Sote-tietojärjestelmien olennaiset vaatimukset ja sertifiointi

THL määräykset 4/2024 ja 5/2024

14.6.2024

Juha Mykkänen

Terveyden ja hyvinvoinnin laitos

Ohjelma

- Klo 9.00 - 9.10 Tilaisuuden avaus, tavoitteet ja kulku
- Klo 9.10 - 10.30 Uudistuneet THL:n määräykset 4/2024 ja 5/2024
- Klo 10.30 - 10.40 Tauko
- Klo 10.40 - 11.10 Kelan puheenvuoro ja keskustelua
- Klo 11.10 - 11.40 Valviran puheenvuoro - Ajankohtaista asiakastietolain mukaisesta rekisteröinnistä
- Klo 11.40 Kysymyksiä ja keskustelua
- Klo 12.00 Tilaisuuden päätös

Mitä olennaiset vaatimukset ovat ja miten ne täytetään?

Mitkä olennaiset vaatimukset koskevat järjestelmääni?

Mihin luokkaan järjestelmäni kuuluu?

Miten laissa vaadittu selvitys annetaan?

Millainen prosessi sertifiointi on?

Mitä yhteistestaukseen kuuluu?

Mitä tietoturvallisuuden arviointiin kuuluu?

Miten näitä asioita valvotaan?

Tämän osion sisältö

- Tietojärjestelmien ja hyvinvointisovellusten olennaiset vaatimukset, luokittelu ja sertifiointi määräysten 4/2024 ja 5/2024 pohjalta
  - Perusteet ja rajaukset
  - Järjestelmien luokittelu ja riskitaso
  - Olennaiset vaatimukset, profiilit ja järjestelmälomake
  - Sertifiointiprosessi
  - Muutokset aiempiin säädöksiin
  - Nostoja merkittävimmistä täydennyksistä aiempiin määräyksiin
  - Erityiskysymyksiä: poikkeamat, vaatimusten voimassaolo, EU-kehitysnäkymiä
  - Yhteenveto

Oppimistavoitteet:

1) yleiskuva,
2) tieto aiempiin säädöksiin verrattuna muuttuneista asioista ja
3) lisätietojen löytämisen helpottaminen

Sote-tiedonhallinnan määräykset 2024

- 1.1.2024 voimaan tulleen asiakastietolain pohjalta THL on päivittänyt joukon valtakunnallisia sote-tiedonhallinnan määräyksiä
  - 1/2024 Määräys sosiaalihuollon asiakasasiakirjoista
  - 2/2024 Määräys valtakunnallisten tietojärjestelmäpalveluiden avulla terveydenhuollon ulkopuolelle välitettävistä asiakirjoista
  - 3/2024 Määräys tietoturvasuunnitelmaan sisällytettävistä selvityksistä ja vaatimuksista
  - **4/2024 ja 5/2024 Määräykset sosiaali- ja terveydenhuollon tietojärjestelmien ja hyvinvointisovellusten olennaisista vaatimuksista, sertifioinnista ja luokittelusta**

Uutiset ja linkit

- Uutinen 6.5.2024 Päivitetyt määräykset sote-tietojärjestelmien olennaisiin vaatimuksiin ja sertifiointiin
- Uutinen 28.3. 2024 Määräys sosiaalihuollon asiakasasiakirjoista on julkaistu
- Uutinen 20.2.2024 Määräys tietoturvasuunnitelmaan sisällytettävistä selvityksistä ja vaatimuksista on julkaistu
- Uutinen 26.1.2024 Valtakunnallisten tietojärjestelmäpalveluiden avulla välitettävistä asiakirjoista on julkaistu uusi määräys

- THL määräykset Finlex-palvelussa
- THL määräykset-sivu
- Asiakastietolaki 703/2023

Perusteet ja rajaukset

Esityksen painopiste: tietojärjestelmien ja hyvinvointisovellusten olennaiset vaatimukset, luokittelu ja sertifiointi

Uusia ja vanhoja riskejä ja uhkia...

TIETOTURVA

OmaKanta-huijaus yrittää viedä rahasi – näin sen erottaa aidosta sivusta

TIETOTURVA | Marjukka Puolakka

17.4.2015 klo 07:00

Ovatko henkilökohtaiset terveystiedot turvassa? - Yhdysvalloissa 29 miljoonaa tietorikkomusta

JAA ARTIKKEL

MAA

TT: Vastaamon uhreja on päätyn tsemurhaan

Asiasta kertoo STT:lle uhreja edustava juristi.

TIETOSUOJARIKOS

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

Jokaisella on oikeus tietää omi käsittelystä. P

TIETOTURVA

82 % 16.18

LAPIN KESKUSSAIRAALA

SAMI GUOVDDASBUOHCCEVIESSU

yle UUTISET

Rovaniemi tänään 10:12

It-vika pysäytti Lapin keskussairaalan

Lapin kesku poliklinikkak tietojärjestel

Vika havaittiin t

TIETOTURVA

Karmea saldo yhdelle päivälle: Kiristäjät iskivät 6 sairaalaan

Verkkokiristyksen iljettävä muoto on yleistynyt Yhdysvalloissa j ihmishenkiä.

Potilasturvallisuus

Kalkkitabletti vaihtui psyykenlääkkeeksi: Viisi potilasta s väärän lääkkeen

esti sen, että joku

johtaja sanoo, että

TIETOTURVA

Kyberhyökkäys kaatoi Irlannin terveydenhuollon – tietokoneet pimeinä sairaalassa

Vain koronarokotusohjelma sääst terveydenhu

ensa

ita

ntarjoajan

yle Etusivu Vaalikone Venäjän hyökkäys UMK24

Teknologia

Tekoälyn tekemät monimutkaiset huijaukset lisääntyvät Suomessakin muutaman vuoden sisään, asiantuntij ennakoi

kimaan ihmisääntä keräämänsä aineiston

olla huijausta.

