Tiedonvälittäjät
Tieto ja tiedonhallinnan ohjaus 3.5.2024

MÄÄRÄYS SOSIAALI- JA TERVEYDENHUOLLON TIETOJÄRJESTELMIEN JA HYVINVOINTISOVELLUSTEN OLENNAISISTA VAATIMUKSISTA

Valtuutussäännökset

Laki sosiaali- ja terveydenhuollon asiakastietojen käsittelystä (703/2023) 10 § 4 momentti, 20 § 2 momentti, 79 § 4 momentti, 82 § 4 momentti, 84 § 4 momentti, 85 § 3 momentti

Kohderyhmät

Sosiaali- ja terveydenhuollon tietojärjestelmäpalvelujen tuottajat ja tietojärjestelmien valmistajat
Hyvinvointisovellusten valmistajat
Kanta-välityspalvelujen tuottajat
Sosiaali- ja terveydenhuollon palvelunantajat
Apteekit
Kansaneläkelaitos
Tietoturvallisuuden arviointilaitokset
Välittäjät

Voimaantulo

Määräys tulee voimaan 10. päivänä toukokuuta 2024 ja se on voimassa toistaiseksi.

Tämä määräys korvaa aiemmat THL:n määräykset 5/2021 (määräys sosiaali- ja terveydenhuollon tietojärjestelmien olennaisista toiminnallisista ja tietoturvavaatimuksista) ja 6/2021 (määräys omatietovarantoon liittyvien hyvinvointisovellusten sertifioinnista ja olennaisista vaatimuksista). Laki sosiaali- ja terveydenhuollon asiakastietojen käsittelystä (703/2023) kumoaa aiemman määräyksen antamiseen valtuuttaneen lain sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (784/2021), jonka nojalla annetut alemman asteiset säädökset kumoutuvat.

Sisällys

1 Määräyksen tarkoitus

Tämän määräyksen tarkoitus on täsmentää sosiaali- ja terveydenhuollon asiakas- ja potilastietojen käsittelyyn tarkoitettuihin tietojärjestelmiin kohdistuvat olennaiset vaatimukset, jotta niiden tarkoituksenmukainen toiminta, yhteensopivuus ja tietoturvallisuus voidaan varmistaa. Lisäksi määräyksen tarkoituksena on täsmentää hyvinvointisovelluksiin kohdistuvat olennaiset vaatimukset.

2 Määräyksen soveltamisala

Tässä määräyksessä käytettävät termit ja määritelmät ovat THL:n määräyksen 4/2024 (luku 2) mukaisia.

Tämä määräys koskee sosiaali- ja terveydenhuollon asiakas- tai potilastietoja käsittelevien tietojärjestelmien sekä hyvinvointisovellusten olennaisten vaatimusten sisältöä (laki sosiaali- ja terveydenhuollon asiakastietojen käsittelystä (703/2023), jäljempänä asiakastietolaki, luku 12 "Tietojärjestelmien ja hyvinvointisovellusten olennaiset vaatimukset"). Terveyden ja hyvinvoinnin laitoksella (jäljempänä THL) on asiakastietolain 84 §:n perusteella valtuus antaa tarkempia määräyksiä olennaisten vaatimusten sisällöstä ja siitä, mitkä olennaiset vaatimukset on täytettävä eri palveluissa käytettävissä järjestelmissä. Lisäksi THL:lla on asiakastietolain 85 §:n perusteella valtuus antaa määräyksiä valtuus antaa määräyksiä vaatimustenmukaisuuden osoittamisessa noudatettavista menettelyistä ja annettavan selvityksen sisällöstä.

Tämä määräys koskee:

- valtakunnallisiin tietojärjestelmäpalveluihin (Kanta-palvelut) liitettäviksi tarkoitettuja asiakas- ja potilastietoja käsitteleviä järjestelmiä ja muita käyttötarkoituksensa perusteella sertifioitavia tietojärjestelmiä (luokka A);
- muita sosiaali- ja terveydenhuollon järjestelmiä, joiden käyttötarkoituksena on asiakas- ja potilastietojen käsittely (luokka B);
- hyvinvointisovelluksia, jotka on tarkoitettu liitettäväksi omatietovarantoon ja joilla käsitellään hyvinvointitietoa (luokka A) sekä
- hyvinvointisovelluksia, joihin henkilö voi saada asiakastietonsa valtakunnallisesta asiakastietovarannosta, reseptikeskuksesta tai tiedonhallintapalvelusta (luokka A).

Määräyksen mukaisten olennaisten vaatimusten käyttökohteita ovat:

- asiakas- tai potilastietoja käsittelevien järjestelmien, osajärjestelmien tai hyvinvointisovellusten käyttötarkoituksen kuvaaminen;
- kansallisesti asetettavien vaatimusten kokoaminen sekä vaatimuksia tarkemmin kuvaavien määritysten kokoaminen ja niihin viittaaminen;
- Kanta-palveluihin liittyvissä luokan A2 ja A3 järjestelmissä ja hyvinvointisovelluksissa Kelan Kanta-palvelujen yhteistestauksessa ja sen eri testauskokonaisuuksissa läpikäytävien vaatimusten selkeyttäminen;
- luokan A2 ja A3 tietojärjestelmien valmistajien ja tietojärjestelmäpalvelujen tuottajien omassa testauksessa, Kelan yhteistestauksessa sekä mahdollisissa asiakastestauksissa testattavien järjestelmäominaisuuksien ryhmittely;
- luokan A tietoturvallisuuden arvioinnissa läpikäytävien tietoturvavaatimusten kuvaaminen tietoturvallisuuden arviointeja varten;
- samoihin toiminnallisiin tai sisällöllisiin kokonaisuuksiin liittyvien vaatimusten ja määritysten ryhmittely ja linkittäminen;
- eri ajankohtina voimassa olevien kansallisten määritysten kokoaminen tietyn toiminnon tai tietosisällön toteuttamiseksi;
- tiettyyn käyttötarkoitukseen suunniteltujen järjestelmien ja hyvinvointisovellusten pakollisten vaatimusten ilmaiseminen profiilien avulla;

- pakollisten vaatimusten aikataulujen ja siirtymäaikojen määrääminen ja kokoaminen (esimerkiksi asiakastietolaissa asetettujen siirtymäaikojen ja tiettynä vuonna voimassa olevien määritysten ja olennaisten vaatimusten suhteen);
- tuki kansallisesti asetettavien olennaisten vaatimusten kuvaamiseen ja huomiointiin järjestelmien suunnittelussa ja toteuttamisessa sekä järjestelmien hankinnoissa;
- järjestelmäkokonaisuuksissa ja modulaarisissa järjestelmissä eri osajärjestelmien sisältämien ominaisuuksien kuvaaminen;
- käytettävän käsitteistön ja vaatimusten yhdenmukaistaminen järjestelmien ja hyvinvointisovellusten valmistajiin, tietojärjestelmäpalvelujen tuottajiin ja niiden käyttäjiin kohdistuvissa vaatimuksissa, jotka perustuvat säädöksiin ja valtakunnallisiin määrityksiin.

3 Määräyksen keskeinen sisältö ja rajaukset

Asiakastietolain mukaan asiakas- tai potilastietojen käsittelyssä käytettävän järjestelmän sekä hyvinvointisovelluksen tulee täyttää yhteentoimivuutta, tietoturvaa ja tietosuojaa sekä toiminnallisuutta koskevat olennaiset vaatimukset. Näiden lisäksi hyvinvointisovellusten tulee täyttää saavutettavuusvaatimukset. Vaatimusten täyttämisestä järjestelmässä vastaa tietojärjestelmäpalvelun tuottaja tai tietojärjestelmän valmistaja ja hyvinvointisovelluksessa hyvinvointisovelluksen valmistaja.

Asiakastietolaissa säädetään myös siitä, että palvelunantajan käyttämien järjestelmien on vastattava käyttötarkoitukseltaan palvelunantajan toimintaa ja täytettävä palvelunantajan toimintaan liittyvät olennaiset vaatimukset. Tämä määräys täsmentää sitä, miten palvelunantajan käyttämissä järjestelmissä olennaisten vaatimusten täyttäminen varmistetaan.

Asiakastietolain sosiaali- ja terveydenhuollon tietojärjestelmän valmistajan tai tietojärjestelmäpalvelun tuottajan sekä hyvinvointisovelluksen valmistajan on osoitettava järjestelmän, palvelun tai hyvinvointisovelluksen vaatimustenmukaisuus. Osoittamiseen kuuluu asiakastietolain 80 §:n ja 85 §:n mukaan selvitys siitä, että järjestelmä tai hyvinvointisovellus täyttää ne olennaiset vaatimukset, jotka vastaavat sen käyttötarkoitusta. Selvitys annetaan määräyksen 4/2024 ja tämän määräyksen mukaisesti.

Tämän määräyksen liitteenä on kansallisesti yhdenmukainen sosiaali- ja terveydenhuollon järjestelmien ja hyvinvointisovellusten olennaisten vaatimusten luettelo (liite 2). Luettelo sisältää sosiaali- ja terveydenhuollon asiakas- ja potilastietojen käsittelyssä käytettävien järjestelmien sekä hyvinvointisovellusten olennaisten vaatimusten ylätason kuvaukset. Määräyksessä myös täsmennetään se, mitkä olennaiset vaatimukset eri käyttötarkoituksiin tarkoitetuissa järjestelmissä tai hyvinvointisovelluksissa tulee vähintään toteuttaa tai täyttää (liitteet 3, profiilit). Lisäksi tässä määräyksessä tarkennetaan olennaisten vaatimusten kuvaamisessa, todentamisessa ja hyödyntämisessä käytettävät menettelyt.

