



THL:n määräysluonnosten esittely

Toimittajayhteistyökokous, Kanta-palvelut
26.10.2021

Antti-Olli Taipale

Esitykseen ovat sisältöä tuottaneet lisäksi Juha Mykkänen, Jussi Lehto, Minna Linsamo ja Tarja Rätty

Terveyden ja hyvinvoinnin laitos

Sote-tiedonhallinnan määräykset 2021

THL antaa vuonna 2021 **kuusi** määräystä sosiaali- ja terveydenhuollon tiedonhallinnan kokonaisuudesta vuoden loppuun mennessä. Määräyksillä ohjataan asiakastietolain täytäntöönpanoa.

1. [Määräys sosiaalihuollon asiakasasiakirjojen rakenteista ja asiakasasiakirjoihin merkittävistä tiedoista](#)
 2. [Määräys valtakunnallisten tietojärjestelmäpalveluiden avulla terveydenhuollon ulkopuolelle välitettävistä asiakirjoista](#)
 3. [Määräys tietoturvasuunnitelmaan sisällytettävistä selvityksistä ja vaatimuksista](#)
 4. [Määräys sosiaali- ja terveydenhuollon tietojärjestelmien luokittelusta ja sertifiointista](#)
 5. [Määräys sosiaali- ja terveydenhuollon tietojärjestelmien olennaisista vaatimuksista](#)
 6. [Määräys omatietovarantoon liitettävien hyvinvointitietoja käsittelevien hyvinvointisovellusten olennaisista vaatimuksista ja sertifiointista](#)
- Määräysluonnokset julkaistu osoitteessa thl.fi/sotetiedonhallinta/lausuntokierroksella
 - Lausuntoaika 3.9-18.10.2021 määräyksen luonnoksessa 1, 13.9-24.10.2021 luonnoksessa 2, 15.9-27.10.2021 luonnoksissa 3-5 ja 29.9-27.10.2021 luonnoksessa 6, palautteet sähköisellä Webropol-lomakkeella

Aiheuutisia määräysten lausuntokierroksista

- [Määräysluonnos sosiaalihuollon asiakasasiakirjarakenteista on lausuttavana 3.9.2021](#)
- [Lausuntokierros THL määräyksestä Kanta-palveluiden avulla terveydenhuollon ulkopuolelle välitettävistä asiakirjoista on käynnistynyt 13.9.2021](#)
- [Lausuntokierros Tietoturvasuunnitelmaan sisällytettävien selvitysten ja vaatimusten määräyksestä on käynnistynyt 15.9.2021](#)
- [Lausuntokierros tietojärjestelmien olennaisista vaatimuksista, luokittelusta ja sertifiointista on käynnistynyt 15.9.2021](#)
- [Lausuntokierros Omatietovarannon hyvinvointisovellusten olennaisista vaatimuksista ja sertifiointista on käynnistynyt 29.9.2021](#)

Miksi määräykset uudistuvat?

- Useiden määräysten (**2-5**) pohjana ovat vuosina 2015-2018 annetut aiemmat määräykset
- Asiakastietolain (muutosten ja lisäysten) toimeenpano edellyttää tarkempaa sääntelyä
 - Uudet palvelut, (mm. sosiaalihuollon asiakastiedon arkisto, omatietovaranto ja hyvinvointisovellukset)
 - Muutokset olemassa oleviin velvoitteisiin (mm. olennaisten vaatimusten kohdistuminen myös palvelunantajiin, muutokset tietoturvasuunnitelmiin ja järjestelmiin kohdistuviin vaatimuksiin)
- Tukevat sote-uudistuksessa tarvittavaa tiedonhallintaa
- Kokoavat yhteen ja jäsentävät joukon tarkempaa materiaalia, tukevat esim. eri järjestelmissä olennaisten määrittelyjen löytämisessä
- Korvaavat joukon aiemmin hajallaan olleita ohjeita ja osin vanhentuneita liitteitä ja materiaaleja
- Huomioivat
 - Muuttuneet ja voimaan tulleet säädökset (AsTL lisäksi myös henkilötietojen käsittely, tiedonhallintalaki, rajaukset suhteessa toisiolakiin jne.)
 - Uudenlaiset tiedonhallinnan ratkaisut: pilvipalvelut, modulaariset tietojärjestelmät, tietoaaltat ensisijaisessa käytössä, katselin- ja asiointijärjestelmät
 - Aiempien määräysten soveltamisesta esiin nousseet kehittämistarpeet

Määräys 1/2021 sosiaalihuollon asiakasasiakirjojen rakenteista ja asiakasasiakirjoihin merkittävistä tiedoista