Uutinen

Microsoftilta varoitus Azure-käyttäjille: pilvikontissa oli vuoto

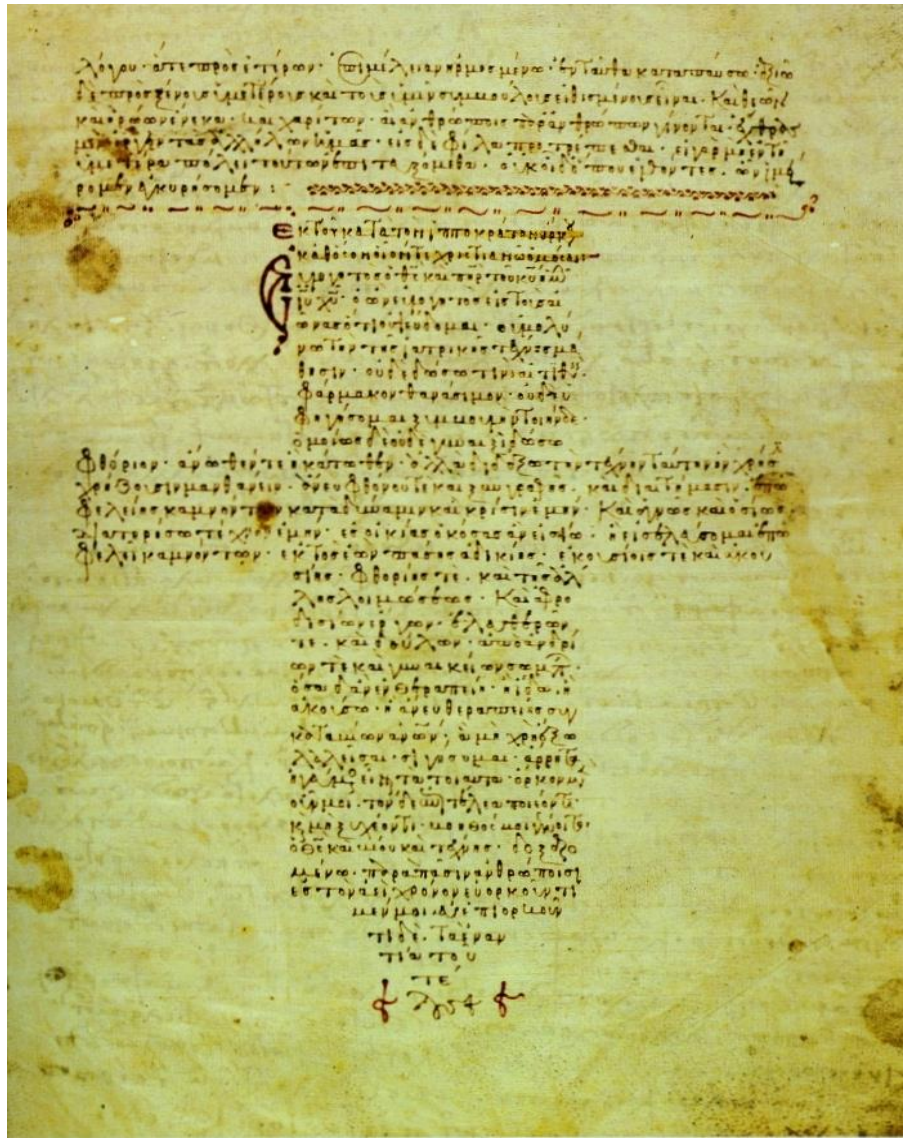
9.9.2021 13:08 | päivitetty 9.9.2021 13:08

Azuren 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)



Koulutuksen fokus

- Sote-tietojärjestelmien sekä hyvinvointisovellusten **olennaiset vaatimukset** ja niiden **todentaminen ja sertifiointi**
  - Asiakastietolain velvoitteet sote-tietojärjestelmille ja hyvinvointisovelluksille
  - Kansalliset ”vähimmäisvaatimukset” eri käyttötarkoituksiin tehdyille järjestelmille
  - Pääfokus: sosiaali- ja terveydenhuollon asiakastietojen käsittelyyn tarkoitetut järjestelmät
    - Kanta-palveluihin liittyvät
    - Muut potilastietojen ja sosiaalihuollon asiakastietojen käsittelyyn tarkoitetut
    - Myös asiakastietolain tarkoittamat hyvinvointisovellukset
  - Erityisesti järjestelmien valmistajiin ja tietojärjestelmäpalvelujen tuottajiin kohdistuvat vaatimukset
  - Sekä julkisissa että yksityisissä palveluissa käytettävät tietojärjestelmät
  - Sekä sosiaali- että terveyspalveluissa käytettävät tietojärjestelmät
- Rajaukset päivän ohjelmassa
  - **pääfokus** tilaisuudessa tänään sote-ammattilaisten käyttämät järjestelmät, hieman sisältöä kuitenkin myös asiakkaille tarjottavista hyvinvointisovelluksista ja muista digipalveluista
  - sote-palveluntuottajien tietoturvasuunnitelmat ja siihen liittyvät tietosuoja- / tietoturvallisuusasiat eivät ole pääaiheena (tästä aiheesta oli erillinen koulutus 4.6.2024)
  - ei käsitellä yksityiskohtaisesti lääkinnällisten laitteiden säädöksiä (mm. MDR, ISO 13485) tai niihin liittyviä menettelyjä: huomioitava erikseen
  - asiakastietolain määräysten kohteena eivät ole toisiolain mukaiset tietojen käyttötarkoitukset

Asiakastietolakiin perustuvien olennaisten vaatimusten ja sertifioinnin (määräysten) tavoitteet

Riskien hallinta

- erityisesti tietoturvallisuus ja tietosuoja, oikeudelliset riskit ja yhteentoimivuus
- tietojärjestelmätoimittaja-, palvelunantaja-, käyttäjä- ja valvontanäkökulmat

Vaatimusten kokoaminen

- vaatimusluettelo = ylätason hakemisto yksityiskohtaisemmista määrityksistä ja standardeista, joiden tekemiseen osallistunut satoja asiantuntijoita, ”omaa tuotetta koskevien vaatimusten ja määritysten” löydettävyys, vaatimusten täyttymisen ilmoittamiseen käytettävä järjestelmälomake

Perusvaatimusten täyttymisen varmistaminen

-kansallisten kehittämistavoitteiden toimeenpano
- lainmukaisuuden varmistaminen + perusvaatimustaso eri käyttötarkoituksiin tehdyille järjestelmille ja sovelluksille (olennaisten vaatimusten profiilit, voimassaoloajat)

Päällekkäisyyksien välttäminen

- esim.: ei päällekkäistä todentamista MDR-vaatimusten kanssa (lääkinnälliset laitteet, potilasturvallisuus), pohja vaikuttavuusarvioille (HTA) ja niiden rakentuminen vakaalle säädöspohjalle, entistä suurempi osa vaatimuksista suoraan kv-standardeista ja malleista, pohja EU-kehitykseen (EHDS)...

