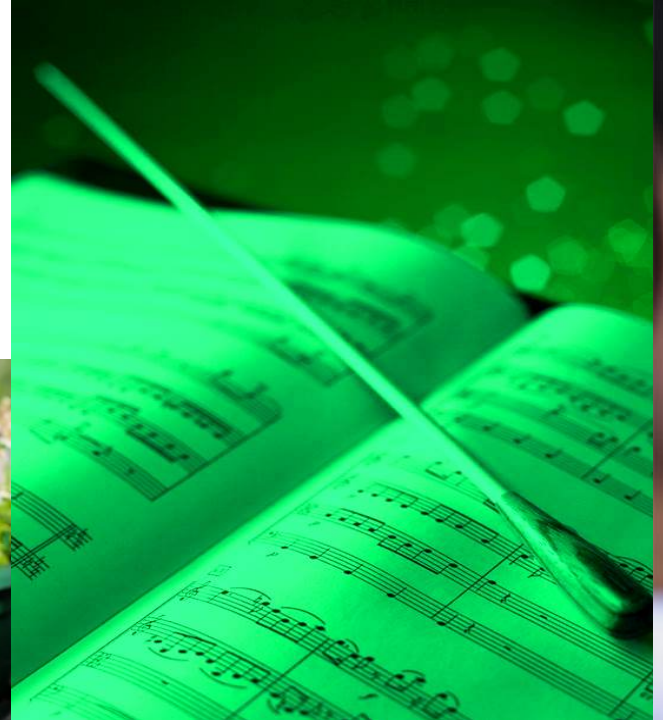


Sote-tietojärjestelmien olennaiset vaatimukset ja sertifiointi

Koulutus 15.12.2021

Sote-tiedonhallinnan määräykset 2021 -projektin ja valmistelutyöryhmän puolesta

Juha Mykkänen, johtava asiantuntija

Terveyden ja hyvinvoinnin laitos

Sote-tietojärjestelmien olennaiset vaatimukset ja sertifiointi – koulutus

Ohjelma

- klo 13:00-13:10
  Tilaisuuden avaus
- klo 13:10-14:20
  Olennaiset vaatimukset ja sertifiointi - Juha Mykkänen, THL
  - **THL määräykset 4/2021 ja 5/2021**
  - perusteet ja rajaukset
  - järjestelmien luokittelu ja riskitaso
  - sertifiointiprosessi
  - olennaiset vaatimukset
  - erityiskysymyksiä
  - muutokset aiempiin säädöksiin ja luonnoksiin
- klo 14:20-14:35
  Tauko
- klo 14.35-15.05
  Yhteistestaus sertifiointiprosessin osana - Laura Klemetti, Kela
- klo 15.05-15.50
  Tietojärjestelmien rekisteri ja valvonta - Antti Härkönen, Valvira
- klo 15.50-16.00 Yhteenveto, keskustelu ja kysymykset

Uusia ja vanhoja riskejä ja uhkia…

POTILASTIETOJÄRJESTELMÄT

Potilastietojärjestelmien päivitys ongelmissa Kanta-Hämeessä: ajanvaraustekstiviestit eivät kulje ja terveysasemille vain kiireellisissä tapauksissa

Potilastietojen kirjaamisen hidastuminen vaikuttaa useaan toimintoon Hämeenlinnan ja Riihimäen alueella.

Ovatko henkilökohtaiset terveystiedot turvassa? - Yhdysvalloissa 29 miljoonaa tietorikkom

TIETOSUOJARIKOS

Yksi klikkaus maksoi sosiaalialan työntekijöille 4800 euroa – tutkivat vieraan perheenäidin tietoja, kun tämä istui kampaajalla

Jokaisella on oikeus tietää omi

käsittelystä. P

TIETOTURVA

Massivinen kyberhyökkäys – rikollisliiga väittää lukinneensa miljoona tietokonetta, vaatii kymmenien miljoonien lunnaita

REvil-verkkorikollisryhmä iski amerikkalaisen pilvipalveluntarjoajan järjestelmiin.

Rovaniemi tänään

It-vika pysäytti Lapin keskussairaalan

Lapin kesku

poliklinikkak

tietojärjestel

Vika havaittiin t

VASTAAMON TIETOMURTO

Psykoterapiakeskus Vastaamon kiristäjä julkaisi yöllä lisää erittäin arkaluontoisia potilaskertomuksia

retaan henkilötietoja ja hyvin intiimejä tietoja terveyden ongelmista.

TIETOTURVA

Kyberhyökkäys kaatoi Irlannin terveydenhuollon – tietokoneet pimeinä sairaalassa

Vain koronarokotusohjelm

terveyden

TIETOTURVA

Onko kiinalainen puhelin vaarallinen? Näin kommentoivat viranomainen ja tietoturva-asiantuntija

Liettualaisten löydökset herättivät pelkoa kiinalaispuhelimiin. Asiantuntijoiden mukaan kyse ei ole yhteen maahan liittyvästä ongelmasta. Kuluttajan asema on kuitenkin vaikea.

IETOSUOJA

Tyhjistä sairaalatiloista löytyi taas salaiseksi tarkoitettuja tietoja – TAYS: "Jossakin prosessi oli katkennut"

Lukituista tiloista löytynyt tietosuojattava materiaali on tuhottu ja tietoturvaloukkauksista on tehty ilmoitukset tietosuojavaltuutetun toimistoon.

TIETOTURVA

Karmea saldo yhdelle päivälle: Kiristäjät iskivät 6 sairaalaan

Verkkokiristyksen iljettävä muoto on yleistynyt Yhdysvalloissa ja

ihmishenkiä.

Azure-käyttäjille: pilvikontissa oli vuoto

9.9.2021 13:08 | päivitetty 9.9.2021 13:08

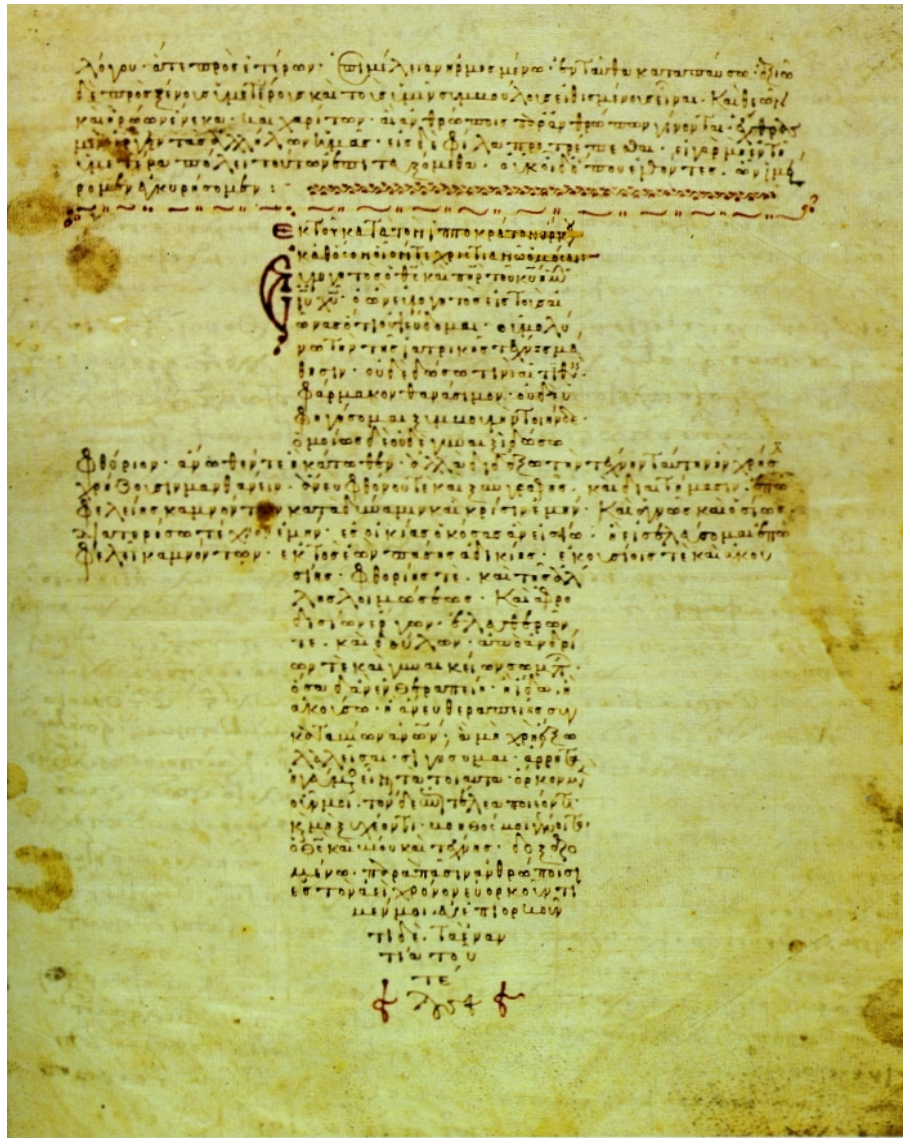
zuren konttipalvelun aukko on onneksi jo korjattu.

…mutta perusasiat pysyvät.

Hippokrateen vala, ote:

”Mikäli parannustyössäni tai sen ulkopuolella ihmisten keskuudessa näen tai kuulen sellaista, mitä ei pidä levitettämän, vaikenen ja pidän sen salaisuutena.”

- Hippokrates (n. 460-370 eKr)



Johdanto

- Sote-palvelut nojautuvat entistä enemmän sähköiseen tiedonhallintaan
- Suomessa on tehty kansainvälisesti vertaillen pitkäjänteistä lainsäädäntö-, strategia- ja kehitystyötä ja panostettu palvelujen ja tuotteiden innovatiiviseen kehittämiseen sekä kansallisesti, alueellisesti että paikallisesti
- Sote-palvelujen kehittäminen ja palvelujen uudistaminen edellyttävät
  - Jatkuvaa aktiivista kehittämistä
  - Yhteentoimivuudesta huolehtimista
  - Tietoturvallisuudesta ja tietosuojasta huolehtimista
  - Kansainvälisten standardien ja suositusten hyödyntämistä
  - Kansallista ohjausta
  - Laajaa yhteistyötä tietojärjestelmäratkaisujen kehittämisessä

Olennaiset vaatimukset ja sertifiointi yksi keskeinen keino näiden tavoitteiden edistämiseen

Sote-tiedonhallinnan määräykset 2021

THL antaa vuonna 2021 **kuusi** määräystä sosiaali- ja terveydenhuollon tiedonhallinnan kokonaisuudesta vuoden loppuun mennessä. Määräyksillä ohjataan **asiakastietolain** 784/2021 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 sertifioinnista
5. Määräys sosiaali- ja terveydenhuollon tietojärjestelmien olennaisista toiminnallisista ja tietoturvavaatimuksista
6. Määräys omatietovarantoon liitettävien hyvinvointitietoja käsittelevien hyvinvointisovellusten olennaisista vaatimuksista ja sertifioinnista

- Määräykset julkaistu / julkaistaan THL:n tiedonhallinnan sivustolla ja viranomaisten säädöskokoelmassa
- Lausuntoajat päättyivät lokakuun loppuun mennessä, jonka jälkeen määräykset liitteineen viimeistelty
- **KIITOKSET runsaasta palautteesta ja kehittämisehdotuksista!**

Iltapäivän fokus

- Sote-tietojärjestelmien **olennaiset vaatimukset** ja niiden **todentaminen ja sertifiointi**
  - Kansalliset ”vähimmäisvaatimukset” eri käyttötarkoituksiin tehdyille järjestelmille
  - Fokus: sosiaali- ja terveydenhuollon asiakastietojen käsittelyyn tarkoitetut järjestelmät
    - Kanta-palveluihin liittyvät
    - Muut potilastietojen ja sosiaalihuollon asiakastietojen käsittelyyn tarkoitetut
  - Erityisesti järjestelmien valmistajiin ja tietojärjestelmäpalvelujen tuottajiin kohdistuvat vaatimukset
  - Sekä julkisissa että yksityisissä palveluissa käytettävät tietojärjestelmät
  - Sekä sosiaali- että terveyspalveluissa käytettävät tietojärjestelmät
- **Oppimistavoitteet:** 1) yleiskuva, 2) tieto aiempiin säädöksiin verrattuna muuttuneista asioista ja 3) lisätietojen löytämisen helpottaminen
- Rajaukset päivän ohjelmassa
  - pääfokus tilaisuudessa tänään sote-ammattilaisten käyttämät järjestelmät, ei asiakkaille tarjottavat sähköiset palvelut tai hyvinvointitietoja käsittelevät hyvinvointisovellukset
  - sote-palveluntuottajien tietoturvasuunnitelmat ja siihen liittyvät tietosuoja- / tietoturvallisuusasiat eivät ole pääaiheena (tästä aiheesta tulossa erillisiä koulutuksia)
  - ei käsitellä yksityiskohtaisesti lääkinnällisten laitteiden säädöksiä (mm. MDR, ISO 13485) tai niihin liittyviä menettelyjä: huomioitava erikseen
  - asiakastietolain määräysten kohteena ei toisiolain mukaiset tietojen käyttötarkoitukset

Asiakastietolaki 784/2021

- 34 § Asiakastietojen käsittelyssä käytettävän tietojärjestelmän tulee täyttää yhteentoimivuutta, tietoturvaa ja tietosuojaa sekä toiminnallisuutta koskevat **olennaiset vaatimukset**
  - Mitä olennaiset vaatimukset ovat ja miten ne täytetään?
  - Mitkä olennaiset vaatimukset koskevat järjestelmääni?
- 35 § Luokkaan A kuuluvan tietojärjestelmän vaatimustenmukaisuus on osoitettava **sertifioinnilla** eli tietojärjestelmäpalvelun tuottajan antamalla **selvityksellä** siitä, että tietojärjestelmä täyttää käyttötarkoituksensa mukaiset toiminnallisuutta koskevat vaatimukset, hyväksytyllä **yhteentoimivuuden testauksella** ja 37 §:n mukaisella tietoturvallisuuden arviointilaitoksen antamalla **tietoturvallisuuden arviointia koskevalla todistuksella**. Luokkaan B kuuluvan tietojärjestelmän vaatimustenmukaisuus on osoitettava tietojärjestelmäpalvelun tuottajan antamalla **kirjallisella selvityksellä** siitä, että tietojärjestelmä asianmukaisesti asennettuna, ylläpidettynä ja käytettynä täyttää käyttötarkoituksensa mukaiset olennaiset vaatimukset
  - Mihin luokkaan järjestelmäni kuuluu?
  - Miten mainittu selvitys annetaan?
  - Millainen prosessi sertifiointi on?
  - Mitä yhteistestaukseen kuuluu?
  - Mitä tietoturvallisuuden arviointiin kuuluu?