- Asiakastietolaki velvoittaa liittymään valtakunnallisten tietojärjestelmäpalvelujen käyttäjäksi (7§). Julkisen osalta alkaen 1.9.2024 ja yksityisen osalta 1.1.2026
- Asiakirjamääräys perustuu uuteen asiakastietolakiin sekä olemassa olevaan asiakirjalakiin
- Määräyksellä yhdenmukaistetaan sosiaalihuollossa käytettävät asiakasasiakirjat ja niiden tietorakenteet. Sosiaalihuollon toimijat ottavat käyttöön rakenteiset ja määrämuotoiset asiakasasiakirjat
- Määräystä sovelletaan sosiaalihuollon asiakastietojen kirjaamisessa, tallentamisessa ja käsittelyssä julkisessa ja yksityisessä sosiaalihuollossa sekä sosiaalihuollon asiakastietojen käsittelyyn tarkoitettujen tietojärjestelmien toteutuksessa
- Tavoitteena on antaa määräys marraskuussa 2021 asiakastietolain voimaantulon yhteydessä (1.11.2021)

Asiakirjamääräyksessä lähtökohtana on ollut, että...

- Määräyksessä 1/2021 (tai sen liitteissä) ei luetella niitä asiakirjoja, jotka tulee tallentaa Kanta-arkistoon vaan viitataan [Sosmetassa](#) julkaistaviin asiakirjoihin
 - ”Sosiaalihuollon asiakasasiakirjojen sisällön ja rakenteen tulee noudattaa Sosmeta-palvelussa julkaistuja asiakasasiakirjarakenteita viimeistään silloin, kun asiakasasiakirjat on asiakastietolain mukaan tallennettava valtakunnalliseen arkistointipalveluun. Sosiaalihuollon asiakastiedon arkistoon tallennettavien asiakasasiakirjojen laatimisessa tulee hyödyntää asiakirjarakenteen valmis-tilassa olevaa versiota. Lisäksi vanhentunut tilassa olevaa versiota voi käyttää erikseen määritellyn siirtymäkauden ajan.”
 - Käytetään Sosmetassa Valmis-tilassa julkaistuja rakenteita
 - Velvoittavuus asiakastietolain siirtymäsäännösten mukaan
 - Muutostilanteissa tuki olisi siirtymäajan myös edelliselle versiolle
 - ”Kun asiakirjarakenteesta julkaistaan uusi valmis-tilassa oleva versio, edellisestä versiosta tulee automaattisesti vanhentunut. Vanhentunut-tilaista asiakirjarakennetta tuetaan Kanta-palveluissa siirtymäkauden ajan.”
- Lisäksi tietenkin -> asiakirjojen tallennus tulee toteuttaa sitä koskevien olennaisten vaatimusten mukaisesti

Asiakirjarakenteet Sosmeta-palvelussa

- Asiakirjarakenteet julkaistaan THL:n ylläpitämässä [Sosmeta-palvelussa](#)
- Rakenteet ovat katseltavissa ja teknisesti ladattavissa Sosmetasta
- Asiakirjoja ei voi laatia palvelussa, vaan ne toteutetaan tietojärjestelmiin

Esimerkki asiakirjarakenteesta Sosmeta-palvelussa – Ilmoitus sosiaalihuollon tarpeesta:

ASIAKIRJARAKENNE

Ilmoitus sosiaalihuollon tarpeesta

Versio:

2021-01-05R2

OID:

1.2.246.537.6.1506.4006.2021.1.5

Tila:

VALMIS

Määritelmä:

ilman henkilön suostumusta palvelunjärjestäjälle tehty ilmoitus henkilön ilmeisestä sosiaalihuollon tuen tarpeesta

Tämä ilmoitus voidaan tehdä silloin, kun henkilö on ilmeisen kykenemätön vastaamaan omasta huolenpidostaan, terveydestään tai turvallisuudestaan tai koska lapsen etu sitä välttämättä vaatii eikä henkilön suostumusta yhteydenottoon sosiaalihuollosta vastaavaan viranomaiseen voida saada.

Asiakirjarakennemäärittely

Muutoshistoria

Ohjeet

Kontekstitiedot

Laajenna kaikki

1	+	Henkilö, josta ilmoitus tehdään	Yksityishenkilö	PAKOLLINEN	TOISTUVA
12	+	Ilmoittaja	Ilmoittaja		TOISTUVA
29		Ilmoittamispäivämäärä	Pvm		
30		Huoli, jonka takia ilmoitus sosiaalihuollon tarpeesta tehdään	Koodi		TOISTUVA
31		Kuvaus tilanteesta ja huolesta	Teksti	PAKOLLINEN	
32		Lisätiedot	Teksti		
33		Lakiselostus	Teksti		

Määräys 2/2021 Valtakunnallisten tietojärjestelmäpalveluiden avulla terveydenhuollon ulkopuolelle välitettävistä asiakirjoista