Asiakastietolaki 703/2023, olennaiset vaatimukset

- 84 § Asiakastietojen käsittelyssä käytettävän tietojärjestelmän ja hyvinvointisovelluksen tulee täyttää yhteentoimivuutta, tietoturvaa ja tietosuojaa sekä toiminnallisuutta koskevat **olennaiset vaatimukset**

Asiakastietolaki 703/2023, vaatimustenmukaisuuden osoittaminen

- 85 § Luokkaan A kuuluvan tietojärjestelmän ja hyvinvointisovelluksen vaatimustenmukaisuus on osoitettava **sertifioinnilla** eli tietojärjestelmäpalvelun tuottajan tai hyvinvointisovelluksen valmistajan antamalla **selvityksellä** siitä, että tietojärjestelmä tai hyvinvointisovellus täyttää käyttötarkoituksensa mukaiset toiminnallisuutta koskevat vaatimukset, sekä hyväksytyllä **yhteentoimivuuden testauksella** ja 87 §:n mukaisella tietoturvallisuuden arviointilaitoksen antamalla **tietoturvallisuuden arviointia koskevalla todistuksella**. Tietojärjestelmäpalvelun tuottaja tai hyvinvointisovelluksen valmistaja vastaa siitä, että tietojärjestelmä tai hyvinvointisovellus on sertifioitu.
- 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.
- Tietojärjestelmäpalvelun tuottajan tulee vakuuttaa osana vaatimuksista annettavaa selvitystä, että järjestelmässä on toteutettu ne toiminnot, jotka selvityksen mukaisesti kuuluvat järjestelmän käyttötarkoitukseen.

thl

Tietoturvasuunnitelman ja sote-tietojärjestelmien olennaisten vaatimusten säädökset

Lait (STM)

- Laki sosiaali- ja terveydenhuollon asiakastietojen käsittelystä 703/2023
  - Aiemmat versiot ja päivitykset 159/2007, 1227/2010, 250/2014, 784/2021
  - Huom. 2023 asiakastietolaissa myös muu kuin sähköinen käsittely entistä selkeämmin lain piirissä
- Laki sähköisestä lääkemääräyksestä 61/2007
  - Päivitykset: 251/2014, 786/2021 ja 706/2023

Määräykset (THL)

- Määräys 4/2024: Määräys sosiaali- ja terveydenhuollon tietojärjestelmien ja hyvinvointisovellusten luokittelusta ja sertifioinnista
- Määräys 5/2024: Määräys sosiaali- ja terveydenhuollon tietojärjestelmien ja hyvinvointisovellusten olennaisista vaatimuksista
  - Aiemmat versiot ja edeltäjät ja aiempia täydentäneet määräykset: Määräykset 1/2015, 2/2016, 4/2021, 5/2021, 6/2021, 1/2022, 1/2023
- Liittyy aiheeseen: Määräys 3/2024: Määräys tietoturvasuunnitelmaan sisällytettävistä selvityksistä ja vaatimuksista
  - Aiemmat versiot ja edeltäjät: Määräykset 3/2021 ja 2/2015

Asiakastietolain avainkohdat järjestelmien luokittelun, olennaisten vaatimusten ja sertifioinnin näkökulmasta

- 3 § **Määritelmät**
- 77 § Tietoturvasuunnitelma
- 79 § Tietojärjestelmien ja hyvinvointisovellusten **käyttötarkoitus** ja **luokittelu**
- 80 § Tietojärjestelmien ja hyvinvointisovellusten **rekisteröinti**
- 81 § Tietojärjestelmän ja hyvinvointisovelluksen **ottaminen tuotantokäyttöön**
- 82 § Tietojärjestelmän ja hyvinvointisovelluksen **käyttöönoton jälkeinen seuranta**
- 83 § **Tietojärjestelmäpalvelun tuottajan ja tietojärjestelmän valmistajan** sekä hyvinvointisovelluksen valmistajan yleiset velvollisuudet
- 84 § Tietojärjestelmälle ja hyvinvointisovellukselle asetettavat **olennaiset vaatimukset**
- 85 § **Vaatimustenmukaisuuden osoittaminen**
- 86 § **Yhteentoimivuuden testaaminen**
- 87 § **Tietoturvallisuuden arviointi**
- 88 § Kansaneläkelaitoksen ja tietoturvallisuuden arviointilaitoksen ilmoittamisvelvollisuus
- 89 § Tietojärjestelmien valvonta ja tarkastukset
- 90 § Ilmoittaminen tietojärjestelmän ja hyvinvointisovelluksen **olennaisten vaatimusten poikkeamista** sekä tietoverkkoihin kohdistuvista tietoturvallisuuden häiriöistä
- 97 § **Ohjaus, valvonta ja seuranta**
- 102 § Siirtymäsäännökset

Lähtökohtia – nostoja määritelmistä / AsTL 3 § - tietojärjestelmä

- ***tietojärjestelmä*** on *”valmistajan suunnittelemien ominaisuuksien mukaisesti tarkoitettu käytettäväksi asiakastietojen sähköiseen käsittelyyn, asiakasasiakirjojen tallentamiseen valtakunnallisiin tietojärjestelmäpalveluihin 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 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”*

Lähtökohtia – nostoja määritelmistä / AsTL 3 § - hyvinvointisovellus

- *hyvinvointisovellus* on *”sovellus, joka liittyy omatietovarantoon ja jolla käsitellään hyvinvointitietoa, sekä sovellus, johon henkilö voi saada asiakastietonsa valtakunnallisesta asiakastietovarannosta, reseptikeskuksesta tai tiedonhallintapalvelusta”*
- *lain ja määräysten termi ”hyvinvointisovellus” koskee VAIN Kanta-palveluihin liittyviä hyvinvointisovelluksia*
- laissa käytetään termiä ”hyvinvointisovelluksen valmistaja” usein kuvaamaan samoja velvoitteita, joita asetetaan tietojärjestelmäpalvelun tuottajalle, mutta kohdistuen hyvinvointisovelluksiin

Asiakastietolaki 83 § - 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
- Hyvinvointisovelluksen valmistaja on vastuussa **hyvinvointisovelluksen suunnittelusta ja valmistuksesta**
- 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

thl

Asiakastietolaki 79 § ja 84 §: käyttötarkoitus, luokittelu ja olennaiset vaatimukset