Määräys koskee sekä Kanta-palveluihin liittyviä että muita asiakas- ja potilastietojen käsittelyyn tarkoitettuja järjestelmiä, jotka kuuluvat luokkaan A tai luokkaan B sekä luokkaan A kuuluvia hyvinvointisovelluksia. Useat vaatimuksista ja niiden perusteena olevista määrityksistä koskevat Kanta-palveluihin liittyviä luokkaan A2 tai A3 (ks. määräys 4/2024) kuuluvia järjestelmiä tai hyvinvointisovelluksia.

Määräyksessä käytetyt termit ja rajaukset vastaavat THL:n määräyksessä 4/2024 käytettäviä termejä ja rajauksia.

Määräyksen ja sen liitteiden valmisteluun on osallistunut Terveyden ja hyvinvoinnin laitoksen (THL), Kansaneläkelaitoksen (Kela), Sosiaali- ja terveysalan lupa- ja valvontaviraston (Valvira), Sosiaali- ja terveysministeriön (STM), Liikenne- ja viestintäviraston (Traficom Kyberturvallisuuskeskus) sekä sosiaali- ja terveydenhuollon palvelunantajien kehittämisprojektien asiantuntijoita. Määräyksessä on huomioitu aiempien säädösten soveltamisessa tunnistettuja kehittämistarpeita. Tietojärjestelmille ja palvelunantajille asetettavat vaatimukset ovat pääosin vastaavia kuin aiemmissa määräyksissä.

Ennen tämän määräyksen antamista THL järjesti lausuntokierroksen kuullakseen asianomaisia sidosryhmiä. Lausuntopalaute on huomioitu soveltuvin osin määräyksessä ja sen liitteissä. Lisätietoja määräyksen valmistelusta on liitteen 1 luvussa 7.

4 Suhde muihin säädöksiin, ohjeisiin ja määrityksiin

THL on antanut määräyksen sosiaali- ja terveydenhuollon tietojärjestelmien sekä hyvinvointisovellusten luokittelusta ja sertifioinnista (4/2024). Tämä määräys täsmentää määräyksessä 4/2024 kuvatuilla menettelyillä todennettavat vaatimukset ja vaatimustenmukaisuuden ilmoittamisessa ja todentamisessa käytettävät menettelyt.

Tämän määräyksen liitteessä 2 oleva olennaisten vaatimusten luettelo viittaa useisiin tarkempiin määrityksiin ja ohjeisiin, joissa kuvataan yksityiskohtaisia toiminnallisia ja tietosisältöihin kohdistuvia vaatimuksia. Luettelo on tarkoitettu selkeyttämään ja tukemaan järjestelmien ja sovellusten kehittämistä, sertifiointia, testausta, tietoturvallisuuden arviointia, hankintaa ja eri osapuolten välistä viestintää. Määräyksen soveltamisessa luettelo toimii myös hakemistona, jonka kautta keskeisimmät kansallisia vaatimuksia kuvaavat määritykset ovat löydettävissä.

Määräyksessä ja sen liitteissä kuvatut olennaiset vaatimukset korvaavat aiemman asiakastietolain sekä THL:n määräysten 4/2021, 5/2021 ja 6/2021 nojalla asetetut olennaiset vaatimukset. Pääosa olennaisista vaatimuksista on samoja kuin aiemmissa määräyksissä.

Määräystä ei sovelleta järjestelmiin, joiden käyttötarkoituksena ovat pelkästään Sosiaali- ja terveysalan tietolupaviranomaisen (Findata) antaman määräyksen 1/2022 (Muiden palveluntarjoajien tietoturvallisille käyttöympäristöille asetettavista vaatimuksista) mukaiset käyttökohteet. Findatan määräystä sovelletaan kaikkiin niihin toisiolaissa säädettyihin käyttötarkoituksiin, joihin toisiolain mukaan tarvitaan tietolupa: tieteellinen tutkimus, tilastointi, opetus sekä viranomaisen suunnittelu- ja selvitystehtävä.

THL on antanut erillisen määräyksen 1/2024 sosiaalihuollon asiakasasiakirjoista ja niihin merkittävistä tiedoista.

THL:n määräyksessä 3/2024 kuvataan sote-palvelunantajilta, välittäjiltä, apteekeilta sekä Kelalta edellytettävään tietoturvasuunnitelmaan sisällytettävät selvitykset ja vaatimukset. Osana tietoturvasuunnitelmaa kuvataan, kuinka tietoturvasuunnitelman kohde osaltaan varmistaa tuotantokäytössä toimivien järjestelmien ja toiminnassaan mahdollisesti käytettävien hyvinvointisovellusten vaatimustenmukaisuuden osana tietoturvasuunnitelmaa ja sen kautta tapahtuvaa omavalvontaa.

Tämän määräyksen kohdealueena eivät ole lääkinnällisten laitteiden säädökset. Määräyksen 4/2024 luvussa 4 kuvatut lääkinnällisten laitteiden säädökset on huomioitava tietojärjestelmissä ja hyvinvointisovelluksissa, jotka täyttävät lääkinnällisen laitteen määritelmän.

5 Olennaiset toiminnalliset vaatimukset

Olennaiset toiminnalliset vaatimukset koskevat järjestelmiin ja hyvinvointisovelluksiin toteutettavia toimintoja ja eri tietosisältöjen käsittelyn kyvykkyyksiä. Olennaisia toiminnallisia vaatimuksia ovat tämän määräyksen liitteessä 2 (Olennaisten vaatimusten luettelo) kuvatut toiminnot ja tietosisällöt, jotka viittaavat erillisiin tarkempiin määrityksiin. Näissä tarkemmissa määrityksissä kuvataan tarkemmin myös pakollisia ja vapaaehtoisia toimintoja ja tietoja. Olennaisia toiminnallisia vaatimuksia on luettelon välilehdillä ”Toiminnot”, ”Tietosisällöt” ja ”Digitaalisten palvelujen vaatimukset”.

Monet olennaiset toiminnalliset vaatimukset keskittyvät tässä määräyksessä niihin toiminnallisuuksiin ja tietoihin, jotka ovat keskeisiä Kanta-palveluihin suoraan tai välillisesti liittyvien järjestelmien ja hyvinvointisovellusten näkökulmasta.

6 Olennaiset tietoturvavaatimukset

Olennaiset tietoturvavaatimukset koskevat järjestelmiin ja hyvinvointisovelluksiin toteutettavia ja niiden kautta täytettäviä tietoturvallisuuden ja tietosuojan varmistamiseksi toteutettuja ominaisuuksia. Lisäksi niihin sisältyy järjestelmän, osajärjestelmän tai hyvinvointisovelluksen suunnittelussa, toteuttamisessa tai tarjoamisessa tarvittavia toimenpiteitä sekä muita hyvinvointisovellusten sertifioinnissa läpikäytäviä vaatimuksia. Olennaisia tietoturvavaatimuksia ovat tämän määräyksen liitteessä 2 (Olennaisten vaatimusten luettelo, välilehdet ”Tietoturvavaatimukset” ja ”Digitaalisten palvelujen vaatimukset”) kuvatut tietoturvavaatimukset.

Olennaisten vaatimusten luettelossa Tietoturvavaatimukset-välilehdellä kohdat ”Otsikko” ja ”Selite” kuvaavat vaatimuksen sitovan sisällön. Vaatimusten toteutuminen todennetaan osana tietoturvallisuuden arviointia luokkaan A kuuluvassa järjestelmässä ja hyvinvointisovelluksessa. Todentamisessa käytetään kullekin vaatimukselle määriteltyä todentamistapaa, jos vaatimus on järjestelmän tai hyvinvointisovelluksen käyttötarkoituksen näkökulmasta relevantti (ks. luku 10.2). Todentaminen osana sertifiointiprosessia tapahtuu määräyksen 4/2024 mukaisesti.

Osa tietojärjestelmän käyttöympäristöön kohdistuvista tietoturvavaatimuksista voi toteutua tietojärjestelmäpalvelun tuottajan vastuulla olevan järjestelmän kautta, osa käyttäjäorganisaation kautta. Yksityiskohdat riippuvat järjestelmän toteutustavasta, ja asia tulisi huomioida toimijoiden välisissä sopimuksissa sekä käyttäjäorganisaatioiden tietoturvasuunnitelmissa. Tietojärjestelmäpalvelun tuottajan on otettava kantaa siihen, mitkä järjestelmän käyttöympäristön olennaisista tietoturvavaatimuksista toteutuvat järjestelmän tai siihen liittyvien tietojärjestelmäpalvelun tuottajan palvelujen kautta, ja mitkä käyttöympäristön vaatimuksista ovat järjestelmää käyttävän palvelunantajan vastuulla (ks. luku 9). Vaatimukset, jotka sisältyvät järjestelmään tai tietojärjestelmäpalvelun tuottajan palveluun, todennetaan osana tietoturvallisuuden arviointia. Todentamisessa ja sertifioinnissa ei edellytetä palvelunantajaorganisaation osallistumista käyttöympäristöön kohdistuvien vaatimusten todentamiseksi.

Osa tämän määräyksen liitteissä olevissa tietoturvavaatimuksista viittaa vaatimusten perusteena oleviin säädöksiin, erillisiin määrityksiin tai standardeihin. Jos vaatimus perustuu suoraan tiettyyn lähdedokumenttiin, tämä mainitaan erikseen (suorat lähteet). Osa lähteistä tukee vaatimusten tulkintaa ja soveltamista.

7 Vähimmäisvaatimusten profiilit

Tiettyyn käyttötarkoitukseen tarkoitetun järjestelmän, osajärjestelmän, järjestelmäkokonaisuuden tai hyvinvointisovelluksen vähimmäisvaatimukset voidaan ilmaista kansallisen vähimmäisvaatimusprofiilin (profiili) avulla. Yksi profiili sisältää osajoukon olennaisten vaatimusten luettelossa kuvatuista olennaisista vaatimuksista. Määräyksen liitteissä 3a-3h on profiileja, jotka kokoavat useisiin eri käyttötarkoituksiin sosiaali- ja terveydenhuollon järjestelmien tai hyvinvointisovellusten kansallisesti asetettavat vähimmäisvaatimukset. Kussakin liitteessä on yksi tai useampia profiileja.

