://www.finlex.fi/fi/laki/ajantasa/2001/20011383

mäpalvelun tuottaja vastaa tietojärjestelmän valmistajalle asetettuihin vaatimuksiin valmistajana, valmistajan lukuun tai valmistajan puolesta;
- **Todentamisella** menettelyä, jolla osoitetaan, että järjestelmä täyttää sille asetetun vaatimuksen. Todentamistapoja ovat mm. dokumentaation läpikäynti, ohjelmiston toiminnallinen testaus, ohjelmiston valmistajan tai tietojärjestelmäpalvelujen tuottajan dokumentoitu haastattelu ja tietojärjestelmän tuottamien sanomien, lokien tai muiden tuotosten läpikäynti;
- **Vaatimustenmukaisuustodistuksella** hyväksytyn auditointilaitoksen antamaa todistusta siitä, että tietojärjestelmä tai tietojärjestelmäpalvelu on hyväksytysti läpäissyt sertifioinnin.

3. Suhde muihin määräyksiin, ohjeisiin ja määrityksiin

Tämä määräys koskee sosiaali- ja terveydenhuollon asiakas- ja potilastietojen käsittelyssä käytettävien tietojärjestelmien olennaisia vaatimuksia tietoturvavaatimusten osalta. Toiminnallisten ja muiden olennaisten vaatimusten osalta annetaan erillinen määräys.

Tietojärjestelmien toteutuksessa on kuitenkin lisäksi soveltuvin osin noudatettava sähköisen lääkemääräyksen[6] ja Potilastiedon arkiston sekä tiedonhallintapalvelun kanta.fi-verkkosivuilla[7] julkaistuja määrittelyjä, joiden toteuttaminen tietojärjestelmissä todennetaan Kelan yhteistestauksella[8].

Tämän määräyksen lisäksi annetaan määräys omavalvontasuunnitelmasta, jonka mukaisesti palvelujen antajan on kuvattava tietoturvaan ja tietosuojaan sekä tietojärjestelmien käyttöön liittyvät asiat. Osana omavalvontasuunnitelmaa on kuvattava se, kuinka palvelujen antaja varmistuu siitä, että käytettävät tietojärjestelmät ja tietojärjestelmäpalvelut täyttävät tämän määräyksen mukaiset vaatimukset.

Tämän määräyksen lisäksi järjestelmien toteutuksessa on otettava huomioon muuhun lainsäädäntöön kirjatut kyseisiin tietojärjestelmiin kohdennetut vaatimukset.

4. Yleistä

Asiakastietolain 19 a §:n mukaisesti sosiaali- ja terveydenhuollon asiakastietojen käsittelyssä käytettävän tietojärjestelmän tulee täyttää yhteentoimivuutta, tietoturvaa ja tietosuojaa sekä toiminnallisuutta koskevat olennaiset vaatimukset. Tietoturvavaatimukset potilastietojärjestelmille, apteekkien tietojärjestelmille, tietojärjestelmien käyttöympäristöille ja Kanta-välittäjäpalveluille on koottu tämän määräyksen liitteeseen 1.

[6] Sähköisen reseptin määrittelyt http://kanta.fi/fi/web/ammattilaisille/sahkoisen-reseptin-maarittelyt
[7] Määrittelyt Potilastiedon arkistolle http://kanta.fi/fi/web/ammattilaisille/potilastiedon-arkiston-maarittely
[8] Testaus http://kanta.fi/fi/web/ammattilaisille/testaus

Ennen tämän määräyksen antamista Terveyden ja hyvinvoinnin laitos on asiakastietolain 19 a §:n 3 momentin mukaisesti kuullut sosiaali- ja terveydenhuollon sähköisen tietohallinnon neuvottelukuntaa. Määräysluonnoksen sisällöstä on järjestetty lausuntokierros, jolla saadut kommentit on otettu huomioon lopullisessa määräyksessä.