- koskee
 - (terveydenhuollon) palvelunantajia
 - todistuksia tuottavien palvelujen valmistajia / tietojärjestelmäpalvelujen tuottajia
 - kysely- ja välityspalvelun käyttöönottavia terveydenhuollon ulkopuolisia toimijoita,
 - kysely- ja välityspalvelun käyttöönottavien terveydenhuollon ulkopuolisten toimijoiden tietojärjestelmäpalvelujen tuottajia
 - Kelan Kanta-palveluita
- määrittelee, minkä tyyppisiä **terveydenhuollon** asiakirjoja saa välittää Kanta-palveluihin kuuluvan Kysely- ja välityspalvelun avulla
- sosiaalihuollon asiakirjojen välitystarpeita tarkennetaan myöhemmin
- määriteltyjä asiakirjoja saa välittää niille tahoille, joilla on **lainsäädännön perusteella oikeus** kyseisiin asiakirjoihin ja asiakirjojen tietosisältöihin
- välitys edellyttää
 - asiakkaan esittämää pyyntöä tai
 - vastaanottajan lakiin perustuvaa pyyntöä tai
 - tiedon luovuttajan lakiin perustuvaa tiedonantovelvollisuutta

Määräysluonnos 2/2021 – lausuntopyyntösivu

TIEDONHALLINTA
SOSIAALI- JA
TERVEYSALALLA

Ajankohtaista

Lausuntokierroksella

Sosiaalihuollon
asiakirjarakenteiden
kuulemiset 2019-2021

Lausuntopyyntö:
Määräys sosiaalihuollon
asiakasasiakirjojen
rakenteista ja
asiakasasiakirjoihin
merkittävistä tiedoista

**Määräysluonnos
valtakunnallisten
tietojärjestelmäpalvel-
uiden avulla
terveydenhuollon
ulkopuolelle
välitettävistä
asiakirjoista**

Määräysluonnos valtakunnallisten tietojärjestelmäpalveluiden avulla terveydenhuollon ulkopuolelle välitettävistä asiakirjoista

THL on valmistellut määräystä valtakunnallisten tietojärjestelmäpalveluiden avulla terveydenhuollon ulkopuolelle välitettävistä asiakirjoista.

Uusi laki Sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä kumooa THL:n aiemmin vuonna 2018 antaman määräyksen Valtakunnallisten tietojärjestelmäpalveluiden avulla terveydenhuollon ulkopuolisille toimijoille luovutettavista todistuksista ja lausunnoista.

Kumoutunut määräys korvataan uudella määräyksellä vastaamaan uuden asiakastietolain sisältöä.

Määräyksen on valmistellut THL:n asiantuntijat.

Lausuntoja pyydetään erityisesti:

- Kysely- ja välityspalvelun käyttöönottavilta terveydenhuollon ulkopuolisilta toimijoilta
- Kysely- ja välityspalvelun käyttöönottavien terveydenhuollon ulkopuolisten toimijoiden tietojärjestelmäpalvelujen tuottajilta
- Kysely- ja välityspalvelun kautta kyseltäviä ja välitettäviä asiakirjoja Kanta-palveluihin tuottavilta tietojärjestelmätoimittajilta
- Kelan Kanta-palvelujen asiantuntijoilta

3. Määräys asiakirjojen välittämisestä **LUONNOS**

Tämän määräyksen nojalla voidaan välittää ammattihenkilön antamia seuraavantyyppisiä todistuksia, lausuntoja ja asiakirjoja sekä niiden tietosisältöjä sosiaali- ja terveydenhuollon ulkopuolisille tahoille:

1. Lääkintölaillisia todistuksia ja lausuntoja sekä muita todistuksia, jotka vahvistetaan terveydenhuollon ammattihenkilöistä annetun lain 23 §:n mukaisesti
2. Muita lääkärintodistuksia ja lausuntoja, joissa selvitetään potilaan terveydentilaa ja jotka ovat välttämättömiä lausunnon vastaanottavan tahon tehtävien suorittamiseksi
3. Kuolemansyyn selvittämisestä annetun asetuksessa tarkoitettuja, THL:n hyväksymiä ja vahvistamia kuolintodistuksia
4. Muita terveydenhuollon asiakirjoja tai niiden määrättyjä tietosisältöjä, jotka ovat välttämättömiä vastaanottavan organisaation lakisääteisen tehtävän hoitamiseksi

Kysely- ja välityspalvelun kautta voidaan luovuttaa edellä lueteltujen todistusten, lausuntojen ja asiakirjojen liitteet.

Edellä luetellut todistukset, lausunnot ja asiakirjat tai niiden erikseen rajatut tietosisällöt saa välittää Kansaneläkelaitoksen (Kela) Kanta-palveluiden kysely- ja välityspalvelun avulla niille tahoille, joilla on lainsäädännön perusteella oikeus kyseisiin asiakirjoihin ja asiakirjojen tietosisältöihin. Välitys edellyttää asiakkaan esittämää pyyntöä tai vastaanottajan lakiin perustuvaa pyyntöä taikka tiedon luovuttajan lakiin perustuvaa tiedonantovelvollisuutta.

THL laatii todistusten, lausuntojen ja asiakirjojen tai niiden erikseen rajattujen tietosisältöjen välittämiseen liittyvät erilliset toimintamallit todistuksia, lausuntoja ja asiakirjoja laativille ja vastaanottaville toimijoille.