Profiilin mukaiset olennaiset vaatimukset on toteutettava tai täytettävä järjestelmässä tai hyvinvointisovelluksessa, jonka käyttötarkoitukseen sisältyy profiilissa kuvattu käyttötarkoitus. Profiilin mukaisten vähimmäisvaatimusten toteuttaminen on edellytyksenä tiettyyn käyttötarkoitukseen käytettävän järjestelmän, järjestelmäkokonaisuuden tai hyvinvointisovelluksen ottamiselle tuotantokäyttöön. Tämän määräyksen liitteenä olevat profiilit ovat velvoittavia, pois lukien profiilit 3f1 ja 3f2, jotka ovat ohjeellisia ja eivät kohdistu hyvinvointisovelluksiin eivätkä sote-palveluissa käytettäviin tietojärjestelmiin.

Tietojärjestelmäpalvelun tuottajan tai hyvinvointisovelluksen valmistajan on ilmoitettava kaikki ne valtakunnalliset vähimmäisvaatimusten profiilit, joiden mukainen käyttötarkoitus järjestelmään tai hyvinvointisovellukseen sisältyy. Poikkeuksena ovat profiilit, joiden kuvauksessa on erikseen ilmaistu, että kyseistä profiilia ei tarvitse erikseen

ilmoittaa, jos järjestelmä täyttää jonkin toisen (laajemman) profiilin mukaiset vaatimukset1. Ilmoittaminen tehdään määräyksen 4/2024 (luku 6) mukaisesti Kelalle, tietoturvallisuuden arviointilaitokselle ja Valviralle käyttäen tämän määräyksen liitteenä 4 olevaa järjestelmälomaketta.

Yksi järjestelmä, osajärjestelmä, järjestelmäkokonaisuus tai hyvinvointisovellus voi täyttää useiden profiilien mukaiset vaatimukset. Järjestelmään tai hyvinvointisovellukseen on oltava toteutettuna ja järjestelmälomakkeelle merkittynä vähintään ne olennaiset vaatimukset, jotka ovat pakollisia järjestelmän tai hyvinvointisovelluksen käyttötarkoitusta vastaavissa profiileissa.

Tietyn profiilin mukaiset vaatimukset voidaan täyttää yhden tai useamman järjestelmän, osajärjestelmän tai hyvinvointisovelluksen kautta. Tällöin ilmoituksissa ja sertifioinnissa on kuvattava, minkä muiden järjestelmien, osajärjestelmien tai hyvinvointisovellusten kanssa käytettynä järjestelmä, järjestelmäpalvelu tai hyvinvointisovellus täyttää profiilin mukaiset vaatimukset, ja mitä muita edellytyksiä vaatimusten täyttämiselle on. Luokan A järjestelmissä ja hyvinvointisovelluksissa vaatimusten täyttyminen on tarvittaessa todennettava osana sertifiointia myös silloin, kun vaatimuksia täytetään muiden järjestelmien, osajärjestelmien tai hyvinvointisovellusten kautta. Lisätietoja vaatimusten täyttämisestä modulaarisissa järjestelmäkokonaisuuksissa on liitteen 1 luvussa 6.3.

Tietojärjestelmän tai hyvinvointisovelluksen käyttötarkoitukseen sisältyvien profiilien edellyttämien vaatimusten toteuttaminen tai täyttäminen sekä niiden todentaminen yhteistestauksessa tai tietoturvallisuuden arvioinnissa siltä osin kuin vaatimukset ovat sertifioinnissa todennettavia on edellytys luokan A järjestelmien ja hyvinvointisovellusten hyväksytylle sertifioinnille ja tuotantokäyttöönotolle.

Valviran ylläpitämässä tietojärjestelmien rekisterissä ilmoitetaan kunkin järjestelmän, osajärjestelmän ja hyvinvointisovelluksen käyttötarkoitukseen sisältyvät profiilit. Luokan A järjestelmän tai hyvinvointisovelluksen rekisteröinti Valviran tietojärjestelmärekisteriin edellyttää sitä, että sitä koskevien profiilien mukaisiin vaatimuksiin liittyvät tietoturvallisuuden vaatimukset on hyväksytysti todennettu tietoturvallisuuden arvioinnissa ja että järjestelmä tai sovellus on saanut tietoturvallisuustodistuksen. Luokan A2 ja A3 järjestelmiltä ja sovelluksilta edellytetään myös hyväksyttyä Kelan kanssa suoritettua yhteistestausta niistä profiileihin kuuluvista olennaisista vaatimuksista, jotka liittyvät Kanta-palveluihin.

THL voi antaa tiettyyn käyttötarkoitukseen tarkoitettujen järjestelmien tai hyvinvointisovellusten vähimmäisvaatimuksista myös antaa erillisiä määräyksiä, jotka viittaavat olennaisten vaatimusten luettelon avulla määriteltyihin profiileihin.

Profiilien käyttöä ja suhdetta olennaisiin vaatimuksiin kuvataan myös liitteessä 1 luvussa 7.

8 Olennaisten vaatimusten täyttäminen / tietojärjestelmäpalvelun tuottaja ja hyvinvointisovelluksen valmistaja

Tietojärjestelmäpalvelun tuottaja tai hyvinvointisovelluksen valmistaja käyttää olennaisten vaatimusten täyttämisen osoittamiseen liitteessä 4 olevaa järjestelmälomaketta, jonka avulla järjestelmää ja hyvinvointisovellusta koskevia tietoja ilmoitetaan järjestelmien sertifioinnissa ja rekisteröinnissä määräyksen 4/2024 mukaisesti. Järjestelmälomakkeen avulla annetaan asiakastietolain 85 §:n mukainen selvitys olennaisten vaatimusten täyttämisestä. Kaikki järjestelmään, hyvinvointisovellukseen tai osajärjestelmään toteutetut olennaiset vaatimukset kuvataan yhdellä järjestelmälomakkeella. Tämän luvun järjestelmiä ja hyvinvointisovelluksia koskevia kohtia voidaan soveltaa myös osajärjestelmiin, joita voidaan sertifioida osana laajempaa järjestelmäkokonaisuutta.

Luokan B tietojärjestelmä täyttää siihen kohdistuvat olennaiset vaatimukset, kun:

[1] Määräyksen 5/2024 voimaan tullessa profiili 3g1 (liitteessä 3g) on tällainen profiili, jonka sisältämiin vaatimuksiin on otettu kantaa kaikissa liitteiden 3a-3f mukaisissa profiileissa. Tässä tapauksessa järjestelmälomakkeessa ei tarvitse erikseen ilmoittaa profiilia 3g1, jos järjestelmä täyttää jonkin muun profiilin mukaiset vaatimukset.

1. tietojärjestelmäpalvelun tuottaja on kuvannut järjestelmän käyttötarkoituksen, luokitellut järjestelmän ja arvioinut järjestelmän riskitason määräyksen 4/2024 mukaisesti;
2. tietojärjestelmäpalvelun tuottaja on yksilöinyt järjestelmälomakkeeseen ne olennaisten vaatimusten profiilit (liitteen 3 taulukoissa esitetyt profiilit), jotka ovat osa järjestelmän käyttötarkoitusta;
3. tietojärjestelmäpalvelun tuottaja on merkinnyt järjestelmälomakkeeseen ne olennaisten vaatimusten toiminnot, joiden mukaisia toiminnallisuuksia järjestelmään sisältyy;
4. tietojärjestelmäpalvelun tuottaja on merkinnyt järjestelmälomakkeeseen ne olennaisten vaatimusten tietosisällöt, joita järjestelmässä käsitellään, ilmaisten sen mitä tietoja järjestelmä tuottaa tai käyttää;
5. tietojärjestelmäpalvelun tuottaja on merkinnyt järjestelmälomakkeeseen ne olennaisiin vaatimuksiin sisältyvät tietoturvavaatimukset, jotka järjestelmässä toteutetaan tai sen kautta täytetään;
6. kohtien 3-5 mukaisesti merkityt vaatimukset sisältävät vähintään järjestelmää koskevien profiilien mukaiset vaatimukset;
7. kohtien 3–5 mukaisiin vaatimuksiin on järjestelmälomakkeessa ohjeistetulla tavalla merkitty a) ne vaatimukset, jotka järjestelmässä täytetään muiden järjestelmien, hyvinvointisovellusten tai osajärjestelmien avulla, b) ne vaatimukset, joihin liittyen järjestelmässä on tehty merkittäviä muutoksia, mikäli tällaisia vaatimuksia on ja c) ne vaatimukset, jotka eivät ole sovellettavissa, mikäli tietyn vaatimuksen kuvaamisessa näin on ohjeistettu;
8. tietojärjestelmän valmistaja tai tietojärjestelmäpalvelun tuottaja on *itse testannut ja todennut järjestelmässä toimivaksi* kohtien 3–7 mukaiset olennaiset vaatimukset.

Luokan A1 järjestelmä tai hyvinvointisovellus täyttää siihen kohdistuvat olennaiset vaatimukset, kun:

9. luokan B mukaiset edellytykset (edellä) on täytetty[2];
10. järjestelmää tai hyvinvointisovellusta koskevat olennaiset tietoturvavaatimukset (kohta 5) on *toteutettu, täytetty ja dokumentoitu* siten, että voidaan suorittaa tietoturvallisuuden arviointi ja antaa todistus hyväksytystä tietoturvallisuuden arvioinnista.