Määräykset osana säädösten toimeenpanoa

Sote **toiminnan ja käytäntöjen** seuranta, arviointi, kehittäminen ja asiantuntijatuki [THL-laki 2§2]

Rekisterien ja tietoperustan ylläpito [THL-laki 2§4]

Sote-asiakastiedon **sähköisen käsittelyn ja tietohallinnon sekä tietojärjestelmäpalvelujen** suunnittelu, ohjaus, seuranta [THL-laki 2§4b, AsTL 39§]

Sote-alan keskeiset **termit, määritykset ja luokitukset** kehittäminen ja ylläpito [THL-laki 2§5]

Tiedonsaantioikeus, päätökset **tiedonkeruista**, määräykset **laaturekistereista** [THL-laki 5§]

Määräykset mitkä asiakirjat saa **luovuttaa kysely- ja välityspalvelun avulla** [AsTL 22§]

Määräykset **valtakunnallisten tietojärjestelmäpalvelujen** edellyttämistä **tietosisällöistä, tietorakenteista, koodistoista** [AsTL 9§]

Koodistopalvelun sisältöjen ylläpito ja jakaminen [AsTL 6§]

Määräykset **toiminnallisuutta, yhteentoimivuutta, tietoturvaa ja tietosuojaa koskevista tietojärjestelmien olennaisista vaatimuksista** [AsTL 34§]

Määräykset **tietojärjestelmien luokittelusta** ja **vaatimustenmukaisuuden menettelyistä** ja merkittävistä **poikkeamista** [AsTL 29§, 32§, 35§]

Määräykset **tietosuojan ja tietoturvallisuuden** ja järjestelmien käytön **omavalvontasuunnitelmasta** [AsTL 27§]

Määräykset **sosiaalihuollon asiakasasiakirjojen rakenteista ja tiedoista** [Laki sos.h. asiakasasiakirjoista 5§9]

Olennaiset vaatimukset ja sertifiointi

Perusteet ja rajaukset

Olennaiset vaatimukset ja tietoturvasuunnitelmat: miksi?

- Lainsäädäntöön tehtiin vuonna 2014 merkittäviä muutoksia sekä sote-palvelujen tuottajille että järjestelmätoimittajille, päivitys ja tarkennuksia vuonna 2021
- Varmistettava, että
  - Järjestelmissä on käyttötarkoituksensa kannalta oikeat toiminnallisuudet, riittävät tietoturvaominaisuudet ja että ne pystyvät liittymään osaksi Kanta-palvelujen kautta tapahtuvaa tietojen vaihtoa

    → tietojärjestelmien **OLENNAISET VAATIMUKSET**
  - Sote-organisaatioissa ja palveluntuottajilla on asianmukaiset tietoturvakäytännöt ja käyttöympäristössä huolehditaan asianmukaisesta tietoturvasta

    → **TIETOTURVASUUNNITELMAT ja niiden omavalvonta**
  - Erityishuomio Kanta-palvelujen kautta edelleen laajenevassa tietojen saatavuudessa, mutta myös muu asiakastietojen sähköinen käsittely säädösten kohteena

Olennaisten vaatimusten säädökset

- Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä 784/2021 (aiempi 159/2007, päivitetty myös 2014)
- Laki sähköisestä lääkemääräyksestä 61/2007 (päivitetty myös 2014 ja 2021)
- Määräykset:
  - THL:n määräys 4/2021: Määräys sosiaali- ja terveydenhuollon tietojärjestelmien luokittelusta ja sertifioinnista
  - THL:n määräys 5/2021: Määräys 5/2021: Määräys sosiaali- ja terveydenhuollon tietojärjestelmien olennaisista toiminnallisista ja tietoturvavaatimuksista
  - THL:n määräys 3/2021: Tietoturvasuunnitelmaan sisällytettävät selvitykset ja vaatimukset
  - (korvaavat aiemmat määräykset 1/2015, 2/2015, 2/2016)
- Lisäksi saatavilla ja tulossa ohjeita ja tukimateriaalia

Asiakastietolain avainkohdat järjestelmien luokittelun, olennaisten vaatimusten ja sertifioinnin näkökulmasta

- 3 § **Määritelmät**
- 27 § Tietoturvasuunnitelma
- 29 § Tietojärjestelmien ja hyvinvointisovellusten **käyttötarkoitus** ja **luokittelu**
- 30 § Tietojärjestelmien ja hyvinvointisovellusten **rekisteröinti**
- 31 § Tietojärjestelmän ja hyvinvointisovelluksen **ottaminen tuotantokäyttöön**
- 32 § Tietojärjestelmän ja hyvinvointisovelluksen **käyttöönoton jälkeinen seuranta**
- 33 § **Tietojärjestelmäpalvelun tuottajan ja valmistajan** sekä hyvinvointisovelluksen valmistajan yleiset velvollisuudet
- 34 § Tietojärjestelmälle ja hyvinvointisovellukselle asetettavat **olennaiset vaatimukset**
- 35 § **Vaatimustenmukaisuuden osoittaminen**
- 36 § **Yhteentoimivuuden testaaminen**
- 37 § **Tietoturvallisuuden arviointi**
- 38 § Tietoturvallisuuden arviointilaitoksen ilmoittamisvelvollisuus
- 39 § **Ohjaus, valvonta ja seuranta**
- 40 § Tietojärjestelmien valvonta ja tarkastukset
- 41 § Ilmoittaminen tietojärjestelmän **olennaisten vaatimusten poikkeamista**
- 52 § Siirtymäsäännökset

Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä

Lähtökohtia – nostoja määritelmistä / AsTL 3 §

- ***tietojärjestelmä*** on *”valmistajan suunnittelemien ominaisuuksien mukaisesti tarkoitettu käytettäväksi asiakastietojen sähköiseen käsittelyyn, asiakasasiakirjojen tallentamiseen ja ylläpitoon tai valtakunnallisiin tietojärjestelmäpalveluihin liittämiseen tai jolla sosiaali- ja terveydenhuollon ammattihenkilö voi hyödyntää hyvinvointitietoja”*
- ***tietojärjestelmän valmistaja*** on taho, joka *”on vastuussa sosiaali- ja terveydenhuollon tietojärjestelmän suunnittelusta ja valmistuksesta”*
- ***tietojärjestelmäpalvelun tuottaja*** on taho, joka *”tarjoaa tai toteuttaa palvelunantajalle tietojärjestelmää, jossa käsitellään asiakas- tai hyvinvointitietoa, ja joka vastaa tietojärjestelmän valmistajana, valmistajan lukuun tai yhden tai useamman valmistajan puolesta tietojärjestelmälle asetetuista vaatimuksista”*
- ***sertifiointi*** on menettely, *”jolla todennetaan tietojärjestelmän tai hyvinvointisovelluksen täyttävän sitä koskevat tuotantokäyttöä varten vaadittavat olennaiset vaatimukset”*

Asiakastietolaki 33 § - Tietojärjestelmäpalvelun tuottajan ja valmistajan sekä hyvinvointisovelluksen valmistajan yleiset velvollisuudet

- Tietojärjestelmän valmistaja on vastuussa sosiaali- ja terveydenhuollon tietojärjestelmän **suunnittelusta ja valmistuksesta** riippumatta siitä, suorittaako se nämä toimet itse vai tekeekö joku muu ne sen lukuun
- Tietojärjestelmäpalvelun tuottajan on laadittava **kuvaus tietojärjestelmänsä käyttötarkoituksesta** ja annettava sen yhteydessä järjestelmän käyttäjälle yhteentoimivuuden, tietoturvallisuuden ja tietosuojan sekä toiminnallisuuden kannalta tarpeelliset tiedot ja ohjeet järjestelmän käyttöönotosta, tuotantokäytöstä ja ylläpidosta
- Tietojärjestelmän mukana annettavien tietojen ja ohjeiden on oltava suomen-, ruotsin- tai englanninkielisiä
- Tietojärjestelmää käyttävälle sosiaali- tai terveydenhuollon henkilöstölle tarkoitettujen tietojen ja ohjeiden on oltava suomen- tai ruotsinkielisiä
- Tietojärjestelmän valmistajalla on oltava **laatujärjestelmä**, jota sovelletaan tietojärjestelmän suunnitteluun ja valmistukseen tietojärjestelmän käyttötarkoituksen edellyttämällä tavalla

Asiakastietolaki 29 § ja 34 §: sote-tietojärjestelmien käyttötarkoitus ja olennaiset vaatimukset

- **I Toiminnalliset vaatimukset**
  - Kuvattava **käyttötarkoitus** ja **luokiteltava järjestelmä**
  - Tietojärjestelmäpalvelun tuottajan annettava **selvitys** toiminnallisten vaatimusten täyttymisestä (A- ja B-luokan järjestelmät)
  - Vaatimusten täyttyminen osoitetaan tietojärjestelmäpalvelun tuottajan antamalla selvityksellä
  - *Määräysten 4-5/2021 kautta selvitys annetaan vertailtavalla tavalla ja sertifiointia / rekisteröintiä tukien*
- **II Yhteentoimivuuden vaatimukset**
  - *Todennetaan* luokan A2 ja A3 järjestelmille (Kanta-palveluihin liittyvät) **Kelan yhteistestauksen** kautta
- **III Tietoturvavaatimukset**
  - *Todennetaan* luokan A (A1, A2, A3) järjestelmille tietoturvallisuuden arviointilaitoksen suorittamassa **tietoturvallisuuden arvioinnissa**
- Yhteentoimivuuden ja tietoturvallisuuden vaatimukset nojautuvat toiminnallisiin vaatimuksiin
  - käyttötarkoitus ja siitä annettu kuvaus, järjestelmää koskevat olennaiset vaatimukset

Olennaisten vaatimusten todentamisesta vastaa tietojärjestelmäpalvelun tuottaja tai valmistaja
Palvelunantajan on varmistettava olennaisten vaatimusten toteutuminen käyttämissään tietojärjestelmissä

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

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

HUOM. Tietojärjestelmän luokittelusta ja sertifioinnista vastaa tietojärjestelmäpalvelun tuottaja!

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 määrityksiin

5 Olennaiset **toiminnalliset vaatimukset**

6 Olennaiset **tietoturvavaatimukset**

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** sertifioinnissa
- 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**

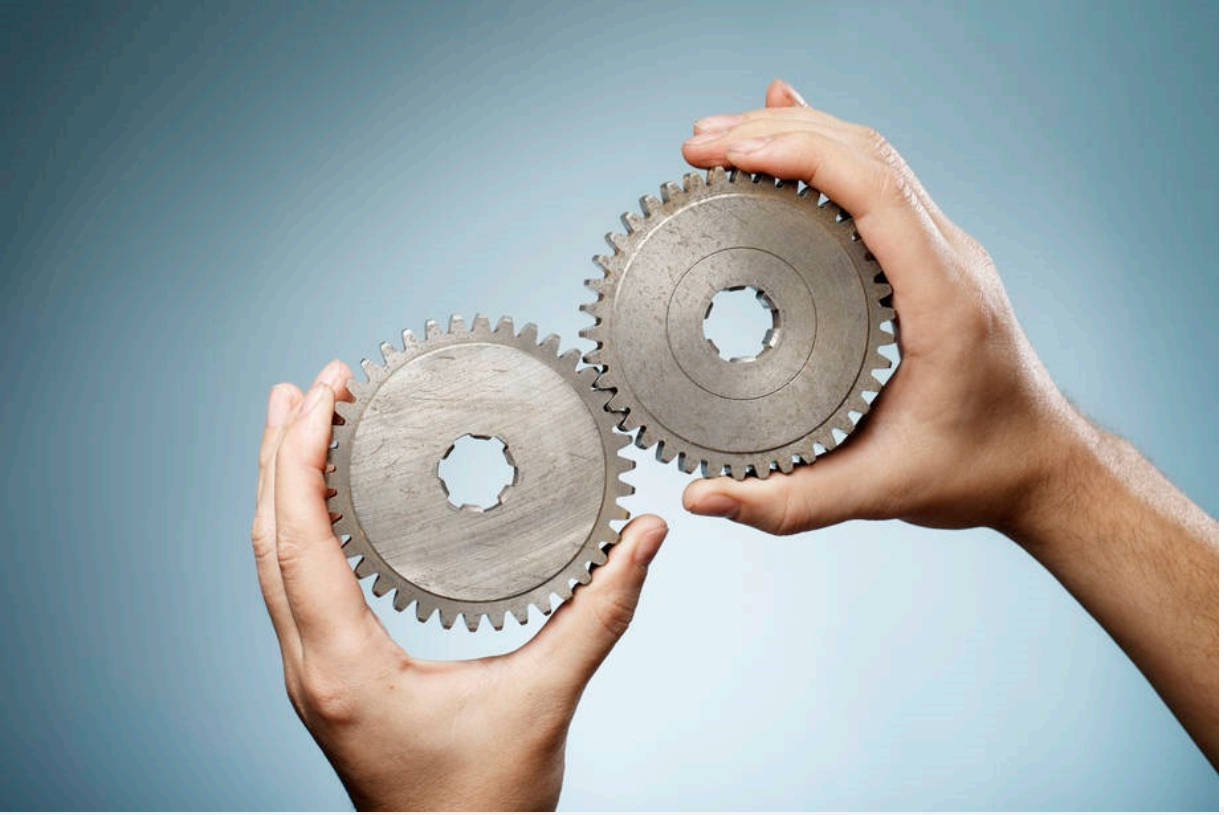
Liite 3a-3g Vähimmäisvaatimusten **profiilit**