Määräys 6/2021 – Omatietovarantoon liitettävien hyvinvointitietoja käsittelevien hyvinvointisovellusten olennaisista vaatimuksista ja sertifiointista

Määräys 6/2021 osat:

- **LUONNOS** Määräys 6/2021 Omatietovarantoon liitettävien hyvinvointitietoja käsittelevien hyvinvointisovellusten olennaisista vaatimuksista ja sertifiointista
- **LUONNOS:** Määräys 6/2021 Liite 1: Olennaiset vaatimukset
- **LUONNOS:** Määräys 6/2021 Liite 2: Luokkaan A kuuluvien Omatietovarantoon liittyneiden hyvinvointisovellusten muutosten ilmoittaminen

Asiakastietolain määritelmiä:

- *hyvinvointitiedolla* henkilön **itsensä tuottamia** terveyttään ja hyvinvointiaan koskevia tietoja, jotka henkilö on tallentanut **omatietovarantoon**;
- *omatietovarannolla* **hyvinvointitietojen** säilyttämistä ja käsittelemistä varten valtakunnallisiin tietojärjestelmäpalveluihin muodostettua keskitettyä sähköistä tietovarantoa;
- *hyvinvointisovelluksella* yksityishenkilön käyttämää **omatietovarantoon liittyvää** sovellusta, jolla **käsitellään hyvinvointitietoja**, ja johon henkilö voi (myöhempien siirtymäsäännösten mukaisesti) saada asiakastietonsa arkistointipalvelusta, reseptikeskuksesta ja tiedonhallintapalvelusta;

Määräyksen 6/2021 merkitys

- Osa uudistuvan asiakastietolain (784/2021) toimeenpanoa
 - Hyvinvointitietojen käsittelyssä käytettävän hyvinvointisovelluksen tulee täyttää **yhteentoimivuutta, tietoturvaa ja tietosuojaa sekä toiminnallisuutta koskevat olennaiset vaatimukset** (34 §).
 - Hyvinvointisovelluksen tulee täyttää **saavutettavuusvaatimukset** (34 §).
 - Hyvinvointisovellukset **kuuluvat luokkaan A** (29 §)
 - Hyvinvointisovelluksen vaatimustenmukaisuus on osoitettava **sertifioinnilla** eli tietojärjestelmäpalvelun tuottajan tai hyvinvointisovelluksen valmistajan antamalla **selvityksellä** siitä, että tietojärjestelmä tai hyvinvointisovellus täyttää käyttötarkoituksensa mukaiset toiminnallisuutta koskevat vaatimukset, hyväksytyllä **yhteentoimivuuden testauksella** ja tietoturvallisuuden arviointilaitoksen antamalla **tietoturvallisuuden arviointia koskevalla todistuksella** (35 §).

Määräyksen 6/2021 sisällys (LUONNOS):

Sisällys

1. Määräyksen tarkoitus.....	3
2. Määräyksen soveltamisala	3
3. Määritelmät	3
4. Määräyksen keskeinen sisältö ja rajaukset	5
5. Sertifiointiprosessi	6
5.1 Sertifiointi- ja rekisteröintiprosessin vaiheet	6
5.2 Hyvinvointisovelluksen käyttöönotto ja käyttöönoton jälkeinen seuranta	8
5.3 Vaatimustenmukaisuuden uudistaminen	8
6. Olennaiset vaatimukset	8
6.1 Olennaisten vaatimusten osa-alueet.....	9
6.2 Vaatimusten todentamistavat	10
6.3 Merkittävät poikkeamat.....	11
7. Ohjaus ja neuvonta.....	12
8. Voimaantulo	12
Liitteet	13



Tietoturvasuunnitelma

Määräysluonnos 3/2021

Mikä tietoturvasuunnitelma?

Määräys 3/2021 on osa laajempaa määräysten kokonaisuutta, jolla toimeenpannaan uudistuvaa asiakastietolakia

- Uudessa **asiakastietolaissa** aiemman lain tietosuoja ja tietoturvallisuuden sekä tietojärjestelmien käytön omavalvontasuunnitelma **korvautuu tietoturvasuunnitelmalla**
- Sosiaali- ja terveydenhuollon toimijat **velvoitetaan laatimaan** tietoturvasuunnitelma
 - aiempi omavalvontasuunnitelma on pohja uuden lain mukaiselle tietoturvasuunnitelmalle
 - sisältö pääosin vastaava kuin aiemman lain edellyttämässä omavalvontasuunnitelmassa
- Suunnitelma edesauttaa asiakas- ja potilastietojen **turvallista** käsittelyä ja **parantaa** sote-toimijoiden **tietosuoja ja tietoturvaa**
- Määräys **tarkentaa** tietoturvasuunnitelmaan tarvittavien **selvitysten sisältöä** ja **tietoturvallisuudelle** sosiaali- ja terveyspalveluissa **asetettavia vaatimuksia**
- Uuden asiakastietolain ja määräysten kautta täsmennetään myös **tietojärjestelmiin kohdistuvien olennaisten vaatimusten toteutumista** sote-palveluiden järjestäjien ja tuottajien näkökulmasta
 - tietoturvasuunnitelma väline olennaisten vaatimusten täyttämisen varmistamisessa
- **Tietoturvasuunnitelma** on **Ei-julkinen** asiakirja
 - ”Tämän määräyksen mukaista tietoturvasuunnitelmaa ei tule sisällyttää tai yhdistää julkaistaviin tai julkisesti saatavilla oleviin omavalvontasuunnitelmiin.”
- Tietoturvasuunnitelma on hyvä käytännön työväline – kokoava dokumentti, ”**kokonaisturvallisuuden tilannekuva**”