Luokan A1, A2 tai A3 järjestelmän tuotantokäyttöönotto edellyttää sitä, että yllä kuvattu todennettuja tietoturvavaatimuksia koskeva tietoturvallisuustodistus on annettu ja sitä vastaavat tiedot löytyvät Valviran tietojärjestelmärekisteristä (ks. määräys 4/2024 luku 9).

Luokan A2 järjestelmä tai hyvinvointisovellus **tai luokan A3** järjestelmä täyttää siihen kohdistuvat olennaiset vaatimukset, kun:

11. luokan A1 mukaiset edellytykset (yllä) on täytetty;
12. järjestelmälomakkeeseen on merkitty käsiteltävien tietosisältöjen (kohta 4) osalta, mitä tietoja järjestelmä tai hyvinvointisovellus tuottaa Kanta-palveluihin tai hyödyntää Kanta-palveluista;
13. Kanta-palveluihin liittyviin määrityksiin liittyvät järjestelmää koskevat toiminnalliset vaatimukset (toiminnot ja tietosisällöt, kohdat 3–8), on *toteutettu, täytetty, dokumentoitu ja testattu tietojärjestelmäpalvelun tuottajan toimesta* siten, että järjestelmälle voidaan hyväksytysti suorittaa tarvittavat yhteistestaukset Kelan Kanta-palvelujen yhteistestauksen ohjeiden mukaisesti.

Edellä kuvattujen asioiden ilmoittamista järjestelmälomaketta käyttäen kuvataan määräyksen 5/2024 liitteen 1 luvussa 2.3.

[2] Hyvinvointisovelluksen valmistaja vastaa kohtien 1–8 mukaisista seikoista vastaavalla tavalla kuin tietojärjestelmäpalvelun tuottaja.

Luokan A2 tai A3 tietojärjestelmän tuotantokäyttöönotto edellyttää sitä, että kaikki järjestelmän Kanta-palveluihin liittyvät toiminnot ja tietosisällöt, joihin kohdistuu yhteistestauksen sisältöjä, on hyväksytysti yhteistestattu (ks. myös määräys 4/2024 luku 9).

Luokkaan A kuuluvan järjestelmän tai hyvinvointisovelluksen vaatimustenmukaisuus on osoitettava sertifioinnilla ennen tuotantokäyttöönottoa. Olennaiset vaatimukset täyttävä luokan A tai B järjestelmä tai hyvinvointisovellus on rekisteröitävä Valviran tietojärjestelmärekisteriin. Sertifioinnin ja rekisteröinnin prosessi kuvataan määräyksessä 4/2024 (luku 7) ja tämän määräyksen liitteessä 1. Edellä mainittujen edellytysten numerointi ei suoraan vastaa sertifiointi- ja rekisteröintiprosessin vaiheita.

Jos luokan A järjestelmä ilmoitetaan yhteistestaustarpeen uudelleenarviointiin tai arviointiin siitä, tarvitaanko järjestelmälle uusi tietoturvallisuuden arviointi, on uudet ja olennaisia muutoksia sisältävät toiminnot ja tietosisällöt merkittävä selkeästi liitteen 4 mukaiseen järjestelmälomakkeeseen (ks. myös määräys 4/2024 luku 10).

Tämän määräyksen mukainen järjestelmälomake on täytettävä riippumatta siitä, vastaako järjestelmän tai hyvinvointisovelluksen käyttötarkoitus mitään (ei yhtäkään, yhtä tai useampaa) kansallista profiilia. Järjestelmälomakkeelle merkitään myös muut kuin profiileihin kuuluvat olennaiset vaatimukset, jotka on toteutettu tai täytetään järjestelmän tai hyvinvointisovelluksen kautta. Järjestelmälomakkeella ilmoitetut olennaiset vaatimukset on täytettävä järjestelmässä tai hyvinvointisovelluksessa.

Järjestelmälomakkeeseen tehtyjen merkintöjen on vastattava järjestelmäversiota, joka ilmoitetaan yhteentoimivuuden testaukseen, tietoturvallisuuden arviointiin tai jota ollaan rekisteröimässä Valviran tietojärjestelmärekisteriin. Sertifioinnissa tai rekisteröinnissä käytettävään järjestelmälomakkeeseen ei merkitä sellaisia ominaisuuksia, jotka ovat vasta suunnitteluvaiheessa tai joita ei ole toteutettu järjestelmään.

Integraatiorajapintojen tai muiden järjestelmien tai osajärjestelmien kautta täytettävät vaatimukset voidaan merkitä järjestelmälomakkeeseen. Pakollisten vaatimusten täyttyminen on tarvittaessa pystyttävä todentamaan osana sertifiointia myös näissä tapauksissa.

Tietojärjestelmäpalvelun tuottajan ja hyvinvointisovelluksen valmistajan on seurattava olennaisten vaatimusten muutoksia ja tehtävä muutosten edellyttämät korjaukset (asiakastietolaki 82 §). Jos muutokset edellyttävät uutta yhteistestausta tai uutta tietoturvallisuuden arviointia, nämä toimenpiteet on suoritettava ennen muutokset sisältävän järjestelmän tai hyvinvointisovelluksen version tuotantokäyttöön ottamista.

Tietojärjestelmäpalvelun tuottajan ja hyvinvointisovelluksen valmistajan on varmistettava tietoturvallisuustodistuksen uusimiseen hakeutuessaan, että järjestelmässä tai hyvinvointisovelluksessa on yhteistestattu Kanta-palveluihin liittyvät ominaisuudet voimassa olevien määritysten ja määritysversioiden mukaisesti määräys 4/2024 luvun 7.2 mukaisesti.

Tietojärjestelmäpalvelun tuottaja vastaa siitä, että järjestelmään sisältyvät tai sen kautta sertifioidut olennaiset vaatimukset täyttyvät järjestelmän eri käyttöympäristöissä. Käyttäjäorganisaatiolle on tarvittaessa annettava ohjeistus järjestelmän käyttämiseksi siten, että järjestelmään sisältyvät olennaiset vaatimukset täyttyvät.

Palvelunantaja, Kela, arviointilaitos, THL tai muu taho voi tehdä ilmoituksen Valviralle, mikäli järjestelmä ei täytä tuotantokäytössä edellytettäviä olennaisia vaatimuksia.

9 Olennaisten vaatimusten täyttäminen / palvelunantaja

Asiakastietolain 84 §:n mukaisesti palvelunantajan ja apteekin käyttämien järjestelmien on vastattava käyttötarkoitukseltaan palvelunantajan toimintaa ja täytettävä palvelunantajan toimintaan liittyvät olennaiset vaatimukset. Olennaiset vaatimukset on täytettävä asiakastietolain 101 ja 102 §:n olevien voimaantulo- ja siirtymäaikasäännösten mukaisesti. Olennaiset vaatimukset voidaan täyttää yhden tai useamman järjestelmän tai osajärjestelmän muodostaman kokonaisuuden kautta.

Palvelunantajan on asiakastietolain 77 §:n ja THL määräyksen 3/2024 mukaisesti kuvattava tietoturvasuunnitelmassaan ne järjestelmät, joita se käyttää asiakas- ja potilastietojen käsittelyyn.

Palvelunantajan tulee varmistaa, että sen käyttämät järjestelmät tai osajärjestelmät kokonaisuutena sisältävät ne profiilien mukaiset käyttötarkoitukset ja toteuttavat kyseisten profiilien mukaiset vaatimukset, joita tarvitaan palvelunantajan toiminnassa.

Palvelunantajan on asiakastietolain mukaisia määräaikoja noudattaen liityttävä Kanta-palvelujen käyttäjäksi. Liittyminen edellyttää sitä, että palvelunantajalla on järjestelmä tai järjestelmäkokonaisuus, jonka kautta täytetään Kanta-palveluihin liittymisen edellytykset ja pystytään toteuttamaan palvelunantajan toiminnassa tarvittavien asiakastietojen käsittely ja tallentaminen. Liittymiseen käytettävä järjestelmä voi olla luokkaan A3 kuuluva järjestelmä tai sellainen järjestelmäkokonaisuus, jossa Kanta-palveluihin liittyvät vaatimukset täytetään vähintään luokkaan A2 kuuluvien järjestelmien tai osajärjestelmien avulla (ks. määräys 4/2024 luku 5 ja määräys 4/2024 liite 1).

Palvelunantajan tulee varmistaa, että sen käyttämät luokkaan A1, A2 tai A3 kuuluvat järjestelmät tai hyvinvointisovellukset on hyväksytysti sertifioitu, tuotantokäytössä näiden järjestelmien Kanta-palvelujen kautta toteutettavat ominaisuudet on hyväksytysti yhteistestattu suhteessa voimassa oleviin vaatimuksiin, ja että niitä koskeva tietoturvallisuustodistus on voimassa. Palvelunantajan on myös muilta osin pyrittävä varmistamaan, että kukin sen käyttämä järjestelmä tai sovellus täyttää käyttötarkoituksensa mukaiset olennaiset vaatimukset. Palvelunantajan tulisi hyödyntää Valviran tietojärjestelmärekisteriä sekä hankinta- ja ylläpitosopimuksia tietojärjestelmäpalvelujen tuottajien ja hyvinvointisovellusten valmistajien kanssa näiden seikkojen varmistamisessa. Järjestelmän kautta täytettävien ja sertifioitujen olennaisten vaatimusten täyttymisestä vastaa ensisijaisesti tietojärjestelmäpalvelun tuottaja (ks. luku 8), mutta järjestelmää on käytettävä sen käyttötarkoituksen ja tietojärjestelmäpalvelun tuottajan antamien ohjeiden mukaisesti.

Palvelunantajan tulee osaltaan varmistaa, että sen toiminnassa käytettävistä luokkiin A1, A2, A3 tai B kuuluvista järjestelmistä on voimassa olevat tiedot Valviran tietojärjestelmärekisterissä.