Liite 4 **Järjestelmälomake**

Olennaisten vaatimusten toteuttamisesta tietojärjestelmään ja todentamisesta vastaa valmistaja / tietojärjestelmäpalvelun tuottaja
Palvelunantajan osaltaan huolehdittava että käytetyt tietojärjestelmät täyttävät olennaiset vaatimukset ja vastaavat palvelunantajan toimintaa

Rajauksia / määräykset 4/2021 ja 5/2021

- Määräykset 4/2021 ja 5/2021 kohdistuvat tietojärjestelmiin, ei hyvinvointisovelluksiin (joille määräys 6/2021)
- Määräykset eivät vaikuta esim. asiakastietolaissa asetettuihin sote-toimijoiden Kanta-liittymisvelvoitteiden aikatauluihin
- Määräykset kohdistuvat asiakastietolain määritelmän mukaisiin tietojärjestelmiin
  - Tietojärjestelmä tai osa sitä voi olla myös lääkinnällisten laitteiden säädösten tarkoittama lääkinnällinen laite, jolloin valmistajan huomioitava lääkinnällisten laitteiden säädösten mukaiset luokittelut ja vaatimukset – tämä arviointi riippumaton esim. asiakastietolain mukaisesta luokittelusta
    - MDR-säädösten mukaiset menettelyt ovat kuitenkin hyödyllisiä myös asiakastietolain mukaisten vaatimusten täyttämisessä (ja päinvastoin)
  - Sertifioitavia tietojärjestelmiä eivät myöskään ole yleiskäyttöiset ohjelmistot tai alustat itsessään
- Asiakastietojärjestelmien sertifioinnissa ei ole kyse EU:n yleisen tietosuoja-asetuksen mukaisesta rekisterinpitäjään tai henkilötietojen käsittelijän sertifioinnista
- Toisiolain mukaiset käyttötarkoitukset ja Findatan määräys tietoturvallisten käyttöympäristöjen vaatimuksista eivät asiakastietolain nojalla annettujen määräysten piirissä: tieteellinen tutkimus, tilastointi, opetus, viranomaisen suunnittelu- ja selvitystehtävät



Järjestelmien luokittelu ja riskitaso

Sote-tietojärjestelmien riskit ja niihin varautuminen

- Terveys- ja hyvinvointiriskit, potilasturvallisuus (safety): sovellukset ohjaavat vääränlaiseen käyttäytymiseen tai toimivat virheellisesti aiheuttaen suoraan tai välillisesti haittaa tai riskejä asiakkaille
- Tietosuojariskit (privacy): asiakkaan tiedot karkaavat sivullisille
- Tietoturvallisuusriskit (security)
- Riskit sote-palvelujen toimivuuden tai sujuvuuden näkökulmasta (mm. yhteentoimivuus)
- Varautuminen poikkeustilanteisiin
- Varautuminen väärinkäytöksiin
- Varautuminen ohjelmistovirheisiin
- Lainsäädäntöön liittyvät ja sopimukselliset

- Kuinka vastataan:
  - Ratkaisujen kehittämisessä riskien tunnistaminen ja niihin varautuminen, testaus
  - Huomiointi sopimuksissa (mm. hankinnat, ylläpito, toimijoiden välisten vastuiden määrittely)
  - Kansallisten palvelujen ja tietojärjestelmien pakolliset ominaisuudet (mukaan lukien olennaiset vaatimukset)
  - Testaus- ja tietoturvallisuuden arviointikriteerit (mukaan lukien olennaiset vaatimukset)
  - Riskitason ja järjestelmän luokan huomiointi sertifioinnissa
  - Ulkoiset todentamiset (yhteistestaus ja tietoturvallisuuden arviointi)
  - Tietoturvasuunnitelmat ja niiden omavalvonta
  - Viranomaisvalvonta

Järjestelmien luokittelu

Määräys 4/2021 luku 5 ja liite 1

- **Luokka A**: sertifioitavat
  - **Luokka A1**: ”tietoturvallisuuden arvioinnin suorittavat”
    - tietoturvallisuuden arviointia vaativat järjestelmät, joilta ei edellytetä yhteistestausta
    - myös muuntyyppisiä järjestelmiä aiempien teknisten Kanta-välityspalvelujen lisäksi
    - luokkaan voi kuulua sekä suppeampia että laajempia järjestelmiä
    - luokkaan voi kuulua laajasti asiakastietoja käsitteleviä / korkean riskitason järjestelmiä, jotka eivät liity Kanta-palveluihin
    - luokasta B luokkaan A siirtyminen mahdollista
  - **Luokka A2**: ”Kanta-palveluihin liittyvät, suppeat”
    - yhteistestausta ja tietoturvallisuuden arviointia vaativat, Kanta-palveluihin liittyvät, rajattua tietosisältöä tai käyttötarkoitusta palvelevat järjestelmät
  - **Luokka A3**: ”Kanta-palveluihin liittyvät, laajat”
    - yhteistestausta ja tietoturvallisuuden arviointia vaativat, Kanta-palveluihin liittyvät, sote-palveluja tuottavaan organisaatioon kohdistuvat vaatimukset kattavasti tai merkittävässä määrin täyttävät, laajasti hoidollisia tietoja käsittelevät tai erityisen arkaluonteista tai erityissuojattavaa tietoa sisältävät järjestelmät
    - erikseen ”kriittiset luokan A3 järjestelmät” joissa erityisiä varautumisvaatimuksia
- **Luokka B**: ei-sertifioitavat
  - asiakas- tai potilastietojen käsittelyyn tarkoitetut järjestelmät
  - voi sisältää mm. erikoistuneita järjestelmiä, lääkinnällisiä laitteita
  - voi sisältää järjestelmiä, joissa tietoturvallisuus varmistetaan pääosin palvelunantajan suojatoimenpiteiden kautta
  - voi sisältää järjestelmiä jotka tuottavat tai käyttävät joitakin tietoja (muiden järjestelmien kautta) Kanta-palveluihin
- Lisäksi: luokittelemattomat (ei asiakastietojen käsittelyyn suunniteltu tietojärjestelmä)
- Esimerkkejä järjestelmien luokittelusta: Määräys 4/2021 Liite 1

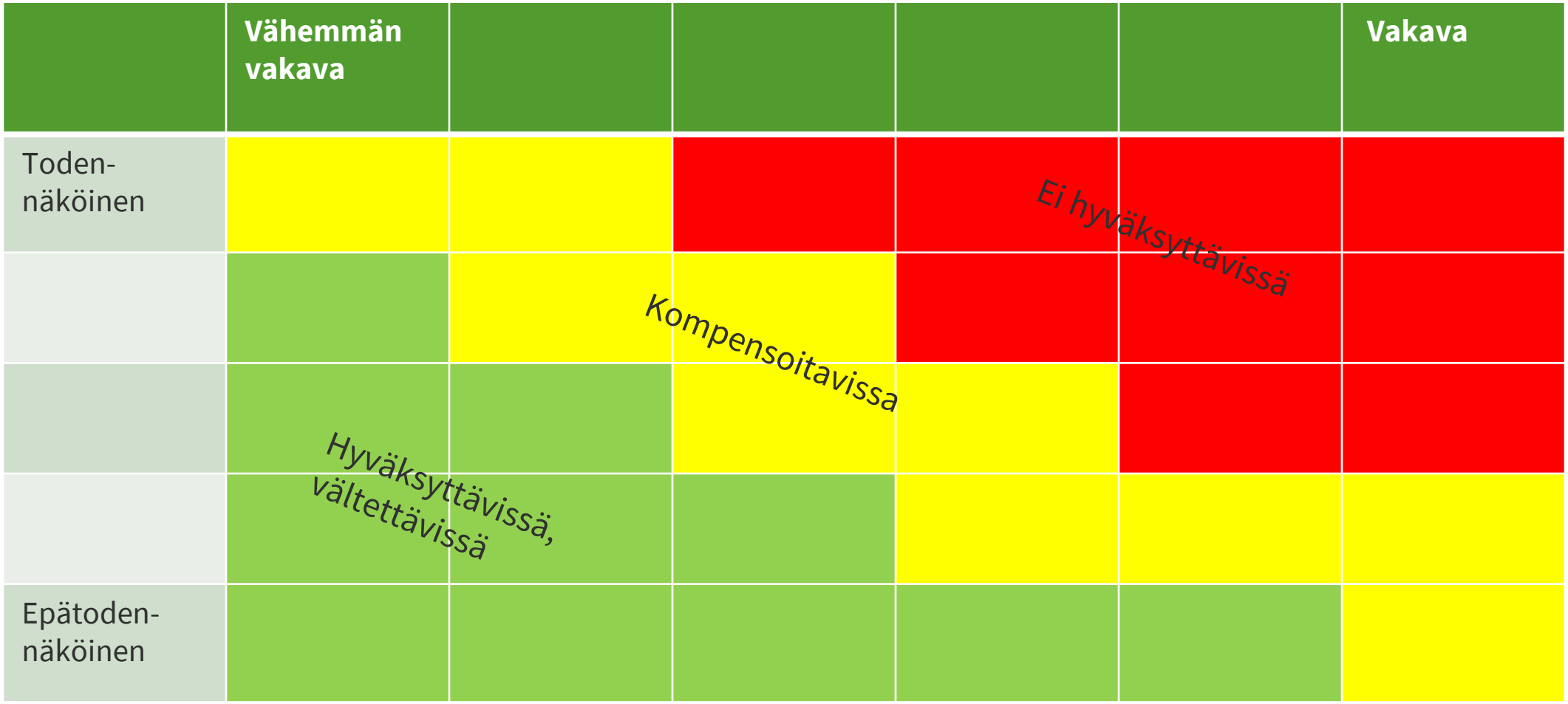
Riskitason määrittely

- Tietojärjestelmäpalvelun tuottajan on määriteltävä järjestelmän *riskitaso*
- Riskitaso ohjaa järjestelmän luokan *lisäksi* erityisesti tietoturvavaatimusten kohdistumista ja niiden todentamista
- Riskitason määrittelyssä huomioitava
  - Asiakastietojen käsittelyn laajamittaisuus
    - (tavoitellun tai olemassa olevan) käyttäjäkunnan laajuus, kansalaispopulaation laajuus, eri tyyppisten asiakastietojen käsittelyn laajuus
    - järjestelmän merkitys asiakas- ja potilasturvallisuudelle ja sote-palvelujen toimivuudelle huoltovarmuus ja varautuminen huomioiden
    - käsiteltävien asiakastietojen luonne ja sensitiivisyys
    - tietojen eheyteen liittyvät riskit (mm. valtakunnallisesti kerättävän tiedon laadun ja hyödynnettävyyden näkökulmasta)
    - liitettävyys ja järjestelmän merkitys osana laajempaa tietojärjestelmäkokonaisuutta
    - tiedon säilytykseen ja käsittelyyn liittyvät ulkoistusriskit
    - Sopimukselliset riskit
- Riskitason arvioinnin tueksi saatavilla mm. *Riskiarviotyökalu sote-tietojärjestelmille* (määräys 4/2021 tukimateriaalina)

Riski

[Ruck & Lowe]

Yksityiskohtainen riskienhallinta on kuitenkin aina järjestelmä-, organisaatio- ja tilannekohtaista!



Luokittelun ja riskitason merkitys

- Luokittelun tarkennusten ja riskitason pohjana erityisesti
  - Kokemukset ja palaute aiemmista säädöksistä, mm. merkittävistä sertifioiduista järjestelmistä edelleen löytyneet ongelmat, kohtuullisuusvaateet ”pienten” järjestelmien sertifioinnissa
  - Tarve järjestelmän käyttötarkoituksen, laajuuden sekä riskien huomiointiin olennaisten vaatimusten kohdistamisessa ja sertifioinnissa (myös mahdollisesti vaikutukset sertifioinnin hintaan ja kuormittavuuteen)
  - Säädösten (GDPR, MDR, tiedonhallintalaki…) riskipohjaistuminen
  - Luonnoksiin saatu lausuntopalaute
- Luokittelu ohjaa:
  - Kaikki luokkiin B, A1, A2, A3 kuuluvat:
    - Täytettävä käyttötarkoitusta vastaavat olennaiset vaatimukset, ilmoitettava Valviran tietojärjestelmärekisteriin
  - A1 lisäksi:
    - Sertifiointi / tietoturvallisuuden arviointi, tietoturvallisuustodistus
  - A2 ja A3 lisäksi:
    - Sertifiointi: yhteistestaus
- Riskitaso ohjaa:
  - Erityisesti tietoturva- ja varautumisvaatimusten kohdistumista
  - Tietoturvallisuuden arvioinnin ”syvyyttä” mm. haavoittuvuuksien etsiminen
  - Kiinnittämään huomiota riskienhallintaan…

Olennaiset vaatimukset

- yleiskuva
- osa-alueet
- profiilit
- järjestelmälomake

Asiakastietolaki 784/2021, 34 § ja 29 §

- Asiakastietojen käsittelyssä käytettävän tietojärjestelmän tulee täyttää yhteentoimivuutta, tietoturvaa ja tietosuojaa sekä toiminnallisuutta koskevat **olennaiset vaatimukset**
- Vaatimusten on täytyttävä käytettäessä tietojärjestelmää sekä **itsenäisesti** että **yhdessä muiden siihen liitettäviksi tarkoitettujen tietojärjestelmien kanssa**
- **Palvelunantajan käyttämien tietojärjestelmien** on vastattava käyttötarkoitukseltaan palvelunantajan toimintaa ja täytettävä palvelunantajan toimintaan liittyvät olennaiset vaatimukset
- Terveyden ja hyvinvoinnin laitos antaa tarkempia **määräyksiä** olennaisten vaatimusten sisällöstä ja siitä, mitkä olennaiset vaatimukset on täytettävä eri palveluissa käytettävissä tietojärjestelmissä ja hyvinvointisovelluksissa
- Tietojärjestelmäpalvelun tuottajan on laadittava kuvaus tietojärjestelmänsä ja hyvinvointisovelluksen valmistajan hyvinvointisovelluksensa käyttötarkoituksesta ja siitä, **kuinka se täyttää sitä koskevat olennaiset vaatimukset**