79 §

- Tietojärjestelmäpalvelun tuottajan on laadittava kuvaus tietojärjestelmänsä ja hyvinvointisovelluksen valmistajan hyvinvointisovelluksensa käyttötarkoituksesta ja siitä, kuinka se täyttää sitä koskevat olennaiset vaatimukset
- Tietojärjestelmät ja hyvinvointisovellukset on jaoteltava käyttötarkoituksensa ja ominaisuuksien perusteella luokkiin A ja B

84 §

- Asiakastietojen käsittelyssä käytettävän tietojärjestelmän ja hyvinvointisovelluksen tulee täyttää yhteentoimivuutta, tietoturvaa ja tietosuojaa sekä toiminnallisuutta koskevat olennaiset vaatimukset
- Hyvinvointisovelluksen tulee täyttää saavutettavuusvaatimukset
- Vaatimusten on täytyttävä käytettäessä tietojärjestelmää sekä itsenäisesti että yhdessä muiden siihen liitettäväksi tarkoitettujen tietojärjestelmien kanssa
- Olennaiset vaatimukset voidaan täyttää yhden tai useamman tietojärjestelmän muodostaman kokonaisuuden kautta

Käyttötarkoituksen kuvaamisesta, luokittelusta ja olennaisten vaatimusten täyttämisestä vastaa tietojärjestelmäpalvelun tuottaja
Hyvinvointisovelluksissa hyvinvointisovelluksen valmistaja
Palvelunantajan on varmistettava olennaisten vaatimusten toteutuminen käyttämissään tietojärjestelmissä

Asiakastietolaki 85 § Vaatimustenmukaisuuden osoittaminen

- 85 § Luokkaan A kuuluvan tietojärjestelmän ja hyvinvointisovelluksen vaatimustenmukaisuus on osoitettava **sertifioinnilla** eli tietojärjestelmäpalvelun tuottajan tai hyvinvointisovelluksen valmistajan antamalla **selvityksellä** siitä, että tietojärjestelmä tai hyvinvointisovellus täyttää käyttötarkoituksensa mukaiset toiminnallisuutta koskevat vaatimukset, sekä hyväksytyllä **yhteentoimivuuden testauksella** ja 87 §:n mukaisella tietoturvallisuuden arviointilaitoksen antamalla **tietoturvallisuuden arviointia koskevalla todistuksella**. Tietojärjestelmäpalvelun tuottaja tai hyvinvointisovelluksen valmistaja vastaa siitä, että tietojärjestelmä tai hyvinvointisovellus on sertifioitu.
- 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.
- Tietojärjestelmäpalvelun tuottajan tulee vakuuttaa osana vaatimuksista annettavaa selvitystä, että järjestelmässä on toteutettu ne toiminnot, jotka selvityksen mukaisesti kuuluvat järjestelmän käyttötarkoitukseen.

thl

Asiakastietolaki 81 § Tietojärjestelmän ja hyvinvointisovelluksen ottaminen tuotantokäyttöön

Edellytykset (luokka A ja luokka B)

- Ajantasaiset tiedot Valviran tietojärjestelmärekisterissä

Luokka A lisäksi

- Tuotantokäyttöönoton ja Kanta-palveluihin liittämisen edellytyksenä sertifiointi
- Tietoturvallisuustodistus ei saa olla vanhentunut
- Hyväksytyt yhteentoimivuuden testaukset voimassa olevien yhteentoimivuutta koskevien vaatimusten osalta (jos yhteistestattava järjestelmä tai hyvinvointisovellus)
- Hyvinvointisovellukset myös: terveyden ja hyvinvoinnin edistämisen käyttötarkoitus

Määräys 4/2024 sosiaali- ja terveydenhuollon tietojärjestelmien ja hyvinvointisovellusten luokittelusta ja sertifioinnista

1 Määräyksen tarkoitus

2 Määritelmät

3 Määräyksen soveltamisala

4 Määräyksen rajaukset ja suhde muihin säädöksiin ja dokumentteihin

5 Tietojärjestelmien ja hyvinvointisovellusten luokittelu ja yleiset vastuut

6 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 ja hyvinvointisovelluksen rekisteröinti ja valvonta

9 Tietojärjestelmän tai hyvinvointisovelluksen käyttöönoton edellytykset

10 Vaatimustenmukaisuuden uudistaminen

11 Ohjaus ja neuvonta

12 Voimaantulo ja siirtymäsäännökset

Liite 1. Esimerkkejä järjestelmien ja hyvinvointisovellusten luokittelusta

Liite 2. Luokkaan A kuuluvien tietojärjestelmien ja hyvinvointisovellusten muutosten ilmoittaminen

Tietojärjestelmän luokittelusta ja sertifioinnista vastaa tietojärjestelmäpalvelun tuottaja

Määräys 5/2024 sosiaali- ja terveydenhuollon tietojärjestelmien ja hyvinvointisovellusten olennaisista vaatimuksista

1 Määräyksen tarkoitus

2 Määräyksen soveltamisala

3 Määräyksen keskeinen sisältö ja rajaukset

4 Suhde muihin säädöksiin, ohjeisiin ja määrityksiin

5 Olennaiset toiminnalliset vaatimukset

6 Olennaiset tietoturvavaatimukset

7 Vähimmäisvaatimusten profiilit

8 Olennaisten vaatimusten täyttäminen / tietojärjestelmäpalvelun tuottaja ja hyvinvointisovelluksen valmistaja

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 määritysten versionhallinta
- 10.4 Poikkeamat vaatimustenmukaisuudesta

11 Ohjaus ja neuvonta

12 Voimaantulo ja siirtymäsäännökset

Liitteet

thl

Olennaisten vaatimusten toteuttamisesta tietojärjestelmään ja todentamisesta vastaa tietojärjestelmäpalvelun tuottaja

Palvelunantajan osaltaan huolehdittava että käytetyt tietojärjestelmät täyttävät olennaiset vaatimukset ja vastaavat palvelunantajan toimintaa

Määräys 5/2024 Liite 1 Olennaisten vaatimusten soveltamisohjeet

Jos aihepiiri on sinulle uusi, aloita tästä dokumentista!