Palvelunantajan on huomioitava omassa toiminnassaan ja järjestelmien käyttöönotossa, tuotantokäytössä sekä tietoturvasuunnitelman mukaisessa toiminnassa olennaiset vaatimukset. Tämä koskee niitä seikkoja ja sertifioinnissa esiin nousseita havaintoja ja edellytyksiä, jotka vaikuttavat olennaisten vaatimusten toteutumiseen palvelunantajan käyttämissä järjestelmissä[3]. Erityisesti on huomioitava Valviran tietojärjestelmärekisterin kautta julkaistavat havainnot järjestelmien vaatimustenmukaisuuden toteuttamiseen.

Palvelunantajan on asiakastietolain 77 §:n mukaan osana tietoturvasuunnitelmaansa osaltaan varmistettava, että tietojärjestelmän käyttöympäristö soveltuu järjestelmän asianmukaiseen sekä tietoturvan ja tietosuojan varmistavaan käyttöön. Osa käyttöympäristöön kohdistuvista vaatimuksista voi toteutua tietojärjestelmäpalvelun tuottajan vastuulla olevan järjestelmän kautta (ks. luku 6). Kunkin järjestelmän on täytettävä ne käyttöympäristöön kohdistuvat olennaiset vaatimukset, jotka ovat tietojärjestelmäpalvelun tuottajan vastuulla. Palvelunantajan on varmistettava, että tietojärjestelmäpalvelun tuottajien ja mahdollisten muiden osapuolten kanssa on sovittu siitä, mitkä käyttöympäristön vaatimuksista täytetään kunkin osapuolen kautta.

Palvelunantaja voi toiminnassaan tarjota asiakkailleen myös hyvinvointisovelluksia tai niitä voi sisältyä palvelunantajan käyttämiin tietojärjestelmiin. Lisäksi palvelunantaja voi hyödyntää asiakastietolain mukaisesti omatietovarannossa olevia hyvinvointitietoja. Hyvinvointisovellusten tarjoaminen tai hyvinvointitietojen hyödyntäminen eivät ole palvelunantajaa velvoittavia. Myös palvelunantajan käyttämissä tietojärjestelmissä voi olla kansalaisille suunnattuja ominaisuuksia ja käyttöliittymiä, esimerkiksi digitaalisten asiointipalvelujen osalta[4].

Jos palvelunantaja toimii itse tietojärjestelmän valmistajan, tietojärjestelmäpalvelun tuottajan tai hyvinvointisovelluksen valmistajan roolissa, on sen täytettävä vastuullaan olevan järjestelmän tai sovelluksen osalta tietojärjestelmän valmistajalle tai tietojärjestelmäpalvelun tuottajalle säädösten asettamat velvoitteet. Näitä ovat järjestelmän tai sovelluksen luokittelu, olennaisten vaatimusten täyttäminen, sertifiointi ja rekisteröinti. Tämä

[3] Kyseessä voi olla esimerkiksi tietoturvallisuusvaatimus, jonka täyttäminen edellyttää toimenpiteitä järjestelmää käyttävän palvelunantajan käyttöympäristössä tai toiminnallinen vaatimus, jonka täyttäminen tapahtuu järjestelmäintegraatiorajapintojen kautta.

[4] Lisätietoja liite 1 luku 6.5 Hyvinvointisovellusten ja asiointipalvelujen vaatimukset ja suhde tietojärjestelmiin

koskee myös mahdollisia tilanteita, joissa palvelunantaja on ottamassa käyttöön järjestelmää, jolla ei ole sellaista määriteltyä vastuutahoa, joka vastaa vaatimustenmukaisuudesta asiakastietolain mukaisesti. Järjestelmää tai sovellusta käyttävä palvelunantaja vastaa näistä toimenpiteistä, jos se ei ole sopinut niihin liittyvistä vastuista minkään tietojärjestelmäpalvelun tuottajan kanssa.

10 Olennaisten vaatimusten todentamisen tarkennuksia

10.1 Vaatimusten täyttymisen arviointi järjestelmissä, jotka eivät liity Kanta-palveluihin

Luokkaan B kuuluville järjestelmille ei suoriteta sertifiointiin kuuluvaa yhteistestausta tai tietoturvallisuuden arviointia. Luokan A1 järjestelmille ei suoriteta yhteistestausta, mutta niille suoritetaan tietoturvallisuuden arviointi (ks. määräys 4/2024 luku 5 ja 7).

Olennaisten vaatimusten luettelossa (liite 2) on eritelty vaatimuksia, jotka nousevat suoraan keskeisimmistä asiakastietojen käsittelyä ohjaavista säädöksistä. Suoraan säädöksistä nousevat vaatimukset asiakas- ja potilastietojen käsittelyyn koskevat kaikkiin eri luokkiin kuuluvia tietojärjestelmiä ja hyvinvointisovelluksia. Kyseisissä vaatimuksissa olevat *Kanta-palveluihin suoraan liittyviä järjestelmiä koskevat määritykset ja viittaukset* eivät kuitenkaan koske luokan B tai A1 järjestelmiä, ellei määritysdokumentissa tai viittauksessa erikseen ole toisin ilmaistu. Näiden vaatimusten sisältö nousee luokan B ja A1 järjestelmille suoraan säännöksistä, joihin eri vaatimuksissa viitataan.

Asiakas- ja potilastietojen käsittelyyn yleisesti liittyviä vaatimuksia, jotka kohdistuvat myös luokkien B ja A1 järjestelmiin, on koottu tämän määräyksen profiililiitteeseen 3g ”Asiakas- tai potilastietojen käsittelyyn tarkoitetun järjestelmän vähimmäisvaatimukset”. Nämä lakisääteiset vaatimukset kohdistuvat kaikkiin asiakas- tai potilastietojen käsittelyyn tarkoitettuihin järjestelmiin, ellei tarkemmassa profiilissa ole erikseen mainittu, että vaatimus ei koske kyseisen profiilin mukaisia järjestelmiä. Lisäksi jos luokan B tai A1 järjestelmä välillisesti käyttää Kanta-palveluissa olevia tietoja tai tuottaa tietoja, jotka toimitetaan Kanta-palveluihin, sitä voivat koskea myös profiilien liitteen 3b "3b2 - Kanta asiakastietovarannosta haettuja tietoja hyödyntävä järjestelmä" tai "3b4 - Kanta asiakastietovarantoon toimitettavia tietoja tuottava järjestelmä" vaatimukset.

Tietojärjestelmäpalvelun tuottaja merkitsee luvun 8 mukaisesti järjestelmälomakkeeseen sekä profiilien kautta järjestelmään kohdistuvat että muut kuin profiileihin kuuluvat olennaiset vaatimukset, joiden mukaisia toimintoja, tietosisältöjä tai tietoturvavaatimuksia tietojärjestelmässä on toteutettu.

10.2 Vaatimusten täyttymisen arviointi ja todentamistavat sertifioinnissa

Luokan A järjestelmien ja hyvinvointisovellusten sertifioinnissa (yhteistestaus ja tietoturvallisuuden arviointi) arvioidaan kunkin sellaisen järjestelmään tai sovellukseen toteutetun vaatimuksen toteutuminen, joka on mukana yhteistestauksen tai tietoturvallisuuden arvioinnin sisällössä. Arvioijana toimii yhteistestauksessa Kela ja tietoturvallisuuden arvioinnissa hyväksytty tietoturvallisuuden arviointilaitos.

Yksittäisen vaatimuksen osalta vaatimuksen arvioija voi ottaa kantaa vaatimuksen täyttymiseen seuraavasti:

- onko vaatimus relevantti järjestelmässä
    - relevantteja vaatimuksia ovat vähintään kaikki järjestelmän tai sovelluksen käyttötarkoitusta vastaavissa profiileissa ilmaistut pakolliset ja suositellut voimassa olevat olennaiset vaatimukset;
    - relevantteja ovat ne olennaiset vaatimukset, jotka tietojärjestelmäpalvelun tuottaja tai hyvinvointisovelluksen valmistaja on merkinnyt toteutetuksi toimittamassaan järjestelmälomakkeessa, sisältäen sekä yllä kuvatut profiileihin kuuluvat että muut järjestelmän kautta täytetyksi merkityt vaatimukset;
    - jos vaatimus on vain osin relevantti arvioitavan tietojärjestelmän, osajärjestelmän tai hyvinvointisovelluksen näkökulmasta tai jos on tarpeen erikseen merkitä, että vaatimus ei ole järjestelmässä tai sovelluksessa relevantti (esim. järjestelmän käyttötarkoitus ja

käyttötarkoituksen rajaukset huomioiden), voi arvioija tehdä asiasta merkinnän arvioinnista syntyvään raporttiin, lausuntoon tai todistukseen, jos asiaa on tarpeen perustella[5];

- relevanteista vaatimuksista:
  - vaatimus täyttyy täysin (normaali tilanne);
  - vaatimus ei täyty tai täyttyy vain osittain, ja täyttymättä jäävä osa kompensoidaan hyväksyttävällä tavalla siten, että vaatimuksen mukainen tavoite saavutetaan, jolloin kompensointitapa on kuvattava;
  - vaatimus ei täyty;
  - tarvittaessa merkintä todentamistavasta ja siitä, kuinka vaatimuksen täyttyminen on todettu, esimerkiksi viite dokumentaatioon, testausraporttiin tai ohjelmiston tuotokseen.

Yllä näkyviä tietoja voi sisältyä yksityiskohtaiseen yhteistestauksesta tai tietoturvallisuuden arvioinnista syntyvään raporttiin.

Järjestelmän tai sovelluksen käyttötarkoitukseen kuuluvien pakollisten olennaisten vaatimusten on täytyttävä tuotantokäyttöön otettavissa järjestelmissä ja sovelluksissa.