Asiakastietolaki 27 § ja 28 §

Asiakastietolaki 27 §

Tietoturvasuunnitelma

Palveluntarjoajan, välittäjän ja Kansaneläkelaitoksen on laadittava tietoturvaan ja tietosuojaan sekä tietojärjestelmien käyttöön liittyvä tietoturvasuunnitelma.

Tietoturvasuunnitelmassa on oltava selvitykset, miten seuraavat asiakas- ja potilastietojen ja järjestelmien käsittelyyn liittyvät vaatimukset varmistetaan:

Asiakastietolaki 27 §:

- 1) ... käytön vaatima **koulutus**
- 2) ... asianmukaisen käytön kannalta tarpeelliset **käyttöohjeet**
- 3) ... **käytetään** tietojärjestelmäpalvelun tuottajan antaman **ohjeistuksen mukaisesti**
- 4) ... **ylläpidetään ja päivitetään** tietojärjestelmäpalvelun tuottajan ohjeistuksen mukaisesti
- 5) ... **käyttöympäristö soveltuu tietojärjestelmien** asianmukaiseen sekä **tietoturvan ja tietosuojan...**
- 6) ... liitetyt **muut tietojärjestelmät** tai muut järjestelmät **eivät vaaranna...suorituskykyä** eivätkä...
- 7) ... asentaa, ylläpitää ja päivittää vain **henkilö...** tarvittava **ammattitaito** ja **asiantuntemus**
- 8) 29 § Tietojärjestelmien ja hyvinvointisovellusten käyttötarkoitus ja luokittelu:
... **on jaoteltava** käyttötarkoitustensa ja ominaisuuksiensa perusteella **luokkiin** A ja B
34 § Tietojärjestelmälle ja hyvinvointisovellukselle asetettavat **olennaiset vaatimukset**
... Tietojärjestelmäpalvelun tuottajan on laadittava kuvaus...käyttötarkoituksesta...täyttää...olennaiset vaatimukset
- 9) ... palveluntarjoajalla, välittäjällä ja Kansaneläkelaitoksella on **suunnitelma**...omavalvonta **järjestetään** ja **toteutetaan** sen toiminnassa...

Asiakastietolaki 28 §

Tietoturvallisuuden omavalvonnan toteuttaminen ja vastuu
Sosiaali- ja terveydenhuollon palveluntarjoajan vastaavan johtajan on huolehdittava, että 27 §:ssä tarkoitettu tietoturvasuunnitelma laaditaan ja sitä noudatetaan. Vastaavan johtajan on annettava kirjalliset ohjeet asiakastietojen käsittelystä ja noudatettavista menettelytavoista sekä huolehdittava henkilökunnan riittävästä asiantuntemuksesta ja osaamisesta asiakastietojen käsittelyssä.



Järjestelmien luokittelu ja sertifiointi Sote-tietojärjestelmien olennaiset vaatimukset

Määräysluonnokset 4/2021 ja 5/2021

Määräysten 3, 4 ja 5 merkitys

3/2021 Määräys tietoturvasuunnitelmaan sisällytettävistä selvityksistä ja vaatimuksista

4/2021 Määräys sosiaali- ja terveydenhuollon tietojärjestelmien luokittelusta ja sertifiointista

5/2021 Määräys sosiaali- ja terveydenhuollon tietojärjestelmien olennaisista toiminnallisista ja tietoturvavaatimuksista