Sote-tietojärjestelmien olennaiset vaatimukset

Asiakastietolaki 29 § ja 34 §, THL Määräys 5/2021

- **I Toiminnalliset vaatimukset**
  - Kuvattava **käyttötarkoitus** ja **luokiteltava järjestelmä**
  - Tietojärjestelmäpalvelun tuottajan annettava **selvitys** toiminnallisten vaatimusten täyttymisestä (A- ja B-luokan järjestelmät)
  - Vaatimusten täyttyminen osoitetaan tietojärjestelmäpalvelun tuottajan antamalla selvityksellä
  - *Määräysten 4-5/2021 kautta selvitys annetaan vertailtavalla tavalla ja sertifiointia / rekisteröintiä tukien*
- **II Yhteentoimivuuden vaatimukset**
  - *Todennetaan* luokan A2 ja A3 järjestelmille (Kanta-palveluihin liittyvät) **Kelan yhteistestauksen** kautta
- **III Tietoturvavaatimukset**
  - *Todennetaan* luokan A (A1, A2, A3) järjestelmille tietoturvallisuuden arviointilaitoksen suorittamassa **tietoturvallisuuden arvioinnissa**
- Yhteentoimivuuden ja tietoturvallisuuden vaatimukset nojautuvat toiminnallisiin vaatimuksiin
  - käyttötarkoitus ja siitä annettu kuvaus, järjestelmää koskevat olennaiset vaatimukset

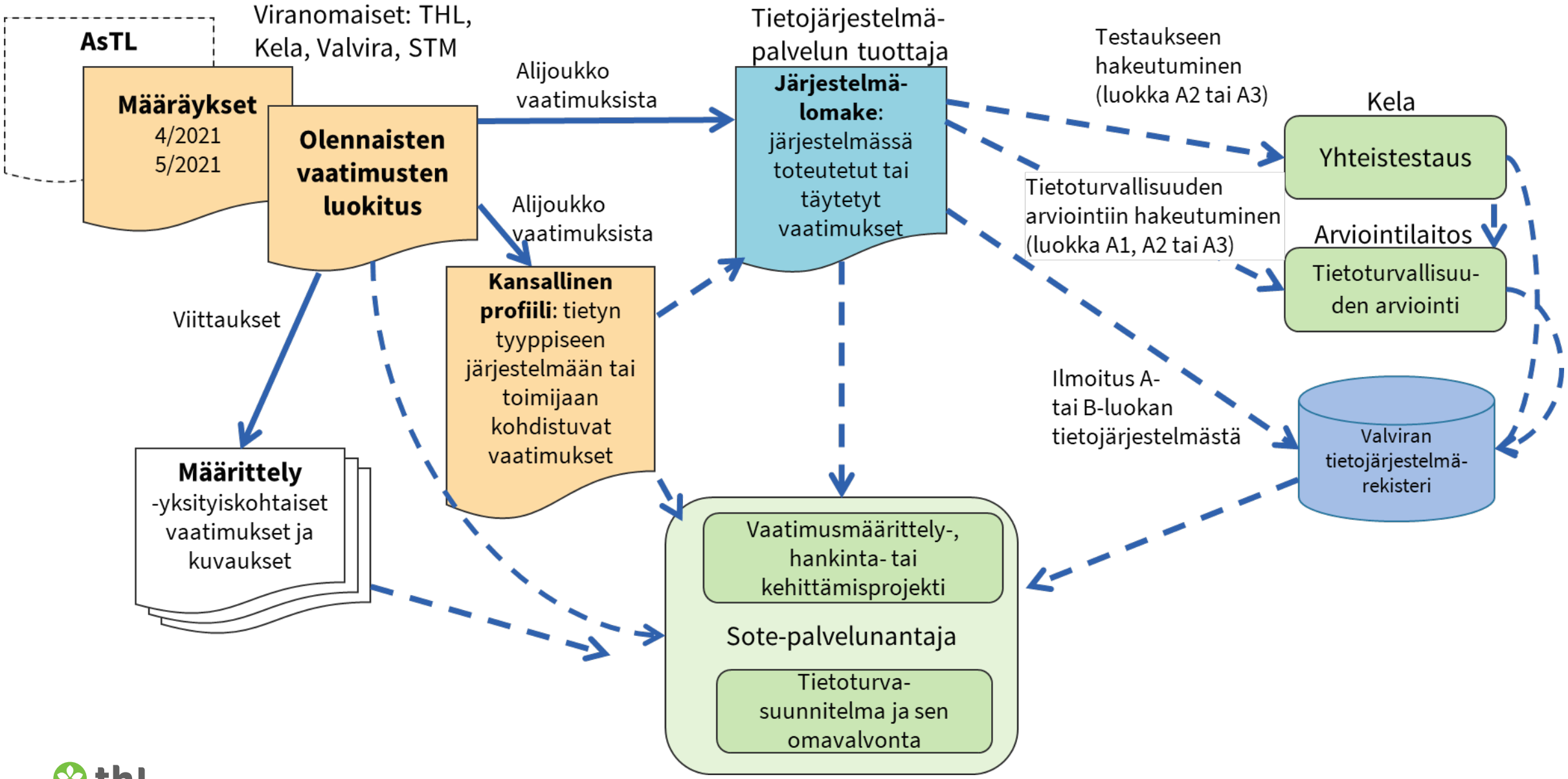
Olennaisten vaatimusten todentamisesta vastaa tietojärjestelmäpalvelun tuottaja tai valmistaja
Palvelunantajan on varmistettava olennaisten vaatimusten toteutuminen käyttämissään tietojärjestelmissä

Olennaisten vaatimusten määräys 5/2021

- *Olennaiset toiminnalliset vaatimukset* koskevat tietojärjestelmiin toteutettavia toimintoja ja tietosisältöjä
- *Olennaiset tietoturvavaatimukset* koskevat tietojärjestelmiin toteutettavia ja niiden kautta täytettäviä tietoturvallisuuden ja tietosuojan varmistamisen ominaisuuksia tai tietojärjestelmän suunnittelussa, toteuttamisessa tai tarjoamisessa tarvittavia toimenpiteitä
- Olennaisten vaatimusten täyttäminen tietojärjestelmäpalvelun tuottajan näkökulmasta: määräys 5/2021 luku 8
  - Käyttötarkoituksen kuvaus, luokittelu, riskitason arviointi
  - Käyttötarkoitusta vastaavien profiilien yksilöinti, järjestelmään sisältyvien toimintojen, tietosisältöjen ja tietoturvavaatimusten tunnistaminen
  - Vaatimusten toteuttaminen / täyttäminen, dokumentointi, oma testaus ja täyttämisen varmistaminen
  - Tietoturvallisuuden arviointi (luokat A1, A2 ja A3)
  - Kanta-palveluihin liittyvien yhteentoimivuuden vaatimusten yhteistestaukset
  - Käytännön välineenä järjestelmälomake
- Luokan A järjestelmän vaatimustenmukaisuus osoitettava sertifioinnilla ennen tuotantokäyttöönottoa
- Luokan A ja B tietojärjestelmät rekisteröitävä Valviran tietojärjestelmärekisteriin

Miten olennaisia vaatimuksia käytetään?

Määräys 5/2021 liite 1 luku 2 (kokoaa useita määräysten 4 ja 5 kohtia)



Olennaisten vaatimusten luokitus

Määräys 5/2021 liite 2

- Kokoaa kansallisesti eri säädösten ja määrittelyjen pohjalta määritellyt olennaiset vaatimukset seuraavissa luokissa
  - **Toiminnot** (järjestelmien toiminnalliset ominaisuudet)
  - **Tietosisällöt** (järjestelmien tuottamat tai hyödyntämät tiedot)
    - erityisesti asiakastiedot, erityisesti ne joihin kohdistuu kansallisia määrittelyjä tai joita toteutetaan Kanta-palveluihin liittyvissä järjestelmissä)
  - **Tietoturvallisuusvaatimukset**
- Kukin vaatimus sisältää viittaukset sen pohjana oleviin säädöksiin tai määrittelyihin, yhteydet muihin vaatimuksiin ja sertifiointiin (yhteistestauksen testauspaketti tai tietoturva-auditoitavat vaatimukset)

Ryhmä	Id	Otsikko	Selite	Lähde	Sertifiointi	Tietosisällön muoto		Yhteydet muihin vaatimuksiin	Tarkennuksia / huomautuksia / lisätietoja
TKUV			**Kuvantaminen**						
	TKUV01	Kuva-aineistot	Radiologisen kuvantamisen kuva-aineistot kuten natiiviröntgentutkimukset, uä-tutkimukset, magneettitutkimukset, TT-tutkimukset, varjoainetutkimukset, ja niihin liittyvät DICOM-tutkimukset ja tutkimusobjektit	Kvarkki tekninen määrittely versio 2.1.1 / 6.6.2016 -> Kuva-aineistojen arkisto (Kvarkki) - tekninen määrittely, versio 2.3.5 / 17.04.2020; Aiempi vaiheistusasetus	Kvarkki	N	R	Toiminnot: KUV04, KUV06, KUV09, KUV11, KUV12, KUV13, KUV14	Kuvantamistutkimukseen kuuluvat kuvat eivät ole rakenteista dataa (paitsi kuva-objektia vastaavat esim. EKG-käyrät), mutta kuva-aineistoihin liittyy rakenteisia tietoja, jotka DICOM standardi määrittelee

Olennaisten vaatimusten ryhmittely / Toiminnot

Määräys 5/2021 liite 2 Olennaisten vaatimusten luokitus

RESL	**Sähköisen lääkemääräyksen käsittely ja lääkitystietojen hallinta**
LTOIM	**Lääketoimitukset**
VV	**Kanta-viestinvälitys ja muut Kanta-palvelut**
ARK	**Kanta-arkistointipalveluun liittyvän järjestelmän perustoiminnot**
LP	**Kanta-lisäpalveluihin liittyvät toiminnot**
KH	**Käyttäjä- ja käyttöoikeushallinta**
KV	**Käyttövaltuuksien tarkastaminen ja allekirjoitus**
SH	**Suostumusten, luovutusten ja informointien hallinta**
KS	**Käytön ja luovutuksen seuranta**
SOS	**Sosiaalihuollon asiakastietojen hallinta**
KUV	**Kuvantamisen toiminnot**
LPYY	**Lähetteet ja pyynnöt**
HTH	**Henkilötietojen hallinta**
ERIL	**Erillisjärjestelmien ja -palvelujen Kanta-toiminnot**
AV	**Ajanvaraus**
PTUK	**Päätöksentuki**

Olennaisten vaatimusten ryhmittely / Tietosisällöt

Määräys 5/2021 liite 2 Olennaisten vaatimusten luokitus

TPOT	**Potilashoidon yhteiset ja potilaskertomuksen tiedot**	Potilaiden hoidossa ja sähköisessä potilaskertomuksessa yli yksittäisten palvelujen tai erikoisalojen tarvittavat tiedot
TSL	**Suostumukset, luovutukset, palvelutapahtumien ja asioiden hallinta**	Käynteihin ja hoitojaksoihin liittyvät palvelutapahtumien tiedot, sosiaalihuollon asioiden hallintaan tarvittavat tiedot, henkilörekisterien ja rekisterinpitäjien välillä tapahtuvien luovutusten hallintaan tarvittavat tiedot
TLOK	**Lokimerkintöjen tietosisällöt**	Asiakas- ja potilastietojen käsittelyssä syntyvien lokitietojen hallinnan tiedot
TMET	**Asiakirjojen kuvailutietojen hallinta**	Potilas- ja asiakasasiakirjojen ja niissä olevien merkintöjen hallintaan tarvittavat kuvailutiedot (metatiedot)
TERI	**Erikoisalat ja palvelukohtaiset määrittelyt**	Palvelu- tai erikoisalakohtaiset asiakas- ja potilastiedot
TSOS	**Sosiaalihuollon asiakirjat**	Sosiaalihuollon palvelujen tuottamisessa ja hallinnassa tarvittavat tiedot
TKUV	**Kuvantaminen**	Terveydenhuollon kuvantamisratkaisuihin liittyvät tiedot
TBIO	**Biosignaalit**	Elintoimintojen mittaamisen signaalimuotoiset tiedot
TPTO	**Palvelujen ja toiminnan ohjaus**	Asiakkaille tarjottavien palvelujen hallinnan ja ohjauksen tiedot
THEN	**Henkilöiden perustiedot**	Asiakkaiden ja potilaiden perustietojen ja tunnistetietojen käsittelyssä tarvittavat tiedot

Olennaisten vaatimusten ryhmittely / Tietoturvavaatimukset

Määräys 5/2021 liite 2 Olennaisten vaatimusten luokitus

ASALK	**Sähköinen allekirjoitus**
ATUNN	**Tunnistaminen**
AKVH	**Käyttövaltuushallinta**
AVALO	**Valvonta ja lokitus**
ATIKO	**Tietojen käsittely ja ohjeistus**
APAKOL	**Muut pakolliset vaatimukset**
ASTUR	**Sovellusturvallisuus**
AKYM	**Järjestelmän käyttöympäristö**

Vähimmäisvaatimusten profiilit
Määräys 5/2021 liitteet 3a-3g

- Kokoavat kansalliset vähimmäisvaatimukset *eri käyttötarkoituksiin* tarkoitetuille järjestelmille
- Yksi järjestelmä voi täyttää useita profiileja
  - Mikään järjestelmä ei täytä KAIKKIA profiileja tai vaatimuksia (esim. apteekit vs. lääkkeiden määrääjät…)
- Kukin profiili sisältää osajoukon olennaisista vaatimuksista
  - Esimerkki: optisen toimialan järjestelmä

Profiilin tunniste	Profiilin nimi	Käyttötarkoitus	Profiilin voimaantulopäivä	Kuvaus	Lisätietoja
3c3	Optisen toimialan järjestelmä	Optisen toimialan palvelujen tuottamisessa käytettävä tietoja Kanta-arkistoon arkistoiva ja sieltä hyödyntävä järjestelmä.	Potilastiedon arkistoon liittymisestä lähtien.	Optisen toimialan palvelujen tuottamisessa käytettäväksi tarkoitettu järjestelmä. Profiili kattaa optikoiden ja silmälääkäreiden Kantapalveluihin liittyvät järjestelmävaatimukset. Järjestelmäkokonaisuuteen voi kuulua myös kuvantamisen profiileja toteuttavia ominaisuuksia silmälääkäreiden vastaanottotoimintaan liittyen.	Voi kuulua eri luokkiin A tai B riippuen käsitteleekö Kanta-arkiston tietoja suoraan tai toisen tietojärjestelmäpalvelun kautta. Mikäli Optisella toimialalla on myös lääkäritoimintaa, tulee lääkemääräys toiminnot toteuttaa Lääkemääryksiä käsittelevän potilastietojärjestelmä -profiilin mukaisesti tietojärjestelmässä tai erillisjärjestelmässä.