Jos pakollinen olennainen vaatimus ei täyty, arvioija voi keskeyttää arvioinnin tai asettaa vaatimuksen täyttämiselle määräajan ennen yhteistestauksen tai tietoturvallisuuden arvioinnin hyväksymistä osana käynnissä olevaa sertifiointiprosessia. Keskeytetyn tai keskeneräisen arvioinnin perusteella tietojärjestelmäpalvelun tuottajan ei tule päivittää järjestelmän tietoja Valviran tietojärjestelmärekisteriin.

Jos relevantti vaatimus ei täyty tai täyttyy vain osittain, mutta sen tavoite on saavutettavissa hyväksyttävästi kompensoiden, arvioija voi tehdä päätöksen hyväksymisestä siten, että hyväksyttävä kompensointi ilmoitetaan yhteistestauslausunnossa tai tietoturvallisuustodistuksessa. Kompensoinnin hyväksyttävyyden arvioimiseksi arvioija voi edellyttää tietojärjestelmäpalvelun tuottajalta tai hyvinvointisovelluksen valmistajalta riskiarviota ja kuvausta vaatimuksen kompensoinnista. Kompensointi on poikkeuksellinen toimenpide, jonka hyväksymiseen on oltava painava peruste esimerkiksi asiakas- tai potilasturvallisuuden tai sote-palvelujen toimivuuden näkökulmasta. Kompensointi ei saa aiheuttaa haittaa tai kohtuuttomia vaatimuksia tai kustannuksia muille toimijoille, erityisesti käyttäjille. Tietojärjestelmäpalvelun tuottajan ja hyvinvointisovelluksen valmistajan on ilmoitettava hyväksytyt kompensoinnit järjestelmää tai sovellusta käyttäville palvelunantajille.

Jos järjestelmässä tai sovelluksessa edellytettyyn vähimmäisvaatimusten profiiliin liittyvä pakollinen vaatimus ei täyty eikä vaatimusta voida hyväksyttävästi kompensoida, järjestelmä tai sovellus ei ole profiilin mukaiset vaatimukset täyttävä. Yhteistestausta tai tietoturvallisuuden arviointia ei voida suorittaa loppuun, ellei pakollisia vaatimuksia täytetä tai kompensoida hyväksytysti. Valviran tietojärjestelmärekisteriin tehtävässä ilmoituksessa ei tule ilmoittaa profiilia, jonka mukaisia toiminnallisia tai yhteentoimivuuden vaatimuksia järjestelmä tai sovellus ei täytä. Järjestelmää tai sovellusta ei tällöin saa ottaa tuotantokäyttöön kyseiseen käyttötarkoitukseen. Tietojärjestelmää voidaan kuitenkin käyttää niihin käyttötarkoituksiin, joihin liittyvät vaatimukset on hyväksytysti sertifioitu ja ilmoitettu. Tällöin tietojärjestelmäpalvelun tuottajan tulee osaltaan varmistaa, että järjestelmää ei oteta käyttöön käyttötarkoitukseen, jonka vaatimuksia se ei täytä.

Kompensaatiot ja vähäiset poikkeamat järjestelmässä ilmoitettujen ja sen käyttötarkoitusta vastaavien profiilien mukaisten pakollisten vaatimusten täyttämisestä merkitään tietoturvallisuustodistukseen, mikäli ne liittyvät tietoturvavaatimuksiin. Tietojärjestelmäpalvelun tuottajan tai hyvinvointisovelluksen valmistajan on ilmoitettava mahdolliset kompensaatiot järjestelmää tai sovellusta käyttäville palvelunantajille. Tietoturvallisuuden arvioinnissa todetut vähäiset poikkeamat, jotka eivät muodosta käyttöönoton estävää merkittävää poikkeamaa, on korjattava kohtuullisen ajan kuluessa, kuitenkin viimeistään seuraavaan tietoturvallisuustodistuksen uusimiseen mennessä.

[5] Joissakin olennaisissa vaatimuksissa on myös ohjeistettu, että tietojärjestelmäpalvelun tuottajan tai hyvinvointisovelluksen valmistajan on erikseen merkittävä ja perusteltava, mikäli kyseinen vaatimus ei ole relevantti järjestelmässä tai sovelluksessa.

Jos sertifioinnissa käy ilmi, että sertifioitavana oleva, jo tuotantokäytössä toimiva tietojärjestelmä tai hyvinvointisovellus ei täytä pakollista relevanttia vaatimusta, on tietojärjestelmä tai sovellus korjattava tai vaatimus kompensoitava hyväksytysti ennen vaatimukseen liittyvän yhteistestauksen tai tietoturvallisuuden arvioinnin hyväksymistä. Merkittävistä poikkeamista tuotantokäytössä on ilmoitettava asiakastietolain 82 §:n mukaisesti.

Valvira voi määrätä asiakastietolain mukaisen velvollisuuden määräajassa täytettäväksi (asiakastietolaki 93 §). Määräaika voi koskea myös sertifiointiin liittyvää tietojärjestelmäpalvelun tuottajan tai hyvinvointisovelluksen valmistajan velvoitetta kuten korjausta tai kompensointia. Määräaika voi koskea kaikkia tuotannossa toimivan järjestelmän tai sovelluksen käyttöympäristöjä (ks. myös tämän määräyksen luku 10.4, kohta 6).

Valviran tietojärjestelmärekisterissä ilmoitetaan asiakastietolain 80 §:n mukaisesti tietoja tuotantokäytössä olevien tietojärjestelmien ja hyvinvointisovellusten merkittävistä poikkeamista, yhteistestauksen tuloksista ja tietoturvallisuustodistuksen voimassaolosta (ks. määräys 4/2024 luku 8). Valvira voi päättää myös muista tietojärjestelmärekisteriin merkittävistä tiedoista, kuten järjestelmän tai sovelluksen käytössä huomioitavista kompensaatioista tai muista sertifioinnin yhteydessä esiin nousseista havainnoista.

Mikäli vaatimuksen toteutumisen arviointi edellyttää vaatimuksen pohjana olevan määritysdokumentin tarkempaa tulkintaa, on arvioijan tarvittaessa pyrittävä vahvistamaan tulkinta määritysdokumentin vastuutaholta kuten Kela tai THL. Vastuutahon tulisi julkaista tarkennettu tulkinta, ensisijaisti varsinaisen määritysdokumentin yhteydessä.

Tietojärjestelmäpalvelun tuottajan ja hyvinvointisovelluksen valmistajan tulee valmistautua yhteistestaukseen tai tietoturvallisuuden arviointiin siten, että relevantit vaatimukset on tunnistettu ja relevanttien vaatimusten täyttämisestä voidaan esittää tarvittava materiaali tai suorittaa tarvittavat todentamistoimenpiteet. Valmistautumiseen kuuluu myös erikseen ilmaistujen ei-relevanttien tai ei sovellettavissa olevien vaatimusten merkitseminen luvun 8 mukaisesti ja tarvittaessa todentamiseen tarvittavien tietojen kokoaminen, jos todentamiseen tarvitaan tietoja kolmansilta osapuolilta.

Tietoturvallisuusvaatimusten todentamisessa käytetään seuraavia todentamistapoja:

V: validointi tai tekninen tarkastus, esimerkiksi järjestelmän tai sovelluksen tuottaman lokin, sanomainstanssin tai järjestelmän tuottaman raportin läpikäynti;

testaus, jossa

TT: tarkistus järjestelmää tai sovellusta käyttämällä (toiminnallisella testauksella) ominaisuuden olemassaolosta ja asianmukaisuudesta osana tietoturvallisuuden arviointia;

HT: tekninen tietoturva- ja haavoittuvuustestaus ja turvallisuustason arviointi osana tietoturvallisuuden arviointia.

D: järjestelmän tai sovelluksen dokumentaation tai muiden järjestelmään liittyvien dokumenttien läpikäynti;

(täydentävä): H: haastattelu osana tietoturvallisuuden arviointia, jolla voidaan syventää ja täydentää arviointia; haastattelu ei ole hyväksyttävä ensisijaiseksi vaatimuksen todentamistavaksi luokan A järjestelmissä tai hyvinvointisovelluksissa.

Vaatimusten todentamisessa on käytettävä todentamistapaa, joka on riittävä kunkin vaatimuksen tai vaatimuskohdan todentamiseen. Riittävä todentamistapa ja -taso riippuu vaatimuksesta, järjestelmän tai hyvinvointisovelluksen tarkemmasta luokittelusta, laajuudesta ja käyttötarkoituksesta (mm. sisällön laajuudesta ja käsiteltävien tietojen luonteesta riippuva riskitaso huomioiden). Eri vaatimusten todentamisen tapaa ja tasoa kuvataan myös tämän määräyksen liitteissä 1, 2 ja 3. Kunkin tietoturvavaatimuksen osalta liitteessä 2 ja tarvittaessa profiileissa ilmaistaan käytettävät todentamisen tasot eri luokkiin tai riskitasoihin sijoittuvissa tai eri käyttötarkoituksiin tarkoitetuissa järjestelmissä ja hyvinvointisovelluksissa.