- Pohjautuvat **aiempiin** olennaisten vaatimusten, sertifiointin ja tietosuojan ja tietoturvallisuuden sekä omavalvonnan määräyksiin
- Luovat pohjaa **sote-uudistuksessa tarvittaville** tiedonhallinnan kyvykkyyksille asiakastietolain toimeenpanon lisäksi
 - Tarkentavat tietojärjestelmiin ja niiden kautta **tietojärjestelmäpalvelujen tuottajiin ja palvelunantajiin kohdistuvat olennaiset vaatimukset** (5)
 - Vahvistavat **tietoturvallisuuden ja tietosuojan** suunnittelun ja toteuttamisen käytäntöjä (3 ja 5)
- Ohjaavat tietojärjestelmiin (luokka A ja B) kohdistettavia **olennaisia vaatimuksia** (5 ja 4)
 - Eri käyttötarkoituksiin käytettävien sote-tietojärjestelmien kansalliset vähimmäisvaatimukset
 - Täsmentävät lain edellyttämän selvityksen olennaisten vaatimusten täyttämisestä
- Ohjaavat luokkaan A kuuluvien järjestelmien **sertifiointia** (4 ja 5)
 - Yhteentoimivuusvaatimusten todentaminen Kelan kanssa järjestettävässä yhteistestauksessa (luokka A2 ja A3)
 - Tietoturvavaatimusten todentaminen tietoturvallisuuden arviointilaitosten kanssa järjestettävässä auditoinnissa (luokka A1, A2 ja A3)
- **Ohjaavat palvelunantajia tietosuojan ja tietoturvallisuuden sekä tiedonhallinnan asianmukaisessa suunnittelussa ja toteuttamisessa** (3)
 - Sitoo yhteen sekä palvelunantajan omat käytännöt että kaikki käytössä olevat tietojärjestelmät ja ICT-palvelut kokonaisturvallisesti

Olennaisten vaatimusten ja sertifiointin keskeisiä muutoksia verrattuna aiempiin säädöksiin

HUOM. Tietojärjestelmän sertifiointista vastaa tietojärjestelmäpalvelun tuottaja!

- Järjestelmien **luokittelu** täsmentyy (B, A1, A2, A3)
 - Tietoturva-auditoidavaksi myös muuta kuin Kanta-palveluihin liittyviä järjestelmiä (A1)
 - Järjestelmien kriittisyyden, laajuuden, käsiteltyjen sisältöjen nykyistä tarkempi huomiointi vaatimusten kohdistamisessa ja todentamisessa
 - Ks. erityisesti määräys 4/2021 Liite 1
- Tietoturvavaatimukset osaksi **samaa perusrakennetta** kuin toiminnalliset vaatimukset (= toiminnot ja tietosisällöt)
 - Ei erillistä tietoturvavaatimusten määräystä, poistettu päällekkäisyyksiä
 - Tietoturvavaatimuksista oma osio olennaisten vaatimusten luokitukseen (ks. määräys 5/2021 Liite 2)
 - Tietoturvavaatimukset osaksi profiileja (= järjestelmän käyttötarkoituksen aiempaa parempi huomiointi)
 - Myös tekninen tietoturvatestausta kriittisimpien järjestelmien todentamistavaksi
- **Uusien järjestelmäratkaisujen** nykyistä parempi huomiointi, mm.
 - Pilvipalveluihin kohdistuvat tietoturvallisuusvaatimukset
 - Modulaariset järjestelmäkokonaisuudet, operatiivisen käytön tietoaltaat, jne.
- AsTL 34 §: **palvelunantajan käyttämien tietojärjestelmien** on vastattava käyttötarkoitukseltaan palvelunantajan toimintaa ja täytettävä palvelunantajan toimintaan liittyvät olennaiset vaatimukset
 - esim. suun terveydenhuollon palveluissa oltava käytössä Suun terveydenhuollon järjestelmäprofiilin mukaiset vaatimukset täyttävä järjestelmä

Rajauksia

- Asiakastietolain määräysten 1-5 kohdealueena asiakas- ja potilastietojen sähköinen käsittely
 - Määräysten kohderyhmänä erityisesti sote-palvelunantajat ja näille palveluja tuottavat tietojärjestelmäpalvelujen tuottajat
- Määräysten kohdealueena ei seuraavat
 - Lääkinnällisten laitteiden säädökset
 - Jos tietojärjestelmä täyttää lääkinällisen laitteen määritelmän, huomioitava sekä asiakastietolaki että lääkinällisten laitteiden säädökset
 - MDR-säädösten mukaiset menettelyt ovat kuitenkin hyödyllisiä myös asiakastietolain mukaisten vaatimusten täyttämässä (ja päinvastoin)
 - Toisiolain 552/2019 mukaiset käyttötarkoitukset, joihin tarvitaan tietolupa
 - Tieteellinen tutkimus, tilastointi, opetus, viranomaisen suunnittelu- ja selvitystehtävät
 - Joillakin tietojärjestelmillä voi olla sekä asiakastietolain mukaisia että toisiokäytön käyttötarkoituksia

Määräys 4/2021 sosiaali- ja terveydenhuollon tietojärjestelmien luokittelusta ja sertifiointista