1 Tavoitteet

2 Yleiskuva olennaisten vaatimusten käytöstä

2.1 Olennaisten vaatimusten luettelo

2.2 Vähimmäisvaatimusten profiilit

2.3 Järjestelmälomake tietojärjestelmäpalvelun tuottajan ja hyvinvointisovelluksen valmistajan työkaluna

3 Valviran tietojärjestelmärekisterin merkitys ja hyödyntäminen

4 Olennaisten vaatimusten ja profiilien hyödyntäminen sote-organisaatioissa

5 Sertifiointiprosessin soveltaminen

6 Tarkennuksia olennaisten vaatimusten soveltamiseen ja voimaantuloon

- 6.1 Vaatimusten voimaantulossa huomioitavat ajankohdat
- 6.2 Riskipohjainen vaatimusten ja todentamistapojen kohdistaminen
- 6.3 Vaatimusten kohdistaminen ja sertifioinnin velvoitteet modulaarisissa järjestelmäkokonaisuuksissa
- 6.4 Kolmansien osapuolten palveluihin liittyvät tietosuoja- ja varautumisvaatimukset
- 6.5 Hyvinvointisovellusten ja asiointipalvelujen vaatimukset ja suhde tietojärjestelmiin
- 6.6 Lääkemääräysten käsittely sekä apteekkien tietojärjestelmät ja verkkopalvelut

7 Lisätietoja määräysten 4/2024 ja 5/2024 valmistelusta

Rajauksia / määräykset 4/2024 ja 5/2024

- Määräykset **eivät vaikuta** esim. asiakastietolaissa asetettuihin **sote-toimijoiden Kanta-liittymisvelvoitteiden aikatauluihin**
- Määräykset kohdistuvat **asiakastietolain määritelmän mukaisiin** tietojärjestelmiin ja hyvinvointisovelluksiin
  - Tietojärjestelmä tai osa sitä voi olla myös lääkinnällisten laitteiden säädösten (esim. MDR) tarkoittama **lääkinnällinen laite**, jolloin valmistajan huomioitava lääkinnällisten laitteiden säädösten mukaiset luokittelut ja vaatimukset – tämä arviointi riippumaton esim. asiakastietolain mukaisesta luokittelusta
    - lääkinnällisten laitteiden säädösten mukaiset menettelyt ovat kuitenkin hyödyllisiä myös asiakastietolain mukaisten vaatimusten täyttämisessä (ja päinvastoin) – päällekkäisyydet pyritty minimoimaan
  - **Yleiskäyttöiset ohjelmistot tai alustat** eivät ole asiakastietolain tarkoittamia tai sertifioitavia tietojärjestelmiä
- 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 ole 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 ja hyvinvointisovellusten luokittelu

Määräys 4/2024 luku 5 ja liite 1

- Luokka A: sertifioitavat
  - Luokka A3: ”Kanta-palveluihin liittyvät, laajat”
  - Luokka A2: ”Kanta-palveluihin liittyvät, suppeat”
  - Luokka A1: ”tietoturvallisuuden arvioinnin suorittavat”
- Luokka B: ei-sertifioitavat
- Lisäksi: luokittelemattomat (ei asiakastietojen käsittelyyn suunniteltu tietojärjestelmä)
- Tietojärjestelmä tai hyvinvointisovellus kuuluu vain yhteen luokkaan, sen mukaan mikä on korkein luokka johon kuulumisen kriteerit se täyttää
  - Ei luokkaa < B < A1 < A2 < A3
- Esimerkkejä järjestelmien luokittelusta: Määräys 4/2024 Liite 1

Luokittelu tarkemmin 1/2

Määräys 4/2024 luku 5 ja liite 1

- Luokka A: sertifioitavat
  - Luokka A1: ”tietoturvallisuuden arvioinnin suorittavat”
    - tietoturvallisuuden arviointia vaativat järjestelmät, joilta ei edellytetä yhteistestausta
    - luokkaan voi kuulua sekä suppeampia että laajempia järjestelmiä
    - luokkaan voi kuulua laajasti asiakastietoja käsitteleviä / korkean riskitason järjestelmiä, jotka eivät liity Kanta-palveluihin
    - tekniset Kanta-välityspalvelut kuuluvat tähän luokkaan
    - 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
    - hyvinvointisovellukset (lähtökohtaisesti)
  - 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
- Esimerkkejä järjestelmien luokittelusta: Määräys 4/2024 Liite 1

Luokittelu tarkemmin 2/2

Määräys 4/2024 luku 5 ja liite 1

- Luokka B: ei-sertifioitavat
  - asiakas- tai potilastietojen käsittelyyn tarkoitetut järjestelmät
  - voi sisältää mm. erikoistuneita järjestelmiä, lääkinnällisiksi laitteiksi luokiteltuja…
  - voi sisältää järjestelmiä, joissa monet tietoturvallisuusseikat 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 4/2024 Liite 1