Jos arvioitavana on olennainen tietoturvavaatimus, joka on todennettu tietojärjestelmässä tai hyvinvointisovelluksessa muiden voimassa olevien säädösten kuin asiakastietolain nojalla kyseisissä säädöksissä hyväksytyn kolmannen osapuolen toimesta, vaatimusta ei todenneta uudelleen. Tämä edellyttää sitä, että kyseinen kolmannen osapuolen suorittama todentaminen on voimassa ja tietojärjestelmäpalvelun tuottaja tai hyvinvointisovelluksen valmistaja esittää todentamisesta ja hyväksymisestä tarvittavan dokumentaation. Dokumentaatiosta tulee ilmetä vähintään todennetun vaatimuksen kohde riittävän tarkasti eriteltynä, säädös tai säännös johon todentaminen on perustunut, todennettu vaatimus lähdeviitteineen ja vaatimuksen vastaavuus kyseiseen olennaiseen vaatimukseen, merkintä vaatimuksen hyväksytystä todentamisesta, todentaneen kolmannen osapuolen tiedot sekä voimassaolo. Esimerkkejä muiden säädösten nojalla todennetuista vaatimuksista ovat lääkinnällisten laitteiden valmistajille suoritetut laatujärjestelmän ulkoiset auditoinnit ja tietoturvavaatimuksissa suorina lähteinä käytettyjen standardien mukaisuuteen kohdistuvat hyväksytyt arvioinnit. Liitteen 4 mukaisella järjestelmälomakkeella ilmoitetaan sellaiset muut arvioinnit, joihin tietojärjestelmäpalvelun tuottaja tai hyvinvointisovelluksen valmistaja esittää jo suoritetun todentamisen riittävän. Nämä ilmaistaan järjestelmälomakkeen perustiedot-sivulla sekä kunkin näin todennetun olennaisen vaatimuksen kohdalla.

Tietoturvatestauksessa ja tietoturvavaatimusten todentamisessa suositellaan sovellettavaksi sopivaa yleistä tietoturvavaatimusten testauksessa käytettävää kehikkoa, kuten OWASP ASVS tai MASVS, sikäli kuin vaatimukset ovat vastaavia tai yhteensopivia liitteessä 2 esitettyjen tietoturvavaatimusten kanssa.

10.3 Vaatimusten ja määritysten versionhallinta

Olennaiset vaatimukset on täytettävä tuotantokäytössä ja sertifioitava voimassa olevien määritysten mukaisesti. Jos olennaisessa vaatimuksessa viitattu määritys sisältää järjestelmän tai sovelluksen luokkaa ja käyttötarkoitusta vastaavia vaatimuksia, on järjestelmässä tai sovelluksessa toteutettava nämä vaatimukset perustuen tarkemman määritysdokumentin voimassa olevaan versioon.

THL tai Kela julkaisevat tiedot siitä, mitkä ovat voimassa olevia määrityksiä ja määritysversioita, ja minkä versioiden nojalla vaatimustenmukaisuus todennetaan. Kela julkaisee ajantasaiset tiedot siitä, mitä määrityksiä ja määritysversioita edellytetään Kanta-palvelujen tuotantoympäristössä ja Kanta-rajapintoihin liittyvässä yhteistestauksessa. Luokkaan A2 tai A3 kuuluvassa tietojärjestelmässä tai hyvinvointisovelluksessa järjestelmätoteutuksen, yhteistestauksen ja puoltavan lausunnon on perustuttava sellaisiin olennaisiin vaatimuksiin, määrityksiin ja määritysversioihin, joita kulloinkin edellytetään Kanta-palveluihin liittyvältä järjestelmältä tai sovellukselta. Kanta-palveluissa on mahdollista tukea useita määritysten versioita eri toiminnoista ja tietosisällöistä. Yhteistestauksessa voidaan tukea tai edellyttää uusia määritysversioita ennen kuin niitä aletaan tukea tai edellyttää tuotantokäytössä.

Jos uuden THL:n tai Kelan tuottamien määrityksen tai määritysversion voimaantulon yhteydessä edellytetään aiemman toteutuksen muuttamista uutta sertifiointia vaativalla tavalla, THL tai Kela ilmaisee tämän määrityksen julkaisun yhteydessä. Jos uudelleensertifiointia tai sertifiointitarpeen uutta arviointia edellytetään, on nämä toimenpiteet toteutettava määräyksessä tai määrityksen yhteydessä ilmaistun määräajan puitteissa. Myös aiempien määritysversioiden mukaiset toteutukset ovat hyväksyttäviä sertifioinnissa ja tuotantokäytössä, jos niiden voimassaolon päättymisestä tuotantokäytössä ja sertifioinnissa ei ole ilmoitettu määrityksessä tai siihen viittaavassa materiaalissa.

Kela tai THL julkaisee tiedon poistuvista tai korvaantuvista määritysversioista ja siitä, mihin asti poistuvan tai korvaantuvan määritysversion mukaisia toteutuksia voidaan hyväksyä luokan A järjestelmien sertifioinnissa ja Kanta-palvelujen tuotantoympäristössä. Sosiaalihuollon asiakasasiakirjojen rakenteiden ja tietojen eri versioiden tukemiseen liittyviä vaatimuksia kuvataan THL:n määräyksessä 1/2024.

Järjestelmämuutoksista tehtäviä ilmoituksia suhteessa luokan A järjestelmien sertifiointiin käsitellään määräyksen 4/2024 liitteessä 2.

Lisätietoja määritysten hyödyntämisestä ja suhteesta olennaisiin vaatimuksiin on tämän määräyksen liitteessä 1.

10.4 Merkittävät poikkeamat olennaisista vaatimuksista

Merkittäviä poikkeamia tuotantokäytössä toimivissa järjestelmissä tai hyvinvointisovelluksissa ovat:

1. Poikkeama, joka aiheuttaa riskejä potilas- tai asiakasturvallisuudelle;
2. Poikkeama, joka aiheuttaa merkittäviä riskejä tietosuojalle, tietoturvallisuudelle tai sosiaali- ja terveyspalvelujen toiminnalle;
3. Sellainen poikkeama olennaisista vaatimuksista tuotantokäytössä olevassa tietojärjestelmässä tai hyvinvointisovelluksessa, joka aiheuttaa merkittäviä tai pitkäaikaisia heijastusvaikutuksia tai lisäpoikkeamia useille palvelunantajille tai useille muille tietojärjestelmille tai hyvinvointisovelluksille;
4. Tietojen oikeellisuudelle, eheydelle tai yhteentoimivuudelle (erityisesti Kanta-palvelujen kautta) laajamittaisia häiriöitä aiheuttava poikkeama;
5. Tuotantokäytössä toimivan järjestelmän tai sovelluksen tietoturvallisuustodistus (tai aiempien säädösten mukaisen vaatimustenmukaisuustodistus) on vanhentunut, erityisesti todistuksen uusimisen pitkittyessä tietojärjestelmän valmistajasta, tietojärjestelmäpalvelun tuottajasta tai hyvinvointisovelluksen valmistajasta johtuvista syistä;
6. Tietojärjestelmään tai hyvinvointisovellukseen ei ole toteutettu sen käyttötarkoitukseen kuuluvaa pakollista olennaista vaatimusta eli järjestelmän käyttötarkoitusta vastaavassa profiilissa pakolliseksi merkittyä vaatimusta;
7. Luokkaan A kuuluvasta tietojärjestelmästä tai hyvinvointisovelluksesta ei ole hyväksytysti sertifioitu kohdan 6 mukaista pakollista olennaista vaatimusta, johon kohdistuu todentaminen yhteistestauksessa tai tietoturvallisuuden arvioinnissa;
8. Tuotantokäytössä toimivassa järjestelmässä tai sovelluksessa toteutettu pakollinen ominaisuus perustuu vanhentuneeseen määritysversioon, jonka voimassaolo tuotannossa tai tuki Kanta-palveluissa on päättynyt siten, että järjestelmässä tai sovelluksessa ei ole pystytty tai ei pystytä siirtymään voimassa olevien vaatimusten mukaiseen toteutukseen säännösten tai valvontaviranomaisen edellyttämässä määräajassa;
9. Säädöksissä asetettuja tai viranomaisten asettamia määräaikoja järjestelmään tai sovellukseen edellytettäville korjauksille ei ole noudatettu, erityisesti noudattamattomuuden toistuessa.

Merkittävistä poikkeamista on ilmoitettava asiakastietolain 82 ja 90 §:n mukaisesti. Tietojärjestelmän valmistajan, tietojärjestelmäpalvelun tuottajan, välittäjän, palvelunantajan tai hyvinvointisovelluksen valmistajan, jota merkittävä poikkeama koskee, on ryhdyttävä toimenpiteisiin poikkeaman korjaamiseksi. Valvira julkaisee tietoa tietojärjestelmiä ja hyvinvointisovelluksia koskevista poikkeamista osana tietojärjestelmien rekisteriä. Valvira ohjaa ja edistää vaatimustenmukaisuutta asiakastietolain mukaisesti. Valvira voi muun muassa tehdä tarkastuksia (89 §), antaa määräyksen velvollisuuden täyttämiseksi tai puutteiden korjaamiseksi (93 ja 94 §), asettaa käyttökiellon (94 §) sekä tehostaa antamaansa määräystä uhkasakolla (96 §).

Jos osana sertifiointiprosessia havaitaan sellainen poikkeama olennaisista vaatimuksista, joka johtaisi merkittävään poikkeamaan tuotantokäytössä, ei sertifiointia voida hyväksytysti suorittaa loppuun ennen kuin poikkeaman aiheuttava seikka on korjattu tai kompensoitu, tai poikkeamasta koituvat virhetilanteet muulla tavoin estetty. Vaatimukset, jotka eivät täyty tai täyttyvät puutteellisesti voivat aiheuttaa korjaustarpeen ennen yhteistestauksen tai tietoturvallisuuden arvioinnin hyväksymistä tai arvioinnin keskeyttämisen, kuten luvussa 10.2 on kuvattu.