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 (5 AIEMMAT KORVAAVAA profiilia)
  - 3f Todistusten profiilit (3 profiilia)
  - 3g Asiakas- tai potilastietojen käsittelyyn tarkoitetun järjestelmän vähimmäisvaatimukset (sis. luokka B tai A1) (1 UUSI profiili)

Olennaisten vaatimusten profiilit (liite 3a-3g)

- Seuraaviin keskeisiin järjestelmien käyttötarkoituksiin olennaisten vaatimusten koonti
  - 3a Sähköisen reseptin profiilit
    - Lääkemääräystä käsittelevä potilastietojärjestelmä (PTJ)
    - Apteekkijärjestelmä
  - 3b Kanta-arkistoon liittyvien järjestelmien vähimmäisvaatimusprofiilit
    - Kanta-arkistointipalvelusta tietoja hakeva sovellus tai palvelu
    - Kanta-arkistointipalvelusta haettuja tietoja hyödyntävä sovellus
    - Kanta-arkistointipalveluun tietoja toimittava sovellus tai palvelu
    - Kanta-arkistointipalveluun toimitettavia tietoja tuottava sovellus
  - 3c Potilastiedon arkiston profiilit
    - Potilaskertomusjärjestelmä (perusvaatimukset)
    - Suun terveydenhuollon järjestelmä
    - **UUSI** Optisen toimialan järjestelmä
  - 3d Sosiaalihuollon asiakastiedon arkiston profiilit
    - Profiilit julkaistaan myöhemmin uudistuvien määrittelyjen yhteydessä
  - 3e Kuvantamisen profiilit
    - **UUSI:** Kuvantamiseen liittyvä potilashallinnon perusjärjestelmä (HIS)
    - **UUSI:** Kuvantamisen toiminnanohjausjärjestelmä (RIS), Kantaan liittynyt
    - **UUSI:** Kuvantamisen toiminnanohjausjärjestelmä (RIS), ei Kantaan liittynyt
    - **UUSI:** Kuvien tallennus- ja jakamisjärjestelmä (PACS)
    - **UUSI:** Kuvantamisen katselinohjelmisto
  - 3f Todistusten profiilit
    - Kanta-arkistosta todistuksia tai lausuntoja kyselevä palvelu
    - Kanta-arkistosta todistuksia tai lausuntoja vastaanottava palvelu
    - Kanta-arkistoon todistuksia tai lausuntoja tuottava palvelu
  - 3g Asiakas- tai potilastietojen käsittelyyn tarkoitetun järjestelmän vähimmäisvaatimukset (sis. luokka B tai A1)
    - **UUSI:** Asiakas- tai potilastietojen käsittelyyn tarkoitetun järjestelmän vähimmäisvaatimukset (sis. luokka B tai A1)

Järjestelmälomake

Määräys 5/2021 Liite 4 Järjestelmälomake

- Lomakepohja, **tietojärjestelmäpalvelun tuottaja** täyttää
- Käytännön työkalu tietojärjestelmän **sertifiointiin ja rekisteröintiin**
- Muodostaa **asiakastietolain edellyttämän selvityksen olennaisten vaatimusten täyttämisestä**
- 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 suhteessa olennaisiin vaatimuksiin
  - **Toiminnot** jotka ovat osa järjestelmän käyttötarkoitusta
  - **Tietosisällöt** jotka ovat osa järjestelmän käyttötarkoitusta
  - **Tietoturvavaatimukset**, jotka täytetään järjestelmän kautta
- Yksi lomake pohjana Kelan **yhteistestaukseen** (A2 ja A3-luokka), **tietoturvallisuuden arviointiin** (A1, A2 ja A3-luokka) ja Valviran **tietojärjestelmärekisteriin tehtäviin ilmoituksiin** (A ja B-luokka)
- Ohjaa luokituksen kautta tarkempiin määrittelyihin
- **PÄIVITETTY** versio määräyksen 5/2021 yhteydessä

”Rasti ruutuun”

Määräys 5/2021 Liite 4 Järjestelmälomake

- Lomakkeeseen merkitään järjestelmään toteutetut tai sen kautta täytetyt olennaiset vaatimukset
  - Mukaan lukien järjestelmän käyttötarkoitusta vastaavien profiilien vaatimukset

Ryhmä	Id	Otsikko	Selite	Toteutetaan järjestelmässä	Lisätietoja
				[täytä oikea merkintä] **X**=toteutuetaan lomakkeella ilmoitettavassa järjestelmässä **M**= muuttunut järjestelmässä verrattua aiempaan järjetelmälomakkeeseen/versioon. Lisätietoja kohdassa ilmaistava tarkemmin, miten muutettu **U**= ulkoinen, toteutetaan toisen järjestelmän tai rajapinnan kautta, lisätietoja kohdassa tämä ilmaistava tarkemmin	[täytä tarvittaessa, esim. mikäli toteutetaan erikseen sertifioidulla toisella järjestelmällä tai tietyn rajapinnan kautta, kyseisen järjestelmän tai rajapinnan nimi]
ARK			**Kanta-arkistoon liittyvän järjestelmän perustoiminnot**		
	ARK01	Asiakirjojen muodostaminen	Asiakirjan muodostus on tietojärjestelmän säännöillä ohjattu automaattinen prosessi. Asiakirja muodostetaan viimeistään, kun potilasasiakirja-asetuksessa (Sosiaali- ja terveysministeriön		
	ARK02	Lomakeasiakirjan muodostaminen	Itsenäisiä lomakkeita ja todistuksia käytetään tiedonsiirtoon eri organisaatioiden välillä. Lomakkeet ja todistukset voivat toimia täysin itsenäisinä sisältäen myös potilaan tunnistamiseen		
	ARK04	Lomakeasiakirjan välittäminen kolmannelle osapuolelle	Arkistoitu asiakirja voidaan välittää kolmannelle osapuolelle kuten eri viranomaisille. Välittäminen voidaan tehdä uuden asiakirjan muodostamisen yhteydessä tai se voi kohdistua aiemmin		

Järjestelmälomakkeeseen liittyviä kokemuksia ja palautteita

- ”Nähdään hyödylliseksi, että oman järjestelmän mukaiseen käyttötarkoitukseen tarkoitetulle järjestelmälle (ja muille samaan tarkoitukseen käytettäville järjestelmille) olisi saatavilla profiilidokumentti, jossa on kuvattu se, mitkä toiminnot ja sisällöt vähintään pitäisi olla toteutettuna.”
- ”Lähdelinkit ovat hyödyllisiä.”
- ”Lomake vaikuttaa hyvinkin hyödylliseltä. Ruksittujen ominaisuuksien kuvailu esimerkiksi vapaamuotoisena tekstinä olisi varsin hankalaa. Lisätietokenttä toimintorivin ohessa on hyvä olla olemassa.”
- ”Lomakkeen kysymyksiin vastaaminen saattaa aiheuttaa uusia kysymyksiä tuotekehityksen ratkaistavaksi, mikä on hyvä asia. -> Vastaan voi tulla asioita, jotka ovat jääneet huomaamatta järjestelmäkehityksessä.”
- ”Nyt tuotettu dokumentaatio auttaa erityisesti järjestelmäilmoituksien jättämisessä Valviraan.”
- ”Palvelun tuottajan tietojärjestelmän käyttötarkoitus on yksiselitteisen selkeä. Järjestelmälomake on tietojärjestelmätoimittajan työväline, jolloin heidän näkemyksensä tulee huomioida määräyksessä.”
- ”Järjestelmälomakkeessa voisi olla selkeämmin dokumentoitu, mitkä vaatimukset ovat tietyn tyyppiselle / tietyn luokan järjestelmälle valideja.” → profiilit, tukimateriaaliin tuleva koontitaulukko

Sertifiointiprosessi

Sertifioinnin kokonaisuus

- Asiakastietolain mukainen sertifiointi koskee luokan luokan A (A1, A2, A3) tietojärjestelmiä
  - Kohteena järjestelmien tietojärjestelmäpalvelun tuottajat / valmistajat, ei käyttäjäorganisaatiot
  - Tekniset Kanta-välityspalvelut kuuluvat luokkaan A1
- Olennaisten vaatimusten täyttämisen ja sertifioinnin muodostettava eheä kokonaisuus sote-palvelun antajien toiminnan ja näiden tietoturvasuunnitelmien kanssa
- Tietojärjestelmäpalvelun tuottaja avainroolissa olennaisten vaatimusten täyttämisen osoittamisessa ja sertifioinnissa (järjestelmän luokittelu, olennaisten vaatimusten täyttämisen osoittaminen, sertifiointiin hakeutuminen, järjestelmän rekisteröinti Valviran tietojärjestelmärekisteriin, muutosilmoitukset..)
- Sertifioinnin osana on yhteentoimivuuden ja tietoturvallisuuden ulkoinen todentaminen (mutta ei kattavaa toiminnallisten vaatimusten todentamista)
- Toiminnalliset vaatimukset (toiminnot ja tietosisällöt) luovat pohjan myös yhteistestaukselle ja tietoturvallisuuden arvioinnille
  - Vaikka eivät ole ulkoisesti todennettavia osana sertifiointia

Sertifioinnin viranomaistoimijat

Kaikissa sertifiointi- ja rekisteröintiprosesseissa mukana:

- **Kela / Kanta-palvelut**: Kelan palvelu, jonka vastuulla on Kanta-palveluiden toteuttaminen, ylläpito ja kehittäminen
  - **Kanta-yhteistestaus**: suunnittelee ja koordinoi **yhteistestauksen**
- **Tietoturvallisuuden arviointilaitos**: Traficomin hyväksymä taho, joka suorittaa sertifiointiprosessin osana olevan tietoturvallisuuden arvioinnin, tuottaa vaatimustenmukaisuustodistuksen ja ottaa vastaan ilmoituksia järjestelmiin tehtävistä muutoksista
- **Valvira**: valvontaviranomainen, joka ylläpitää **rekisteriä** tietojärjestelmistä ja valvoo ja edistää tietojärjestelmien vaatimustenmukaisuutta

Ohjauksessa lisäksi:

- **STM:** strateginen ohjaus ja lainsäädäntö
- **Terveyden ja hyvinvoinnin laitos**: viranomainen, joka vastaa sote-asiakastiedon sähköisen käsittelyn ohjauksesta ja mm. antaa määräykset olennaisista vaatimuksista ja tietoturvasuunnitelmasta sekä olennaisten vaatimusten todentamisessa käytettävistä menettelyistä
- **Traficom**: (liikenne- ja viestintävirasto) valvontaviranomainen, joka hyväksyy tietoturvallisuuden arviointilaitokset ja valvoo niitä

Sertifiointi suhteessa kehitystyöhön ja käyttöönottoihin

Määräys 5/2021 liite 1 luku 5, Määräys 4/2021 luku 7

Kehitystyö

- Vaatimusten selvittäminen ja ratkaisun suunnittelu — Valmistaja / tj-palvelun tuottaja
- Järjestelmäkehitys
- Dokumentointi
- Toimittajan oma testaus

Sertifiointi (luokka A)

- Hakeutuminen sertifiointiin — Valmistaja / tj-palvelun tuottaja
- Yhteistestaus (luokka A2, A3) — Kela
- Tietoturvallisuuden arviointi (luokka A1, A2, A3) — Arviointi-laitos

Käyttöönotto, tuotanto ja päivitykset

- Ilmoitus Valviralle (luokka A tai B) — Valvira
- Käyttöönotto, käyttöönottokoe (Kanta) — Kela
- Tuotantokäyttö — Valmistaja / tj-palvelun tuottaja; Sote-palvelunantaja
- Muutokset järjestelmään, muutosilmoitukset — Kela; Arviointi-laitos

Sertifiointiprosessi uusien säädösten mukaisesti

- Prosessi samanlainen kuin aiemmissakin säädöksissä
- Aiempi vaatimustenmukaisuustodistus nyt todistus tietoturvallisuuden arvioinnista
- Järjestelmien luokittelumuutoksen vaikutukset sertifiointiin
  - Luokka A1: muut kuin järjestelmät, jotka eivät liity Kanta-palveluihin mutta joilta edellytetään tietoturvallisuuden arviointia
    - Myös muuntyyppisiä järjestelmiä aiempien teknisten Kanta-välityspalvelujen lisäksi
    - Voi sisältää sekä suppeampia että laajempia järjestelmiä (ks. järjestelmien luokittelu)
    - Luokasta B luokkaan A järjestelmien siirtyminen mahdollista
  - Luokka A2: Kanta-palveluihin liittyvät, ”suppeat”
  - Luokka A3: Kanta-palveluihin liittyvät, ”laajat”
- Järjestelmän käyttötarkoituksen ja riskitason huomiointi todentamisessa terävöityy
  - mm. tietoturvavaatimukset osaksi profiileja
- Tietoturvavaatimusten todentamisen tarkennukset