- 1 Määräyksen tarkoitus
- 2 Määräyksen soveltamisala
- 3 Määritelmät
- 4 Määräyksen rajaukset ja suhde muihin määräyksiin ja dokumentteihin
- 5 Tietojärjestelmien luokittelu
- 6 Tietojärjestelmän käyttötarkoituksen kuvaaminen ja selvitys olennaisten vaatimusten täyttämisestä
- 7 Sertifiointiprosessi
 - 7.1 Sertifiointiprosessiin liittyvät velvoitteet
 - 7.2 Yhteistestauksen sisältö ja tulokset
 - 7.3 Tietoturvallisuuden arvioinnin sisältö ja tulokset
- 8 Tietojärjestelmän rekisteröinti
- 9 Tietojärjestelmän käyttöönotto
- 10 Vaatimustenmukaisuuden uudistaminen
- 11 Ohjaus ja neuvonta
- 12 Voimaantulo ja siirtymäsäännökset
- Liite 1 Esimerkkejä järjestelmien luokittelusta
- Liite 2 Luokkaan A kuuluvien sosiaali- ja terveydenhuollon tietojärjestelmien muutosten ilmoittaminen

LUONNOS

Määräys 5/2021 sosiaali- ja terveydenhuollon tietojärjestelmien olennaisista toiminnallisista ja tietoturvavaatimuksista

- 1 Määräyksen tarkoitus
- 2 Määräyksen soveltamisala
- 3 Määräyksen keskeinen sisältö ja rajaukset
- 4 Suhde muihin määräyksiin, ohjeisiin ja määrittelyihin
- 5 Olennaiset toiminnalliset vaatimukset
- 6 Olennaiset tietoturvallisuusvaatimukset
- 7 Vähimmäisvaatimusten profiilit
- 8 Olennaisten vaatimusten täyttäminen / tietojärjestelmäpalvelun tuottaja
- 9 Olennaisten vaatimusten täyttäminen / palvelunantaja
- 10 Olennaisten vaatimusten todentamisen tarkennuksia
 - 10.1 Vaatimusten täyttymisen arviointi järjestelmissä, jotka eivät liity Kanta-palveluihin
 - 10.2 Vaatimusten täyttymisen arviointi ja todentamistavat sertifiointissa
 - 10.3 Vaatimusten ja määrittelyjen versionhallinta
 - 10.4 Poikkeamat vaatimustenmukaisuudesta
- 11 Ohjaus ja neuvonta
- 12 Voimaantulo ja siirtymäsäännökset
- Liite 1 Olennaisten vaatimusten soveltamisohjeet
- Liite 2 Olennaisten vaatimusten luokitus
- Liite 3a-3g Vähimmäisvaatimusten profiilit
- Liite 4 Järjestelmälomake

LUONNOS

Tietoturvavaatimusten uudistukset

Määräys 5/2021 Liite 2, osio Tietoturvavaatimukset

- Sisällöllisiä täsmennyksiä ja täydennyksiä
 - 2015 jälkeen uudistuneista säädöksistä nousevat tarkennukset
 - Sertifiointiprosessin soveltamisesta esiin nousseet tarkennustarpeet
 - Tietoturva- ja tietosuojapoikkeamista esiin nousseet tarkennustarpeet
- Uusia ja tarkentuneita vaatimuksia (Määräys 5 liite 2 / Tietoturvavaatimukset)
 - Mm. pilvipalveluihin liittyvät vaatimukset Pitukri-kriteeristöä soveltaen, mm.
 - AKYM07 kovennus, AKYM08 haittaohjelmasuojaus, AKYM 09 pilvipalvelut järjestelmäkuvaus, AKYM10 riskit ja sopimukset
 - AKYM11 varautumisen näkökulmasta suojattavat tiedot, AKYM12 fyysinen sijaintirajaus
- Profiilit ja järjestelmälomake selkeämmin ohjaamaan myös tietoturva-auditointia
 - Järjestelmä tietyn profiilin mukainen → ainakin profiilin mukaiset tietoturvavaatimukset todennettava
 - Aiempien tietoturvavaatimusten normalisointi suhteessa toiminnallisiin vaatimuksiin
- Sertifioinnin todentamistapoihin tarkennuksia
 - Haastattelut eivät enää missään vaatimuksessa ensisijainen todentamistapa
 - Tietoturva-auditointiin mukaan tekninen tietoturvatestaus (luokka A3 ja laajat luokan A1 järjestelmät)
- Erityisesti käyttöympäristön vaatimukset olennaisia myös tietoturvasuunnitelmien (Määräys 3/2021) näkökulmasta

LUONNOS

Olennaisten vaatimusten profiilit

Määräys 5/2021 liitteet 3a-3g

- Kansallisten vähimmäisvaatimusten koonti aihekohtaisesti – profiilin mukaiset vaatimukset toteutettava järjestelmissä, joissa profiilin mukainen käyttötarkoitus
- Yhdessä järjestelmässä voi olla toteutettuna useita profiileja
 - 3a Sähköisen reseptin profiilit (2 profiilia)
 - 3b Kanta-arkistopalveluihin liittyvien järjestelmien vähimmäisvaatimusprofiilit (4 profiilia)
 - 3c Potilastiedon arkiston profiilit (3 profiilia, joista 1 UUSI)
 - 3d Sosiaalihuollon asiakastiedon arkiston profiilit (julkaistaan myöhemmin)
 - 3e Kuvantamisen profiilit (3 vanhaa vai 5 UUTTA profiilia)
 - 3f Todistusten profiilit (3 profiilia)
 - 3g Asiakas- tai potilastietojen käsittelyyn tarkoitettun järjestelmän vähimmäisvaatimukset (sis. luokka B tai A1) (1 UUSI profiili)