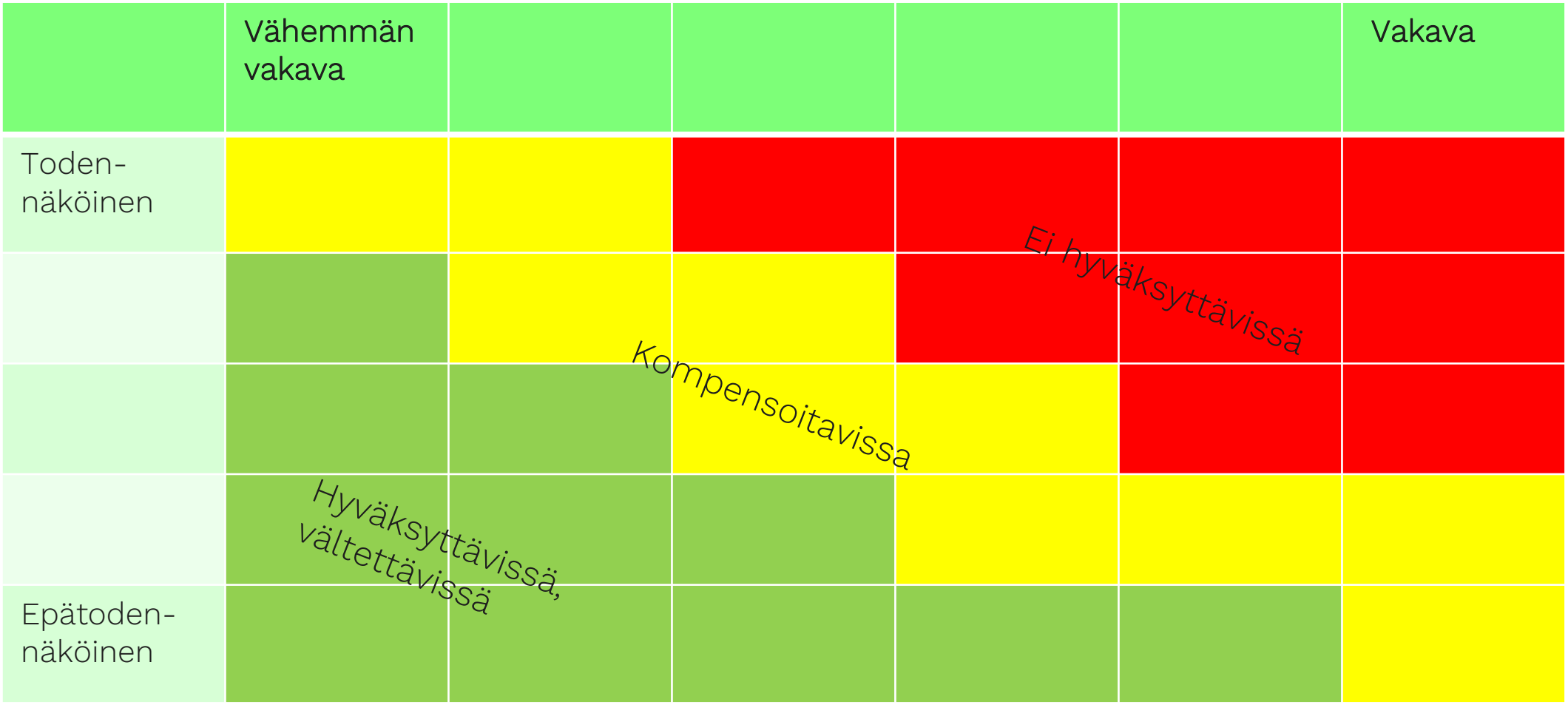
Riskitason määrittely

- 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 4/2024 tukimateriaalina)

Riski

[Ruck & Lowe]

Järjestelmän yleisen riskitason lisäksi riskien hallintaan kuuluu järjestelmän yksityiskohtiin, käyttäjiin / käyttäjäorganisaatioon ja erilaisiin käyttötilanteisiin kuuluva riskien hallinta!



Ks. myös Määräys 5/2024 liite 1, luku 6.2 Riskipohjainen vaatimusten ja todentamistapojen kohdistaminen

Luokittelun ja riskitason merkitys

- Luokittelu ohjaa:
  - Kaikki luokkiin B, A1, A2, A3 kuuluvat:
    - Täytettävä käyttötarkoitusta vastaavat olennaiset vaatimukset, ilmoitettava Valviran tietojärjestelmärekisteriin
  - A1, A2 ja A3 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…
- Täsmennykset vuoden 2024 määräyksissä
  - Kokemukset ja palaute aiemmista säädöksistä, mm. täsmennykset luokkien määräytymiseen
  - Järjestelmien luokittelusta ja siihen liittyvistä kysymyksistä saadut kokemukset (mm. riskiluokittelussa tiedon luonteen aiempaa suurempi korostaminen tiedon laajamittaisen käsittelyn sijaan)
  - Säädösten (GDPR, MDR, tiedonhallintalaki, tekoälyasetus…) riskipohjaistuminen
  - Luonnoksiin saatu lausuntopalaute, mm. pelkästään tietoja tuottavat hyvinvointisovellukset

Olennaiset vaatimukset, profiilit ja järjestelmälomake

Sote-tietojärjestelmien olennaiset vaatimukset (vuodesta 2015)

Olennaisilla vaatimuksilla:

a) ilmaistaan kansallisesti vaadittuja järjestelmien tai sovellusten ominaisuuksia

b) kuvataan järjestelmän tai sovelluksen käyttötarkoitukseen kuuluvia keskeisiä ominaisuuksia

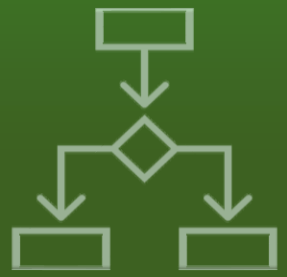
Olennaisten vaatimusten todentamisesta vastaa tietojärjestelmäpalvelun tuottaja (joka voi olla myös valmistaja)

Palvelunantajan on varmistettava olennaisten vaatimusten toteutuminen käyttämissään tietojärjestelmissä

Sote-tietojärjestelmien olennaiset vaatimukset (vuodesta 2015)

Toiminnalliset vaatimukset (luokka A ja B)

- Järjestelmien **luokittelu** ((luokittelematon), **B, A1, A2, A3**)
- Olennaiset **toiminnot** ja **tietosisällöt**, viittaukset tarkempiin määrityksiin
- Vähimmäisvaatimusten **profiilit** eri tarkoituksiin tehdyille järjestelmille
- Vakiomuotoinen **järjestelmälomake** järjestelmien rekisteröintiin ja sertifiointiin



Yhteentoimivuusvaatimukset (Kela ja THL määritykset)

- Vaatimukset ja viittaukset määrityksiin, joilla varmistetaan järjestelmän **yhteentoimivuus** Kanta-palvelujen ja muiden järjestelmien kanssa, pohjana toiminnalliset vaatimukset ja profiilit
- **Sertifiointi: yhteistestaus** Kelan kanssa (luokka A2 ja A3): Kelan yhteistestauslausunnot (Asiakastietolaki 703/2023, 86 §)