Sertifiointiprosessin päätoimenpiteet valmistajan / tietojärjestelmäpalvelun tuottajan näkökulmasta

1. Tuote- ja järjestelmäkehitys
   - Käyttötarkoituksen määrittely
   - Säädösten ja olennaisten vaatimusten huomiointi, mm.
     - mitä profiileja järjestelmä toteuttaa
     - mitkä muut olennaiset vaatimukset järjestelmää koskevat
     - kuinka vastaan olennaisiin vaatimuksiin: toiminnot, tietosisällöt, tietoturvavaatimukset: toteutus
     - HUOM dokumentointi / laatujärjestelmä ja oma testaus osana kehitystyötä
     - HUOM suhde, rajapinnat ja työnjako muiden järjestelmien kanssa vaatimusten täyttämisessä
2. **Hakeutuminen sertifiointiin: yhteydenotto Kanta-palveluihin ja tietoturvallisuuden arviointilaitokselle**
   - Liittyminen ja ilmoittautuminen asiakastestipalveluun, yhteistestaukseen ja tietoturvallisuuden arviointiin, olennaisten vaatimusten järjestelmälomake
3. **Yhteistestausprosessi**
   - Ks. Kelan materiaali
4. **Tietoturvallisuuden arviointi**
   - Arviointivalmiudet, dokumentaatio, arviointitilaisuus / tilaisuudet
5. **Tietoturvallisuustodistus**
   - HUOM. todistus voidaan myöntää vasta kun myös yhteistestaus on hyväksytysti suoritettu
6. **Ilmoitus Valviralle ennen tuotantokäyttöä**
7. Tuotantokäyttöönotto
   - Mm. käyttäjäasennukset, koulutukset, Kanta-liityntäpiste ja käyttöönottokokeet jne.
8. Päivitykset, muutokset ja niihin liittyvät ilmoitukset (→ vaihe 1…)

Tietoturvallisuuden arviointilaitokset

- Traficom hyväksyy tietoturvallisuuden arviointilaitokset ja valvoo niitä
  - Arviointilaitosten hyväksyntä perustuu lakiin tietoturvallisuuden arviointilaitoksista 1405/2011
- Traficom ohje arviointilaitoksille
  - "Jos tietoturvallisuuden arviointilaitoksen pätevyysalueena on VAHTI tai Katakri, se voi tehdä sosiaali- ja terveydenhuollon tietojärjestelmien arvioinnin ja antaa olennaisten vaatimusten täyttymistä koskevan todistuksen."
- Asiakastietolain mukaisiin tietoturvallisuuden arviointeihin hyväksyttyjä arviointilaitoksia tällä hetkellä kaksi: KPMG IT Sertifiointi Oy ja Nixu Certification Oy

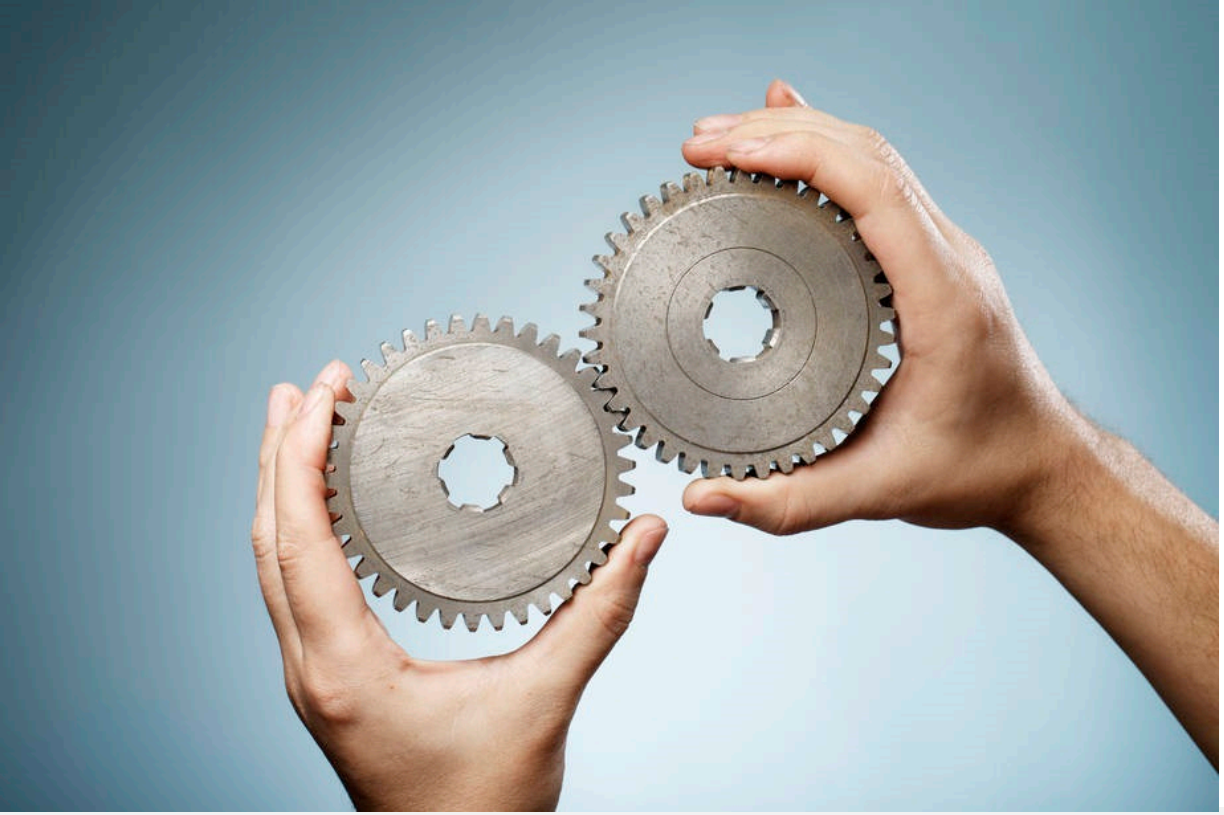
Tietoturvallisuuden arvioinnin menettelyt osana sertifiointia

- Pohjatyö, relevanttien vaatimusten tunnistaminen, toteutus ja huomiointi järjestelmän kannalta, dokumentointi
- Yhteydenotto arviointilaitokseen / sertifiointihakemus, sitoumus
- Sopimus arviointilaitoksen kanssa
  - Tietoturvallisuuden arviointi ja mahdolliset seuranta-auditoinnit maksullisia
- Tarvittavan dokumentaation kokoaminen / tuottaminen
- Arviointitilaisuus / -tilaisuudet
- Havaintojen ja mahdollisten poikkeamien hallinta – korjaukset, tarkennukset, täsmennykset, lisätietojen toimittaminen, tarvittaessa tietoturvallisuuden uusi arviointi
- Todistus tietoturvallisuuden arvioinnista (tietoturvallisuustodistus)
- Järjestelmämuutoksissa uuden tietoturvallisuuden arvioinnin tarpeen arviointi

Tietoturvavaatimusten todentaminen

Määräys 4/2021 Luku 7.3, Määräys 5/2021 luku 10.2

- Todentamisessa käytetään Traficomin ohjeiden mukaisia hallinnollisia ja soveltuvin osin myös teknisiä todentamistapoja
- Todentaminen tehdään Määräyksen 5/2021 kunkin vaatimuksen edellyttämällä tasolla järjestelmän luokka, kriittisyys ja käsiteltävien tietojen luonne huomioiden
- Tietoturvavaatimusten todentamisessa käytetään seuraavia todentamistapoja:
- **V**: validointi tai tekninen tarkastus, esimerkiksi järjestelmän tuottaman lokin, sanomainstanssin tai järjestelmän tuottaman raportin läpikäynti
- **testaus**, jossa
  - **TT**: tarkistetaan sovellusta käyttämällä (toiminnallisella testauksella) ominaisuuden olemassaolo ja asianmukaisuus osana tietoturvallisuuden arviointia
  - **HT**: tekninen tietoturva- ja haavoittuvuustestaus ja turvallisuustason arviointi osana tietoturvallisuuden arviointia
- **D**: järjestelmän dokumentaation tai muiden järjestelmään liittyvien dokumenttien läpikäynti
- (täydentävä): **H**: haastattelu osana tietoturvallisuuden arviointia, jolla voidaan syventää ja täydentää arviointia
  - ei yksin riittävä vaatimuksen todentamistavaksi luokan A järjestelmissä



Esimerkkejä ja nostoja olennaisista vaatimuksista

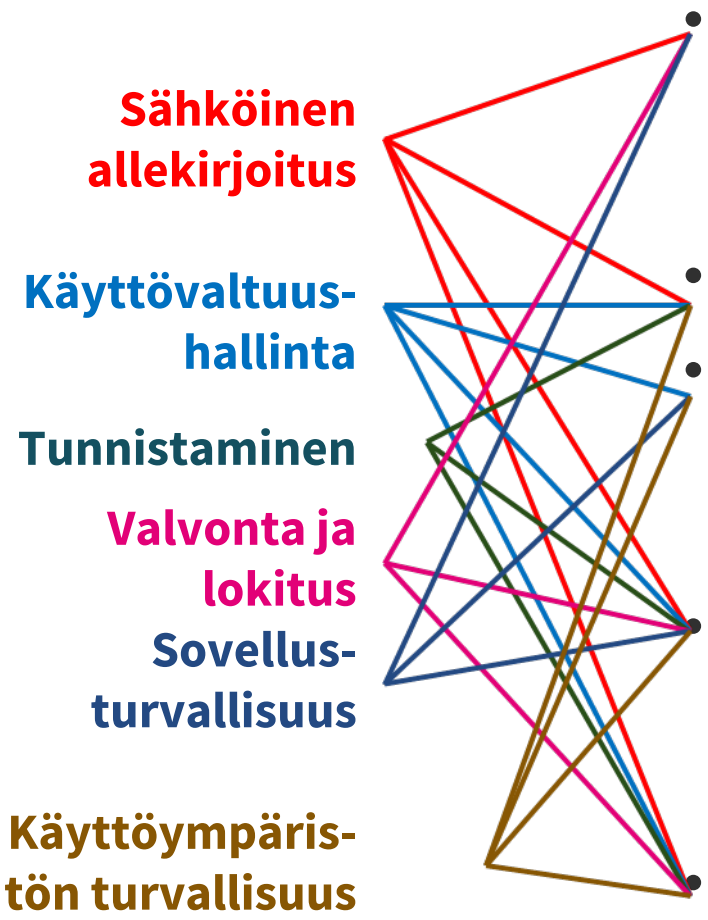
Esimerkki lausuntokierroksen aikana tehdyistä olennaisten vaatimusten tarkennuksista – yhteentoimivuus ja tiedon laatu

- Kommentti: ”Koodistojen lataamisen vaatimus VV09 ei ole riittävä tietojen laadun ja yhdenmukaisuuden varmistamiseksi – olennaista on edellyttää yhteisten koodistojen mukaisen tiedon tuottamista”
- → Koodistojen hyödyntämiseen täsmennetty perusvaatimus:
  - Vaatimus: **VV16 Kansallisten koodistojen mukainen tietojen tuottaminen**
  - Selite: Asiakastietoja tai -asiakirjoja kansallisiin tietojärjestelmäpalveluihin lähettävän järjestelmän ja tiedot tuottavan palvelunantajan on tuotettava lähetettävien asiakirjojen tai sanomien **koodisto-tyyppisiin tietokenttiin sisältö** noudattaen THL:n koodistopalvelun kautta käsiteltyjä ja julkaistuja koodistoja ja luokituksia, ellei tarkemmassa tietosisältömäärittelyssä muuta ilmaista.
  - Lisätietoja: Vaikka vastaaviin tietoihin käytettäisiin paikallisesti muita tai täydennettyjä koodistoja, on Kanta-palveluihin lähetettävissä tiedoissa tieto ilmaistava kansallisen koodiston mukaisesti ja mahdollisten vastaavuuksien määrittely on lähettävän toimijan vastuulla. Paikallisten koodistojen käyttö voi olla mahdollista ja tarpeellista joissakin käyttökohteissa, jolloin kansallisiin tietojärjestelmäpalveluihin lähetettäviin kansallisten koodistojen mukaisiin tietoihin on mahdollista määritellä vastaavuudet. Jos samoja koodistosisältöjä julkaistaan useissa eri kanavissa, on noudatettava koodistoversio ja sen käyttöönottoajankohta ensisijaisesti THL:n kautta julkaistu. Sisältö- tai luokituskohtaisesti on mahdollista poiketa perusvaatimuksesta THL:n tarkempien ohjeiden ja määrittelyjen mukaisesti.
  - Lähteet: AsTL 9 §, Koodistopalvelussa julkaistut luokitukset ja koodistot

Tietoturvallisuuden perusperiaatteet

- Eheys
  - tarkkuus ja yhdenmukaisuus säilyvät tiedon elinkaaren ajan
  - luvaton muokkaaminen ei onnistu tai se havaitaan
- Luottamuksellisuus
- Saatavuus ja luotettavuus
  - tieto on saatavilla, kun sitä tarvitaan
  - ohjelmistot, laitteet, turvallisuus ja viestinvälitykset toimivat
- Autenttisuus
  - tiedon alkuperä on tiedossa
  - tiedonvaihdon osapuolet tunnistetaan luotettavasti
- Kiistämättömyys ja velvoittavuus
  - sopimuksen velvoitteet täytetään
  - osapuoli ei voi kiistää osallistumistaan tapahtumaan