Mikäli tuotannossa toimiva tietojärjestelmä tai hyvinvointisovellus ei täytä voimassa olevia siihen pakollisena kohdistuvia olennaisia vaatimuksia tai sen vaatimustenmukaisuus on vanhentunut, tietojärjestelmäpalvelun tuottajan tai hyvinvointisovelluksen valmistajan on ilmoitettava asiasta Valviralle. Luokan A2 tai A3 järjestelmissä tai hyvinvointisovelluksissa ilmoitus on tehtävä myös Kelalle. Merkittävistä poikkeamista on ilmoitettava 82 §:n mukaisesti Valviralle ja järjestelmää käyttäville palvelunantajille. Hyvinvointisovelluksissa ilmoitus on tehtävä myös

sovelluksen käyttäjille. Jos merkittävä poikkeama johtuu valmistajan toiminnasta tai itse järjestelmästä tai hyvinvointisovelluksesta, on tietojärjestelmäpalvelun tuottajan tai hyvinvointisovelluksen valmistajan arvioitava poikkeamasta koituva riski ja suunniteltava tarvittavat korjaus- tai jatkotoimenpiteet riskiarvion perusteella. Jos kyseessä on sertifioinnissa todennettu vaatimus, jonka täyttymättömyys johtuu järjestelmään tehdyistä muutoksista, on korjauksen jälkeen tehtävä tarvittavat muutosilmoitukset määräyksen 4/2024 liitteen 2 mukaisesti. Nämä toimenpiteet on suoritettava sen lisäksi, mitä asiakastietolain 82 ja 90 §:n muuten säätävät tietojärjestelmän ja hyvinvointisovelluksen käyttöönoton jälkeisestä seurannasta ja poikkeamista ilmoittamisesta.

Järjestelmän, osajärjestelmän tai hyvinvointisovelluksen on toimittava oikeellisesti siihen toteutettujen olennaisten vaatimusten osalta. Järjestelmässä tai sovelluksessa voidaan todeta olevan poikkeama olennaisista vaatimuksista, mikäli se selvästi toimii virheellisesti, esimerkiksi kohdistaa tietoja säännönmukaisesti väärälle henkilölle. Tämä ei edellytä sitä, että oikeellisuusvaatimus olisi erikseen mainittu olennaisissa vaatimuksissa tai niiden viittaamissa määrityksissä.

11 Ohjaus ja neuvonta

Lisätietoja tämän määräyksen soveltamisesta ja sertifiointiprosessista suhteessa tietojärjestelmille ja hyvinvointisovelluksille asetettaviin olennaisiin vaatimuksiin on liitteessä 1. Lisätietoja olennaisista vaatimuksista ja sertifiointiprosessista sekä tuki- ja koulutusmateriaalia löytyy THL:n sivustolta ja Kanta.fi-verkkosivustolta.

Terveyden ja hyvinvoinnin laitos ohjaa ja neuvoo pyynnöstä tämän määräyksen soveltamisessa.

12 Voimaantulo ja siirtymäsäännökset

Tämä määräys tulee voimaan 10. päivänä toukokuuta 2024 ja on voimassa toistaiseksi.

Määräyksen 4/2024 luvussa 12 on kuvattu siirtymäsäännöksiä aiemmin sertifioitujen järjestelmien vaatimustenmukaisuuden todentamisen ja voimassaolon näkökulmasta.

Määräysten sisältämien vaatimusten voimaantulon kannalta on huomioitava:

- *tämän määräyksen 5/2024 voimaantulopäivämäärä*, josta lähtien määräystä ja sen liitteitä sovelletaan tässä luvussa ilmaistuilla tarkennuksilla ja

- *määräyksen 4/2024 siirtymäsäännöksissä ilmaistut päivämäärät*, joiden kautta ilmaistaan ennen määräysten voimaantuloa tehtyjen toimenpiteiden ja vaatimusten voimassaoloa ja jatkuvuutta, kuten aiemmin sertifioitujen järjestelmien ja hyvinvointisovellusten vaatimustenmukaisuuden voimassaoloa tai määräyksen voimaan tullessa käynnissä olevien sertifiointiprosessien menettelyjä.

Profiilien ja vaatimusten toteuttamisen, sertifioinnin ja Valviran tietojärjestelmärekisteriin tehtävien ilmoitusten näkökulmasta tulee lisäksi huomioida seuraavat vaatimusten voimaantuloon liittyvät ajankohdat:

1. Määräyksen 5/2024 liitteissä 3 ilmoitettu ”*Profiilin voimaantulopäivä sertifioinnissa ja ilmoituksissa”*, josta lähtien profiilin mukaisia vaatimuksia viimeistään sovelletaan järjestelmien tai hyvinvointisovellusten sertifioinnissa (yhteistestaus ja tietoturvallisuuden arviointi) ja Valviran tietojärjestelmärekisteriin tehtävissä ilmoituksissa, jos järjestelmän käyttötarkoitus on profiilin mukainen.

2. *Profiilissa yksittäisen vaatimuksen kohdalla näkyvä päivämäärä*. Tämä päivämäärä kuvaa ajankohtaa, jolloin vaatimus on astunut tai astuu voimaan profiilin mukaisissa tuotannossa toimivissa järjestelmissä tai sovelluksissa. Profiilin mukaisessa tuotantokäytössä toimivassa järjestelmässä ja sovelluksessa on toteutettava tai täytettävä vaatimus viimeistään tähän ajankohtaan mennessä. Jos vaatimuksen kohdalla lukee ”suositeltava”, profiilin mukaisessa järjestelmässä ja sovelluksessa suositellaan vaatimuksen toteuttamista, mutta toteuttaminen ei ole tuotantokäyttöön ottamisen edellytys. Jos vaatimuksen kohdalla lukee ”voimassa” tai menneisyydessä oleva päivämäärä, vaatimus perustuu jo aiemmin voimassa

olleisiin säännöksiin ja sen on oltava toteutettuna kaikissa tuotantokäytössä olevissa järjestelmissä ja sovelluksessa, joita vaatimus koskee. Vaatimusten voimassaoloon voi kohdistua myös vaatimus- tai järjestelmäluokkakohtaisia tarkennuksia. Mahdolliset tarkennukset ilmaistaan kussakin profiilissa kunkin vaatimuksen kohdalla. Sertifioinnissa noudatetaan kohdan 1 mukaisia määräaikoja siten, että vaatimukset, joihin kohdistuu yhteistestauksen tai tietoturvallisuuden arvioinnin toimenpiteitä on todennettu ja niitä vastaava ilmoitus on toimitettu Valviran tietojärjestelmärekisteriin ennen kuin järjestelmä, järjestelmäversio, hyvinvointisovellus tai sovellusversio otetaan tuotantokäyttöön. Sertifioinnissa on huomioitava vaatimukset testauksessa ja tuotantokäytössä voimassa olevien ja voimaan tulevien määritysten mukaisesti, kuten luvussa 10.3 on kuvattu.

Jos järjestelmä tai hyvinvointisovellus täyttää useiden eri profiilien mukaisia vaatimuksia, ja jollakin vaatimuksella on eri profiileissa eri voimaantuloaikoja, järjestelmässä tai sovelluksessa on toteutettava kyseinen vaatimus aikaisimman voimaantuloajan mukaisesti.

Myöhemmin annettavilla määräyksillä voidaan korvata tämä määräys tai täydentää sitä. Eri sosiaali- ja terveyspalveluissa erityisesti edellytettävistä olennaisista vaatimuksista tai profiileista voidaan antaa erillisiä määräyksiä. Olennaisten vaatimusten luetteloa voidaan täydentää määräystä muuttamatta erikseen ilmoitettavina ajankohtina. Uusia käyttötarkoituksia varten voidaan julkaista määräykseen ja luetteloon perustuvia profiileja, joista voidaan tehdä sitovia uusilla määräyksillä.

Sirpa Soini

Johtaja

Jarmo Kärki

Yksikönpäällikkö

Liitteet

Liite 1. Olennaisten vaatimusten soveltamisohjeet

Liite 2. Olennaisten vaatimusten luettelo

Liite 3a. Sähköisen reseptin profiilit

Liite 3b. Kanta-asiakastietovarantoon liittyvien järjestelmien profiilit

Liite 3c. Potilastiedon arkiston profiilit

Liite 3d. Sosiaalihuollon asiakastiedon arkiston profiilit

Liite 3e. Kuvantamisen profiilit

Liite 3f. Todistusten profiilit (julkaistaan myöhemmin)

Liite 3g. Asiakas- tai potilastietojen käsittelyyn tarkoitetun järjestelmän vähimmäisvaatimukset (sis. luokka B tai A1)¨

Liite 3h. Kansalaisen digipalvelujen ja hyvinvointitietojen profiilit

Liite 4: Olennaisten vaatimusten järjestelmälomake

Tiedoksi

sosiaali- ja terveydenhuollon asiakas- ja potilastietojärjestelmien sekä apteekkien järjestelmien valmistajat ja tietojärjestelmäpalvelujen tuottajat
sosiaali- ja terveydenhuollon julkiset ja yksityiset palvelunantajat
apteekit
välittäjät
hyvinvointisovellusten valmistajat
sosiaali- ja terveydenhuollon tietohallintopalvelujen ja ICT-palvelujen tuottajat
Kansaneläkelaitos
Sosiaali- ja terveysalan lupa- ja valvontavirasto Valvira
sosiaalialan osaamiskeskukset
tietoturvallisuuden arviointilaitokset
Kyberturvallisuuskeskus
Tietosuojavaltuutetun toimisto
sosiaali- ja terveysministeriö
valtiovarainministeriö
liikenne- ja viestintäministeriö
Lääkealan turvallisuus- ja kehittämiskeskus FIMEA
aluehallintovirastot
Digi- ja väestötietovirasto
Huoltovarmuuskeskus
Suomen Kuntaliitto ry

Tämä määräys julkaistaan viranomaisten määräyskokoelmissa

- FINLEX ® - Viranomaisten määräyskokoelmat: Terveyden ja hyvinvoinnin laitos https://www.finlex.fi/fi/viranomaiset/normi/561001/

ja on saatavissa:

- Terveyden ja hyvinvoinnin laitoksen kirjaamosta sekä

- Internet-osoitteesta https://thl.fi/aiheet/tiedonhallinta-sosiaali-ja-terveysalalla/maaraykset-jamaarittelyt/maaraykset