Eri vaatimusten todentamisessa käytetään Viestintäviraston ohjeiden mukaisia hallinnollisia ja soveltuvin osin myös teknisiä todentamistapoja.

Liitteen 1 vaatimusten kohdassa ”Vaatimus / kontrolli” esitettävät vaatimukset ovat sitovia vaatimuksia, joiden toteutumisen perusteella kunkin vaatimuksen toteutuminen on todennettava. Kohdassa ”todentaminen / auditointi” esitetään suositus kunkin vaatimuksen todentamistavaksi. Vaatimusten kohdeluokittelusta ja tarkasteltavan tietojärjestelmän tai tietojärjestelmäpalvelun tyypistä riippumatta on vastattava kaikkiin niihin vaatimuksiin, jotka ovat sovellettavissa kyseisessä tietojärjestelmässä tai tietojärjestelmäpalvelussa.

Kunkin vaatimuksen osalta on kuvattava sertifiointia ja mahdollista auditointia varten tai sen yhteydessä seuraavat asiat:

- vaatimuksen täyttyminen, jokin seuraavista vaihtoehdoista
  - vaatimus täyttyy täysin
  - vaatimus täyttyy osittain ja täyttymättä jäävä osa kompensoidaan; kompensointitapa kuvattava
  - vaatimus ei täyty
- mikäli vaatimus ei ole relevantti tai on vain osin relevantti arvioitavan tietojärjestelmäpalvelun osalta, mainita tästä perusteluineen
- auditoinnin osalta todentamistapa ja tieto siitä, kuinka vaatimuksen täyttyminen on todettu, esimerkiksi viite dokumentaatioon, testausraporttiin tai ohjelmiston tuotokseen.

Auditoinnin ja yhteistestauksen perusteella auditoidusta järjestelmästä syntyy vaatimustenmukaisuuden tarkastusraportti. Hyväksytysti yhteistestauksen ja auditoinnin läpäissyt tietojärjestelmä tai tietojärjestelmäpalvelu saa vaatimustenmukaisuustodistuksen. A-luokkaan kuuluvan tietojärjestelmän valmistajan, tietojärjestelmäpalvelun tuottajan tai välityspalvelun tuottajan tulee toimittaa Valviralle ilmoitus käyttöönotettavissa olevasta tietojärjestelmästä, jonka liitteenä on vaatimustenmukaisuustodistus. Ilmoituksen sisällössä on oltava vähintään ilmoitukselta edellytettävät pakolliset tiedot. Ilmoitus ja vaatimustenmukaisuustodistus on toimitettava ennen kuin tietojärjestelmä otetaan tuotantokäyttöön käyttöympäristössä.

Vaatimustenmukaisuustodistuksen saaneen tietojärjestelmien olennaisista muutoksista on toimitettava ilmoitus tietoturvallisuuden arviointilaitokselle. Olennaiset muutokset ovat muutoksia, jotka muuttavat tietojärjestelmän toimintaa suhteessa määräyksen liitteenä olevien olennaisten vaatimusten toteutumiseen. Tietojärjestelmän

uudesta versiosta on mahdollista toimittaa ilmoitus myös silloin, kun uuden version muutokset eivät muuta tietojärjestelmän toimintaa suhteessa olennaisiin vaatimuksiin. Ilmoituksesta riippumatta tietojärjestelmäpalvelun tuottaja vastaa siitä, että uusi versio täyttää olennaiset vaatimukset vähintään samalla tasolla kuin aiempi versio. Merkittävät ja laajavaikutteiset muutokset tietojärjestelmässä edellyttävät vaatimustenmukai-suustodistuksen uudistamista.

Myöhemmin annettavilla määräyksillä voidaan korvata tämä määräys. Määräyksen liitteitä ja niiden sisältämiä vaatimuksia voidaan muuttaa itse määräystä muuttamatta erikseen ilmoitettavina ajankohtina. Muutokset voivat olla tarkennuksia esitettyjen vaatimuksien sisällössä tai todentamisessa. Useissa vaatimuksissa siirrytään tulevaisuudessa vähitellen dokumentointi- ja haastattelukäytännöistä testaukseen ja tekniseen todentamiseen. Merkittäviä muutoksia ja vaikutuksia aiheuttavista uusista vaatimuksista annetaan uusi määräys.