Olennaiset tietoturvavaatimukset suhteessa tietoturvatavoitteisiin



- Eheys
  - tarkkuus ja yhdenmukaisuus säilyvät tiedon elinkaaren ajan
  - luvaton muokkaaminen ei onnistu tai se havaitaan
- Luottamuksellisuus
- Saatavuus ja luotettavuus
  - tieto on saatavilla, kun sitä tarvitaan
  - ohjelmistot, laitteet, turvallisuus ja viestinvälitykset toimivat
- Autenttisuus
  - tiedon alkuperä on tiedossa
  - tiedonvaihdon osapuolet tunnistetaan luotettavasti
- Kiistämättömyys ja velvoittavuus
  - sopimuksen velvoitteet täytetään
  - osapuoli ei voi kiistää osallistumistaan tapahtumaan

Tietoturvavaatimusten uudistukset

- 2015 jälkeen uudistuneista säädöksistä nousevat tarkennukset ja ajantasaistukset
- Sertifiointiprosessin soveltamisesta esiin nousseet tarkennustarpeet
- Tietoturva- ja tietosuojapoikkeamista esiin nousseet tarkennustarpeet
- Tietojärjestelmien olennaisten vaatimusten linkitykset palvelunantajien tietoturvasuunnitelmiin (liittyy THL Määräys 3/2021)
- Profiilit ja järjestelmälomake selkeämmin ohjaamaan myös tietoturvallisuuden arviointia
  - Järjestelmä tietyn profiilin mukainen → ainakin profiilin mukaiset tietoturvavaatimukset toteutettava ja luokassa A1/A2/A3 todennettava tietoturvallisuuden arvioinnissa
  - Aiempien tietoturvavaatimusten normalisointi suhteessa toiminnallisiin vaatimuksiin
- Sertifioinnin todentamistapoihin tarkennuksia
  - Haastattelut eivät enää missään vaatimuksessa ensisijainen todentamistapa
  - Testaukseen mukaan tekninen tietoturvatestaus (luokka A3 ja laajat luokan A1 järjestelmät)
- Uusia ja tarkentuneita vaatimuksia ja todentamisia (Määräys 5 liite 2 / Tietoturvavaatimukset)
  - Lähteitä mm. Pitukri, Katakri, OWASP ASVS, Julkisen hallinnon pilvipalvelulinjaukset, VAHTI-suositukset, EDPB suositukset, GDPR:n ja EU:n kyberturvallisuusasetuksen tarkennukset, valtioneuvoston päätös huoltovarmuuden tavoitteista

    ← sovellettuna asiakastietolain mukaiseen tuotesertifiointiin ja mm. luonnoksiin saatu lausuntopalaute huomioiden

Erityiskysymyksiä

Kolmansien osapuolten palveluihin liittyvät tietosuoja-, tietoturva- ja varautumisvaatimukset

Määräys 5/2021 Liite 1 Olennaisten vaatimusten soveltamisohjeet, luku 6.4

- Tietosuoja- ja tietoturvallisuusriskeihin varautuminen sekä **palvelunantajien** että **tietojärjestelmäpalvelun tuottajien** toiminnassa
- Kolmansien osapuolten välineet, alustat ja jaettuja resursseja tarjoavat ICT-palvelut laajasti käytettyjä ja tarpeellisia
  - Esim. palvelinvuokraus, palvelinhallinta, varmistuspalvelut, konesalipalvelut, pilvipalvelut
- Samat perusvaatimukset täytettävä eri tilanteissa ja eri arkkitehtuureissa, tietojärjestelmäpalvelun tuottaja ja palvelunantaja vastaavat osaltaan vaatimusten täyttymisestä myös kolmannen osapuolen palveluita käytettäessä
  - Tietojärjestelmäpalvelun tuottajan varmistettava **läpinäkyvyys** myös asiakkaiden tekemää riskiarviointia varten
- Vaatimuksia selkeytetty suhteessa luonnosversioon
  - EU- ja ETA-tasoinen tietojen liikkuvuusperiaate toteutettava
  - EU:n yleisen tietosuoja-asetuksen mukainen erityisten henkilötietoryhmien suojaaminen ja EU:n lainsäädännön keskeiset perusoikeudet asiakkaiden salassa pidettävien tietojen suojaamisesta
  - Tietojen siirto ja käsittely myös kolmansissa maissa mahdollista, edellyttää kuitenkin mm. siirtoperusteita, tapaus- ja maakohtaista tietosuojan tason ja lainsäädäntöön liittyvien riskien arviointia, riittäviä täydentäviä suojatoimenpiteitä jne.
  - Varautumisvaatimukset (esim. poikkeustilanne jossa tietoliikenneyhteydet rajoitettu Suomen sisäpuolelle) erityisen keskeisiä kriittisissä luokan A3 järjestelmissä

Modulaariset tietojärjestelmäkokonaisuudet

Aiempi usein kysytty kysymys:

- K: Miten tietojärjestelmäkokonaisuudet huomioidaan sertifioinnissa?
- V: Tietojärjestelmäkokonaisuuksia on runsaasti eri tyyppisiä, käyttäjäorganisaatioista ja eri toimijoiden keskinäisistä sopimuksista riippuen. Käytännössä yhdessä käyttöympäristöissä tai sote-organisaatiossa voi olla esim.
  - Yksi järjestelmä, jonka kautta viranomaisvaatimukset täytetään ja todennetaan
  - Useita sovelluksia joilla eri valmistajat, integraattori, välityspalvelujen tuottaja Kanta-palvelujen suuntaan, alusta- ja kapasiteettipalvelujen tarjoajia
  - Useita sertifioituja järjestelmiä eri käyttötarkoituksiin
  - Eri valmistajilta / tietojärjestelmäpalvelujen tuottajilta tulevia sovelluskokonaisuuksia
  - Järjestelyjä ja sopimuksia, joilla sertifioinnin vaatimukset pystytään täyttämään useiden käytössä olevien järjestelmien kautta
  - Järjestelmiä kehitettäessä ja hankittaessa on tärkeää hahmottaa, mitkä olennaiset vaatimukset ja sertifiointimenettelyt kutakin osajärjestelmää koskevat

Modulaariset tietojärjestelmäkokonaisuudet

Määräys 5/2021 Liite 1 luku 6.3

- Tietojärjestelmät entistä vähemmän irrallisia / ”itsenäisiä” monoliitteja
- Määräyksissä selkeytetty **osajärjestelmien** roolia
  - Aiemmissa säädöksissä ”tietojärjestelmäpalvelu” käsite koettu epämääräiseksi
  - Osana laajempaa kokonaisuutta toimiva osajärjestelmä on mahdollista luokitella, sertifioida ja rekisteröidä
  - Sertifiointia voidaan tehdä useille toisiinsa liittyville osajärjestelmille ”kerralla”
    - esim. kuvantamisen tietojärjestelmäkokonaisuuksissa jo toimittu näin
  - Järjestelmä tai osajärjestelmä voi täyttää olennaisia vaatimuksia toisen siihen liitettäväksi tarkoitetun järjestelmän kautta, kun dokumentointi- ja todentamisvaatimukset pystytään täyttämään
- Keskeistä
  - Määritellä selkeästi rajaukset ja vastuut: mitä kuuluu osajärjestelmään, mitkä vaatimukset täytettävä muiden liittyneiden (osa)järjestelmien kautta
  - Sertifioinnissa oltava selkeä kuvaus kokonaisuuteen kuuluvista osajärjestelmistä ja niiden vastuutahoista
  - Osajärjestelmän käyttötarkoituskuvaus ml. profiilien mukaisuus, järjestelmälomake, rekisteröinti, riskitasoarvio itsenäisesti, mutta kokonaisuus huomioiden
  - Esim. järjestelmälomakkeella ”U”-merkinnät: vaatimus täytetään toisen järjestelmän tai rajapinnan kautta, lisätietoja kohdassa ilmaistava tarkemmin

Profiili 3g1: Asiakas- tai potilastietojen käsittelyyn tarkoitettu järjestelmä (sis. luokka B tai A1)

Määräys 5/2021 Liite 3g

- Säädöksistä suoraan nousevat asiakastietojen käsittelyn perusvaatimukset kokoava profiili
- Kohteena kaikki potilastietojen tai sosiaalihuollon asiakastietojen sähköiseen käsittelyyn suunnitellut tietojärjestelmät
  - Sisältää myös luokkaan B tai A1 kuuluviin järjestelmiin kohdistuvat vaatimukset
  - Riippumaton siitä liittyykö Kanta-palveluihin, onko sertifioitava tai kuinka laajaa asiakastietojen käsittely on
- Kanta-palveluihin liittyviä vaatimusmäärittelyjä / lähteitä ei sovelleta
  - Joissakin lähteissä kuitenkin tarkempi kuvaus siitä kuinka lakisääteinen vaatimus toteutettavissa
- Profiilia ei tarvitse ilmoittaa erikseen järjestelmissä, jotka täyttävät muita profiileja
  - Kaikissa muissa profiileissa otettu kantaa 3g1 sisältämiin vaatimuksiin
- Järjestelmälomakkeeseen merkitään normaalisti myös muut kuin profiilista nousevat vaatimukset
  - Myös muut kuin profiilissa olevat toiminnot, tietosisällöt ja tietoturvavaatimukset ilmoitettava ja todennettava / ilmoitettava normaalisti - sen mukaisesti, mitä järjestelmään toteutettu

Poikkeamat vaatimustenmukaisuudesta

Määräys 5/2021 luku 10.4

- Merkittäviä poikkeamia (AsTL 32 §, 41 §) ovat poikkeamat, jotka tuotantokäytössä aiheuttaisivat
  1. Riskejä asiakas- tai potilasturvallisuudelle
  2. Merkittäviä riskejä tietosuojalle, tietoturvallisuudelle tai sote-palvelujen toiminnalle
  3. Poikkeamat olennaisista vaatimuksista jotka aiheuttavat merkittäviä tai pitkäaikaisia heijastusvaikutuksia tai lisäpoikkeamia useille palvelunantajille tai useille muille tietojärjestelmille
  4. Tietojen oikeellisuudelle, eheydelle tai yhteentoimivuudelle laajamittaisia häiriöitä aiheuttavat poikkeamat
  5. Tuotantokäytössä toimivan järjestelmän tietoturvallisuustodistuksen vanheneminen (tarkennuksin)
  6. Tuotantokäytössä toimivassa järjestelmässä toteutettujen ominaisuuksien perustuminen vanhentuneeseen määrittelyversioon (tarkennuksin)
  7. Säädöksissä asetettujen tai viranomaisten asettamien määräaikojen noudattamattomuus järjestelmään edellytettäville korjauksille (tarkennuksin)
  8. Muut valvontaviranomaisen merkittäväksi poikkeamaksi toteamat poikkeamat

Poikkeamat vaatimustenmukaisuudesta

Määräys 5/2021 luku 10.4

- Merkittävistä poikkeamista ilmoitettava AsTL 32 § ja 41 § mukaisesti
- Ryhdyttävä toimenpiteisiin merkittävän poikkeaman korjaamiseksi
- Suunniteltava korjaus- tai jatkotoimenpiteet riskiarvion perusteella
- Sertifiointia ei voida hyväksytysti suorittaa loppuun jos löytyy sellainen poikkeama olennaisista vaatimuksista, joka johtaisi merkittävään poikkeamaan tuotantokäytössä
- Valvira julkaisee tietoa poikkeamista osana tietojärjestelmien rekisteriä ja voi tehdä tarkastuksia, antaa määräyksiä velvollisuuksien täyttämiseksi tai puutteiden korjaamiseksi, asettaa käyttökiellon ja tehostaa antamaansa määräystä tai päätöstä uhkasakolla
- Tietojärjestelmäpalvelun tuottaja tai palvelunantaja eivät saa ottaa tuotantokäyttöön järjestelmää, johon Valviran tietojärjestelmärekisteristä löytyvien tietojen perusteella kohdistuu merkittävä poikkeama, joka estää tuotantokäyttöönoton

Määräysten voimaantulo ja siirtymä aiemmista säädöksistä
Määräys 4/2021 Luku 12

- Määräysten mukaiset menettelyt astuvat voimaan heti määräysten tullessa voimaan
- Aiempien säädösten mukaiset vaatimustenmukaisuustodistukset säilyvät voimassa
  - Uusittava kuitenkin tietoturvallisuustodistukseksi ennen aiemman vaatimustenmukaisuuden umpeutumista, ja viimeistään 3v kuluessa uuden lain voimaantulosta
  - Aiemmin hyväksytyt järjestelmät toimivat tuotannossa ja voidaan ottaa käyttöön voimassaoloaikana
  - Uusiminen AJOISSA, vireille viimeistään 6kk ennen aiemman vaatimustemukaisuuden päättymistä
- Käynnissä olevat sertifiointiprosessit (ennen 1.9.2021 käynnistetty) voidaan suorittaa loppuun prosessin käynnistyessä voimassa olleiden vaatimusten mukaisesti, 6kk
  - Asiasta erillinen merkintä myönnettävään todistukseen, uuden lain mukainen 3v voimassaoloaika
- Aiemmin sertifioitujen luokittelu ja vaatimusten täyttäminen tarkennettava seuraavan sertifioinnin ja Valviralle tehtävän ilmoituksen yhteydessä
- Jos ei tarvita uutta sertifiointia, Valviran tietojärjestelmärekisterin tiedot päivitettävä 1 vuoden kuluessa lain voimaantulosta tai Valviran tarkempien ohjeiden mukaisesti
- Jos (tuotantokäyttöön aiemmin rekisteröity) tietojärjestelmä siirtyy luokasta B luokkaan A, suoritettava sertifiointi voimassa olevien vaatimusten mukaisesti viimeistään kolmen vuoden kuluessa lain voimaantulosta
  - Voi edellyttää järjestelmään / arkkitehtuuriin ja toimijoiden vastuisiin tehtäviä muutoksia
  - Huom. käyttöönoton edellytyksenä joka tapauksessa voimassa olevien vaatimusten mukaisuus
  - Huom. jos aiemmin Kanta-palveluihin liittymätön järjestelmä liittyy Kanta-palveluihin (myös toisen järjestelmän kautta), on luokiteltava ja tarvittaessa sertifioitava ennen liittymistä