LUONNOS

Järjestelmälomake

Määräys 5/2021 Liite 4

- Lomakepohja, valmistaja / tietojärjestelmäpalvelun tuottaja täyttää
- Käytännön työkalu rekisteröintiin ja sertifiointiin
- Toimii osana järjestelmän käyttötarkoituksen kuvaamista
 - Muodostaa asiakastietolain edellyttämän selvityksen toiminnallisten vaatimusten täyttämistä
- Järjestelmän perustietojen kuvaus
- Järjestelmän käyttötarkoituksen tiivis kuvaus
- Tieto siitä, minkä kansallisten profiilien mukainen käyttötarkoitus järjestelmällä on
 - Niiden kansallisesti julkaistujen profiilien luettelo, joiden mukaiset vähimmäisvaatimukset järjestelmän kautta täytetään
- Järjestelmän käyttötarkoituksen tarkempi kuvaus
 - **Toiminnot** jotka ovat osa järjestelmän käyttötarkoitusta
 - **Tietosisällöt** jotka ovat osa järjestelmän käyttötarkoitusta
 - **Tietoturva-vaatimukset**, jotka täytetään järjestelmän kautta
- Suoraviivaistaa ilmoituksia Valviran rekisteriin (A ja B-luokka), Kelan yhteistestausta (A2 ja A3-luokka) ja tietoturvallisuuden auditointia (A1, A2 ja A3-luokka)
- Ohjaa luokituksen kautta tarkempiin määrittelyihin
- **PÄIVITETTY** versio määräyksen 5/2021 yhteydessä

Yhteenveto määräyksistä 5,4 ja 3/2021: Olennaisten vaatimusten, luokittelun ja sertifiointin määräykset – **tukevat:**

- **Tukevat tietojärjestelmien valmistajia ja tietojärjestelmäpalvelujen tuottajia** lakisääteisten vaatimusten täyttämässä ja tulkitsemisessa sekä omien ratkaisujen toiminnallisten ominaisuuksien määrittelemisessä suhteessa määrittelyihin
 - myös suhteessa kumppaneihin ja työnjakoon eri järjestelmien välillä
 - sama järjestelmälomake yhteistestauksessa, auditoinnissa ja rekisteri-ilmoituksissa
- **Tukevat sote-toimijoita** omien tietojärjestelmäratkaisujensa olennaisten vaatimusten täyttämässä, ml. sote-uudistuksen ja hyvinvointialueiden järjestäjät ja tuottajat
 - mm. riskienhallinta, toimialasidonnaisten tietojärjestelmien keskeiset ominaisuudet
- Selkeyttävät **valtakunnallisten palvelujen kehittämiseen liittyvien määrittelyjen ja niihin liittyvien kehitys-, testaus- ja sertifiointitoimenpiteiden** rakennetta
 - mukaan lukien muutoshallinta ja riippuvuuksien hallinta
- **Tukevat** sitä, että sote-toiminnan kokonaissuunnittelussa huomioidaan tarvittavat tietojärjestelmä-, tietosuoja- ja tietoturva-asiat
 - [tietoturvallisuuden, tietosuojan ja tiedonhallinnan jatkumon ”yhteen solmiminen” tapahtuu sote-palvelujen päivittäisessä toiminnassa!](#)

Olennaisten vaatimusten määräys – olennaista tietojärjestelmäpalvelun tuottajan näkökulmasta

- Tietojärjestelmäpalvelun tuottajan ja valmistajan perusvastuut ja pääosa vaatimuksista eivät muutu aiemmasta
 1. Kuvaa järjestelmän käyttötarkoitus ja määrittele järjestelmän luokka
 2. Perehdy olennaisiin vaatimuksiin
 - Mitkä profiilit ja vaatimukset (5/2021) relevantteja järjestelmän käyttötarkoituksen näkökulmasta? - dokumentoi järjestelmälomakkeella
 - Hyödynnä vaatimukset kokoava materiaali
 3. Huomioi relevantit olennaiset vaatimukset järjestelmän suunnittelussa, toteuttamisessa, dokumentaatiossa, ohjeistuksissa
 4. Testaa itse ja varmista laatu, turvallisuus ja vaatimustenmukaisuus
 5. Sertifioi järjestelmä, jos se kuuluu luokkaan A
 6. Tee ilmoitus Valviran tietojärjestelmärekisteriin ennen tuotantokäyttöönottoa
 7. Huomioi vastuut ja vaatimukset sopimuksissa (asiakassopimukset, kumppanuudet)
 8. Huolehdi muutoshallinnasta ja päivityksistä sekä olennaisten vaatimusten seurannasta



Kiitos!