Olennaisten vaatimusten muuttuessa voidaan edellyttää tietojärjestelmän tai tietojärjestelmäpalvelun vaatimustenmukaisuustodistuksen uudistamista. Olennaisten vaatimusten muuttamisen yhteydessä määritellään se, vaaditaanko kaikilta tietojärjestelmiltä ja tietojärjestelmäpalveluilta vaatimustenmukaisuustodistuksen uudistamista, ja mihin mennessä tai minkä ajan kuluttua vaatimusten voimaantulosta tai aiemman vaatimustenmukaisuustodistuksen saannista uutta vaatimustenmukaisuustodistusta edellytetään.

5. Ohjaus ja neuvonta

Lisätietoja sertifiointiprosessista ja sen toimijoista löytyy Kanta.fi-verkkosivustolta[9].

Terveyden ja hyvinvoinnin laitoksen operatiivisen toiminnan ohjaus -yksikkö ohjaa ja neuvoo pyynnöstä tämän määräyksen soveltamisessa.

6. Voimaantulo

Tämä määräys tulee voimaan 1.2.2015 ja on voimassa toistaiseksi.

Määräyksen mukaisten vaatimusten täyttämistä ja tämän osoittavaa sertifiointia ja vaatimustenmukaisuustodistusta, mukaan lukien tietoturva-auditointi, edellytetään kaikilta luokkaan A kuuluvilta tietojärjestelmiltä määräyksen voimaantulon jälkeen. Jos tietojärjestelmälle on suoritettu aiempi hyväksytty auditointi ennen tämän määräyksen voimaantuloa, on vaatimustenmukaisuustodistus saatava ennen kuin aiempi auditointi vanhentuu. Mikäli aiempi sertifiointi tai auditointi vanhentuu alle 6 kk kuluessa

[9] Kanta – Sertifiointi http://www.kanta.fi/fi/web/ammattilaisille/sertifiointi

määräyksen voimaantulosta, on määräyksen mukainen sertifiointi toteutettava 6 kk kuluessa määräyksen voimaantulosta. Mikäli järjestelmä on määräyksen voimaan tullessa Kelan Kanta-palvelujen yhteistestauksessa, on sertifiointi toteutettava ennen kuin ensimmäinen tietojärjestelmää käyttävä palvelun antaja liittyy kyseiseen Kanta-palveluun.

Tietojohtaja Pekka Kahri

Yksikönpäällikkö Vesa Jormanainen

Jakelu

Sosiaalihuollon asiakastietojärjestelmien valmistajat
Terveydenhuollon potilastietojärjestelmien valmistajat
Apteekkien tietojärjestelmien valmistajat
Sosiaalihuollon ja terveydenhuollon palvelujen antajat
Kanta-välityspalveluiden tuottajat
Apteekit
Kansaneläkelaitos
Sosiaali- ja terveysministeriö
Valtiovarainministeriö
Väestörekisterikeskus
Sosiaali- ja terveydenhuollon lupa- ja valvontavirasto
Lääkealan turvallisuus- ja kehittämiskeskus
Viestintävirasto
Aluehallintovirastot
THL / Tietopalvelut-osasto
THL pääjohtaja
Suomen Kuntaliitto ry
Suomen Apteekkariliitto ry
Suomen Lääkäriliitto ry
Suomen Hammaslääkäriliitto ry
Lääkäripalveluyritykset ry
Terveyspalvelualan Liitto ry
Tietosuojavaltuutetun toimisto

Liite 1. Tietoturvavaatimukset A-luokkaan kuuluville järjestelmille ja järjestelmien käyttöympäristöille