Vaatimusten ja profiilien voimassaolo

Määräys 5/2021 liite 1, luku 6.1, Määräys 5/2021 luku 12

- *Profiilin voimaantulopäivä sertifioinnissa ja ilmoituksissa:* profiilin mukaisia vaatimuksia sovelletaan yhteistestauksessa, tietoturvallisuuden arvioinnissa ja Valviran tietojärjestelmärekisteriin tehtävissä ilmoituksissa (huom. edellisen kalvon siirtymätarkennukset), jos järjestelmän käyttötarkoitus on profiilin mukainen
- *Profiilissa yksittäisen vaatimuksen kohdalla näkyvä päivämäärä:* ajankohta, jolloin vaatimus on astunut tai astuu voimaan profiilin mukaisissa tuotannossa toimivissa tietojärjestelmissä
  - Monet vaatimuksista perustuvat jo pitkään voimassa olleisiin säädöksiin tai määrittelyihin, ”voimassa”
  - Asiakastietolain siirtymäsäännöksissä tuotantokäytön voimaantuloaikoja mm. eri tietosisältöjen ja seikkojen vaiheistukseen
- Viitattujen määritysten (erityisesti Kanta-vaatimukset) voimassaolo huomioitava vaatimusten toteuttamisessa
  - THL tai Kela julkaisevat tiedot siitä, mitkä ovat voimassa olevia määrityksiä ja määritysversioita, ja mitä määrittelyversioita edellytetään esim. yhteistestauksessa
- Määräykset eivät vaikuta asiakastietolaissa asetettuihin määräaikoihin esim. Kanta-liittymisten suhteen, ks. asiakastietolaki 52 §

Yhteenveto

Olennaisten vaatimusten ja sertifioinnin keskeisiä muutoksia verrattuna aiempiin säädöksiin

- Järjestelmien **luokittelu** täsmentyy (B, A1, A2, A3)
  - Tietoturvallisuuden arviointiin myös muita kuin Kanta-palveluihin liittyviä järjestelmiä (A1)
  - Järjestelmien käyttötarkoituksen, kriittisyyden, laajuuden ja käsiteltyjen sisältöjen huomiointi vaatimusten kohdistamisessa ja todentamisessa – järjestelmän **riskitason** huomiointi vaatimuksissa ja todentamisessa
- **Tietoturvavaatimukset** osaksi **samaa perusrakennetta** kuin toiminnalliset vaatimukset (= toiminnot ja tietosisällöt)
  - Ei erillistä tietoturvavaatimusten määräystä, poistettu päällekkäisyyksiä
  - Tietoturvavaatimuksista oma osio olennaisten vaatimusten luokitukseen ja tietoturvavaatimukset osaksi profiileja (= järjestelmän käyttötarkoituksen aiempaa parempi huomiointi)
  - Myös **tekninen tietoturvatestaus** korkean riskitason järjestelmien todentamistavaksi
  - **Tietoturvallisuustodistuksen** roolin selkeyttäminen
- **Uusien järjestelmäratkaisujen** nykyistä parempi huomiointi, mm.
  - Palveluntuottajan oman toimintaympäristön ulkopuolelta hankittavien tai käytettävien palvelujen huomiointi tietojärjestelmiin kohdistuvissa tietoturvallisuusvaatimuksissa
  - Modulaariset järjestelmäkokonaisuudet, asiakastietojen ensiokäytön asiointi- ja tietoallasratkaisut jne.
- **Merkittävät poikkeamat** määritelty
- 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

Yhteenveto: olennaisten vaatimusten, luokittelun ja sertifioinnin määräykset – ohjaavat:

- **Täsmentävät** tietojärjestelmien vaatimustenmukaisuuteen ja sertifiointiin liittyvät velvoitteet
- **Kokoavat yhteen** vaatimukset, joita kansallisesti asetetaan asiakas- ja potilastietoja käsitteleville tietojärjestelmille
  - **auttavat tunnistamaan** eri järjestelmiä ja toimijoita koskevat vaatimukset
- Mahdollistavat **olennaisten vaatimusten yhdenmukaisen ryhmittelyn ja viestinnän** sote-tietojärjestelmien kehittämisessä ja hankinnoissa
- Ohjeistavat ja yhdenmukaistavat **lain ja määräysten mukaista sote-tietojärjestelmien käyttötarkoitusten viestintää**
  - ilmoitukset, Valviran rekisteri, sertifioinnin testaus- ja tietoturva-osiot, hankinta- ja kehittämisprojektit

Yhteenveto: olennaisten vaatimusten luokittelun ja sertifioinnin määräykset – tukevat:

- Tukevat **tietojärjestelmien valmistajia ja tietojärjestelmäpalvelujen tuottajia** lakisääteisten vaatimusten täyttämisessä ja tulkitsemisessa sekä omien ratkaisujen toiminnallisten ominaisuuksien määrittelemisessä suhteessa määrittelyihin
  - myös suhteessa kumppaneihin ja työnjakoon eri järjestelmien välillä
  - sama järjestelmälomake yhteistestauksessa, tietoturvallisuuden arvioinnissa ja rekisteri-ilmoituksissa
- Tukevat **sote-toimijoita** omien tietojärjestelmäratkaisujensa olennaisten vaatimusten täyttämisessä, ml. sote-uudistuksen ja hyvinvointialueiden järjestäjät ja tuottajat
  - riskien hallinta, palvelujen jatkuvuuden turvaaminen, toimialasidonnaisten tietojärjestelmien keskeiset ominaisuudet suunniteltava myös sote-uudistuksen yhteydessä (järjestämislaki)
  - tietoturvallisuuden, tietosuojan ja tiedonhallinnan jatkumon muodostaminen mm. tietoturvasuunnitelmaan liittyen (ks. myös määräys 3/2021)
- Selkeyttävät Kanta-palvelujen kehittämiseen ja muiden kansallisten tiedonhallinnan määrittelyjen rakennetta
  - ja määrittelyjen / vaatimusten linkitystä kehitys- ja sertifiointitoimenpiteisiin
  - myös 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 määräykset – olennaista tietojärjestelmäpalvelun tuottajan näkökulmasta

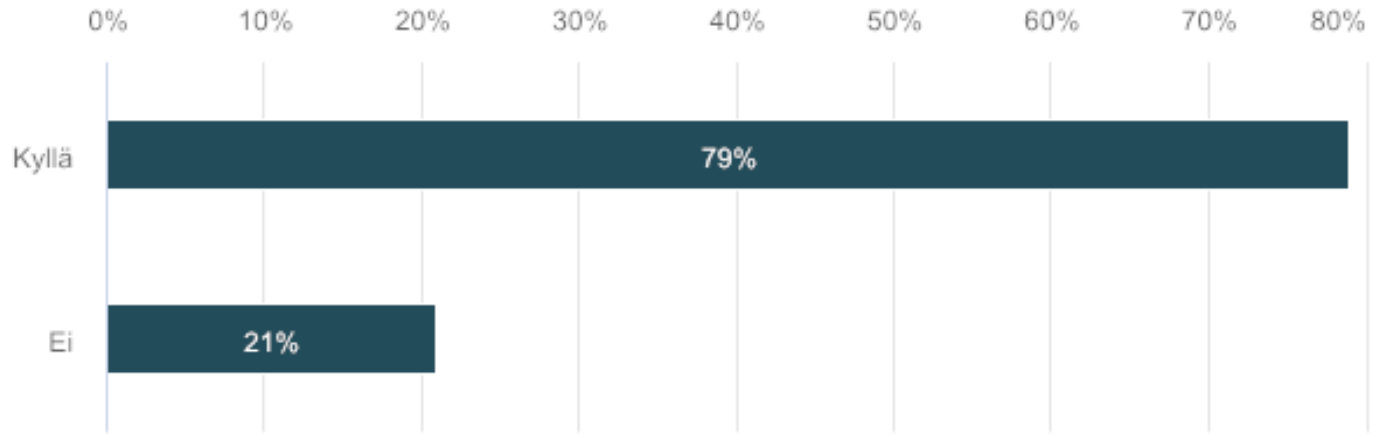
- Tietojärjestelmäpalvelun tuottajan ja valmistajan perusvastuut ja pääosa vaatimuksista eivät muutu aiemmasta, mutta omien tuotteiden ja palvelujen osalta on syytä tarkistaa ja tarvittaessa päivittää asiat:
  1. Kuvaa järjestelmän käyttötarkoitus ja määrittele järjestelmän luokka
  2. Perehdy olennaisiin vaatimuksiin (myös päivitettyihin)
     - 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 A1, A2 tai A3
  6. Tee ilmoitus Valviran tietojärjestelmärekisteriin ennen tuotantokäyttöönottoa
  7. Huomioi vastuut ja vaatimukset sopimuksissa (asiakassopimukset, kumppanuudet), tue asiakkaita käyttöönotossa ja olennaisten vaatimusten toteutumisen varmistamisessa
  8. Huolehdi muutoshallinnasta ja päivityksistä sekä olennaisten vaatimusten seurannasta

Olennaisten vaatimusten hyödyntämismahdollisuuksia tietojärjestelmien tuotekehityksessä ja tarjouspyyntöihin vastaamisessa

- Riskienhallinta ja laadunvarmistus
  - Erityisesti lainsäädäntöjohdannaiset riskit, tietoturvallisuus, tietuoja
- Tuotekehityksen suunnittelu suhteessa olennaisiin vaatimuksiin ja määrittelyihin
  - Relevanttien olennaisten vaatimusten systemaattinen läpikäynti suhteessa tuotteisiin
  - Erityisesti Kanta-palveluihin liittyvien tarkempien vaatimusten koonti
  - Yhteistyö ja työnjako kumppanien ja asiakkaiden kanssa ”tämä vaatimus täytetään ympäristössä X järjestelmän Y kautta..”
  - Sertifiointi on sitä sujuvampaa, mitä paremmin kehitystyössä on huolehdittu riittävistä tietoturvamenettelyistä, riskienhallinnasta, dokumentoinnista, omasta testauksesta ja määrittelyjen mukaisuudesta
- Viestintä, myynti ja markkinointi
  - ”profiilien XX, YY ja ZZ mukaiset vaatimukset täyttävä järjestelmä”
  - ”tasolla A3/A2/A1 sertifioitu järjestelmä”
  - järjestelmälomake osana sertifiointia ja tarjouspyyntöihin vastaamista

Jatkokehitys

- STM valmistelee sote-tiedonhallintasäädösten kokonaisuudistusta
- Tulossa myös uusia ja päivitettyjä asetuksia / STM (mm. käyttöoikeudet)
- Uudet ja päivittyvät kansalliset määrittelyt heijastuvat myös olennaisiin vaatimuksiin
- Uudistamisessa huomioidaan ja arvioidaan myös muu kuin jo määräyksiin vaikuttanut lausunnoilla annettu palaute, esim.
  - ”Tulisiko kansallisten vähimmäisvaatimusten profiileja kohdistaa jatkossa myös sote-palvelutuottajien käyttämiin tietojärjestelmäkokonaisuuksiin (ei pelkästään tietynkäyttötarkoituksen mukaisiin tietojärjestelmätuotteisiin / tietojärjestelmäpalvelujen tuottajiin)?”



Yhteenveto

- Valtakunnallisten määräysten mukaiset olennaiset vaatimukset ovat *vähimmäisvaatimuksia*
- Vaatimusten avain on tietojärjestelmän *käyttötarkoitus*
  - määrittelee, mitä tarkempia vaatimuksia on toteutettava ja mille tasolle
- Järjestelmät (mukaan lukien Kanta-palvelut) ja sote-palveluntuottajien toimintatavat muodostavat jatkumon, jossa kokonaisuutena huolehdittava yhteentoimivuudesta, tietosuojasta ja tietoturvasta
- Kanta-palvelujen kautta tapahtuva tietojen yhteiskäyttö asettaa vaatimuksia kaikille liittyville tahoille ja järjestelmille
- Lisäksi huomioitava muu lainsäädäntö mm. henkilötietojen suojaamiseen liittyvät tietosuojavaatimukset, lääkinnällisten laitteiden säädökset jne.
- Sertifiointi on sitä sujuvampaa, mitä paremmin kehitystyössä on huolehdittu riittävistä tietoturvamenettelyistä, riskienhallinnasta, omasta testauksesta ja määrittelyjen mukaisuudesta, mukaan lukien järjestelmien päivittäminen voimassa olevien vaatimusten ja määrittelyjen mukaiseksi
- Viranomaisvalvonta täydentää eri toimijoiden omia menettelyjä
- Vaatimuksia ja menettelyjä kehitetään jatkuvasti yhteistyön ja saatujen kokemusten kautta

Materiaalit

- Viranomaisten määräyskokoelmat: Terveyden ja hyvinvoinnin laitos: https://www.finlex.fi/fi/viranomaiset/normi/561001/
- THL Määräykset: https://thl.fi/fi/web/tiedonhallinta-sosiaali-ja-terveysalalla/maaraykset-ja-maarittelyt/maaraykset
- THL sote-tiedonhallinta / koulutusmateriaalit: https://thl.fi/fi/web/tiedonhallinta-sosiaali-ja-terveysalalla/ohjeet-ja-soveltaminen/koulutusmateriaalit
- Kanta.fi / Sertifiointi, olennaiset vaatimukset ja omavalvonta: https://www.kanta.fi/jarjestelmakehittajat/sertifiointi
- Valvira / Sosiaali- ja terveydenhuollon tietojärjestelmät: https://www.valvira.fi/terveydenhuolto/sosiaali-ja-terveydenhuollon-tietojarjestelmat
- Kanta-julkaisuaikataulu: https://www.kanta.fi/jarjestelmakehittajat/julkaisuaikataulu

Kiitos!

- tapahtuman osallistujille
- lausunnonantajille
- valmisteluprojektiin ja yhteistyöryhmiin osallistuneille

Kysymykset

Kysymyksiä voi lähettää myös osoitteeseen
sotetiedonhallinta@thl.fi