Tietoturva- ja tietosuojavaatimukset

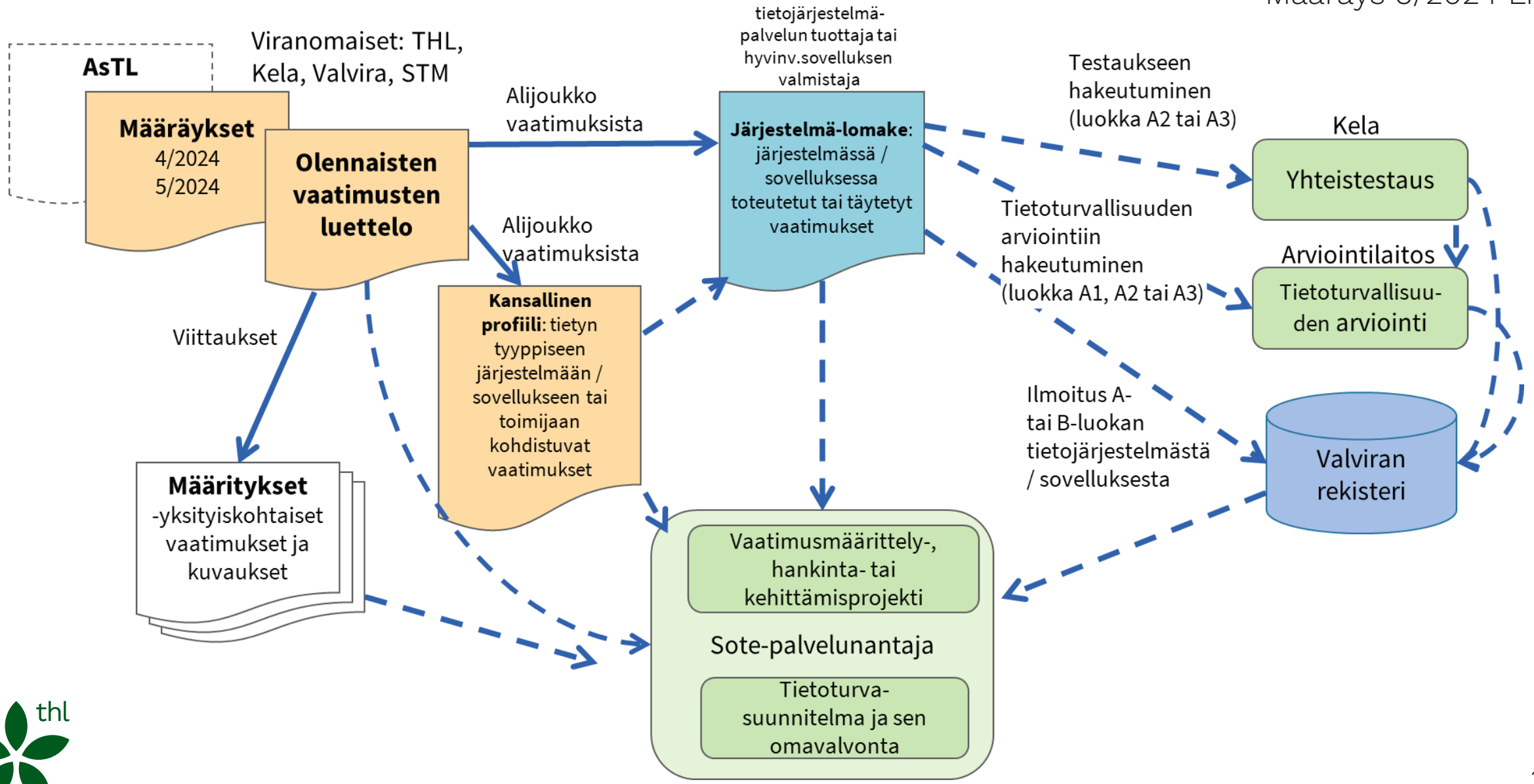
- Vaatimukset, joilla varmistetaan tietoturvallisuuden ja tietosuojan toteutuminen
- Osa linkittyy toiminnallisiin vaatimuksiin
- **Sertifiointi: tietoturvallisuuden arviointi** ulkoisen arviointilaitoksen kanssa (luokka A1, A2, A3)
- **Tietoturvallisuustodistus** hyväksytystä tietoturvallisuuden arvioinnista (voimassa max 3 vuotta)

Olennaisten vaatimusten määräys 5/2024

- *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 5/2024 luku 8
- Luokan A järjestelmän vaatimustenmukaisuus osoitettava sertifioinnilla ennen tuotantokäyttöönottoa
- Luokan A ja B tietojärjestelmät rekisteröitävä Valviran tietojärjestelmärekisteriin
- Käytännön välineenä järjestelmälomake

Olennaisten vaatimusten kokonaisuus

Määräys 5/2024 Liite 1



Olennaisten vaatimusten luettelo

Määräys 5/2024 liite 2

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

Ryhmä Tieto-sisällöt	Id	Otsikko	Selite	Lähde
TLOK		**Lokimerkintöjen tietosisällöt**		
	TLOK01 (2024)	Käyttölokia tuottavan järjestelmän lokimerkinnät	Yhtenäinen käyttölokimerkintöjen tuottamisen kansallinen tietosisältö	Asiakas- ja potilastietojen käsittelyssä syntyvien lokitietojen hallinnan kansalliset vaatimusmäärittelyt v1.2 *Katakri I-10 (Turvallisuuten liittyvien tapahtumien jäljitettävyys)*

Olennaisten vaatimusten luettelo

Määräys 5/2024 liite 2

Ryhmä Tieto-sisällöt	Id	Otsikko	Selite	Lähde
TLOK		Lokimerkintöjen tietosisällöt		
	TLOK01 (2024)	Käyttölokia tuottavan järjestelmän lokimerkinnät	Yhtenäinen käyttölokimterkintöjen tuottamisen kansallinen tietosisältö	Asiakas- ja potilastietojen käsittelyssä syntyvien lokitietojen hallinnan kansalliset vaatimusmäärittelyt v1.2 *Katakri I-10 (Turvallisuuten liittyvien tapahtumien jäljitettävyys)*

Sertifiointi		Tietosisällön muoto			Yhteydet muihin vaatimuksiin	Tarkennuksia ja huomautuksia
Yhteis-testaus-kokonaisuu	Tietoturval-lisuuden arviointi	Muu / määritte-lemätö	Näyttö-muoto	Raken-teinen muo		
	AVALO02			R	KS01, KS02, KS03, TSL07, AVALO02, TLOK02	Suositeltavaa toteuttaa tässä vaatimuksessa viitattujen loki-määritysten pohjalta hyvissä ajoin ennen profiileissa näkyvien pakollisuuksien ajankohtia. Viitatut muut vaatimukset ennen pakollisuuksia toteutettavissa myös aiempien määritysten mukaisesti.

Olennaisten vaatimusten ryhmittely / Toiminnot

Määräys 5/2024 liite 2 Olennaisten vaatimusten luettelo

TOIMINTOJEN ryhmittely	
RESL	Sähköinen lääkemääräys ja lääkitystiedot
LTOIM	Lääketoimitukset ja toimitustiedot
VV	Kanta-viestinvälitys ja muut Kanta-palvelut
ARK	Kanta asiakastietovarantoon liittyvän järjestelmän perustoiminnot
LP	Kanta-lisäpalveluihin liittyvät toiminnot
KH	Käyttäjä- ja käyttöoikeushallinta
KV	Käyttövaltuuksien tarkastaminen ja allekirjoitus
SH	Luovutusten, tahdonilmaisujen ja informointien hallinta
KS	Käytön ja luovutusten seuranta
SOS	Sosiaalihuollon asian- ja asiakkuudenhallinta
KUV	Kuvantamisen toiminnot
LPYY	Lähetteet ja pyynnöt
HTH	Henkilötietojen hallinta
ERIL	Erillisjärjestelmien Kanta-toiminnot
AV	Ajanvaraus
PTUK	Päätöksentuki

Olennaisten vaatimusten ryhmittely / Toiminnot

Määräys 5/2024 liite 2 Olennaisten vaatimusten luettelo

TOIMINTOJEN ryhmittely		
RESL	Sähköinen lääkemääräys ja lääkitystiedot	Sähköisen lääkemääräyksen tekemiseen ja käsittelyyn ja lääkitysmerkintöjen käsittelyyn tarkoitettujen järjestelmien toiminnot
LTOIM	Lääketoimitukset ja toimitustiedot	Lääketoimitusten tekemiseen käytettävät apteekkien järjestelmien toiminnot
VV	Kanta-viestinvälitys ja muut Kanta-palvelut	Kanta-palveluihin liittyvien viestinvälitykseen ja asiakirjojen metatietoihin liittyvät toiminnot, mukaan lukien Kanta-liittymispalvelun toiminnallisuudet
ARK	Kanta asiakastietovarantoon liittyvän järjestelmän perustoiminnot	Kanta asiakastietovarantoon (erityisesti potilastiedon arkisto PTA tai sosiaalihuollon asiakastiedon arkisto SHA) liittyvien järjestelmien toiminnot, sisällöissä mm. asiakirjojen lähettäminen ja hakeminen, palvelutapahtumien hallinta, jne. Asiakastietovarannon palveluihin liittymisessä käsiteltäviä tietosisältöjä esitetään erikseen sivulla "Tietosisällöt"
LP	Kanta-lisäpalveluihin liittyvät toiminnot	Kanta-palvelujen kysely- ja välityspalveluun, vanhojen tietojen arkistointiin, ostopalvelujen hallintaan sekä muihin lisäarvopalveluihin liittyvät toiminnot
KH	Käyttäjä- ja käyttöoikeushallinta	Käyttäjien ja heidän käyttöoikeuksiensa hallintaan liittyvät järjestelmien toiminnot ja ominaisuudet
KV	Käyttövaltuuksien tarkastaminen ja allekirjoitus	Käyttövaltuuksien tarkastamiseen, pääsynhallintaan ja sähköisiin allekirjoituksiin liittyvät toiminnot ja ominaisuudet
SH	Luovutusten, tahdonilmaisujen ja informointien hallinta	Asiakas- ja potilastietojen luovuttamiseen eri rekisterien ja rekisterinpitäjien välillä liittyvien luovutuslupien, kieltojen, luovutuslupien ja niihin liittyvien informointien hallintaan liittyvät toiminnot
KS	Käytön ja luovutusten seuranta	Tietojen ja järjestelmien käytön sekä tietojen luovutusten seurantaan ja lokimerkintöihin sekä lokipalveluihin liittyvät toiminnot ja ominaisuudet.
SOS	Sosiaalihuollon asian- ja asiakkuudenhallinta	Sosiaalihuollon asiakastietojärjestelmien asian ja asiakkuuden hallintaan liittyvät toiminnot sekä tiedonsaantioikeuteen liittyvät toiminnot.
KUV	Kuvantamisen toiminnot	Terveydenhuollon kuvantamisratkaisujen tiedonjakoon ja arkistointiin liittyvät toiminnot
LPYY	Lähetteet ja pyynnöt	Lähetteiden, hoitopalautteiden, pyyntöjen, vastausten ja konsultaatioiden tiedonvälitykseen liittyvät toiminnot ja niihin liittyvät rajapinnat
HTH	Henkilötietojen hallinta	Asiakkaiden ja potilaiden keskeisten tunniste-, yhteys- ja perustietojen hallinnan toiminnot
ERIL	Erillisjärjestelmien Kanta-toiminnot	Toiminnot, joiden avulla muiden järjestelmien kautta liittyvät (esimerkiksi kuvantamisen tai laboratorion) erillisjärjestelmät kykenevät hyödyntämään ja tuottamaan Kanta-palveluissa tarvittavia tietoja sekä varmistamaan hoitosuhteen, tai jotka liittyvät erityisalakohtaisten palvelujen tuottamiseen
AV	Ajanvaraus	Ajanvarauksiin liittyvät toiminnot
PTUK	Päätöksentuki	Asiakas- tai potilastietojen pohjalta tehtävät ehdotukset, ammattilaiselle asiakastietojen pohjalta näytettävät muistutteet ja muut järjestelmien päätöksenteon tuki -ominaisuudet

Olennaisten vaatimusten ryhmittely / Tietosisällöt

Määräys 5/2024 liite 2 Olennaisten vaatimusten luettelo

TIETOSISÄLTÖJEN ryhmittely	
TPOT	Potilashoidon yhteiset ja potilaskertomuksen tiedot
TSL	Luovutukset, suostumukset, palvelutapahtumien ja asioiden hallinta
TLOK (uusi)	Lokimerkintöjen tietosisällöt
TMET	Asiakirjojen ja kuvailutietojen hallinta
TERI	Erikoisalat ja palvelukohtaiset määrittelyt
TSOS	Sosiaalihuollon asiakirjat
TSOP	Sosiaalihuollon palvelutehtävien asiakirjat
TKUV	Kuvantaminen
TBIO	Biosignaalit
TPTO	Palvelujen ja toiminnan ohjaus
THEN	Henkilöiden perustiedot
TOTV (uusi)	Hyvinvointitiedot / omatietovaranto

Olennaisten vaatimusten ryhmittely / Tietoturvavaatimukset

Määräys 5/2024 liite 2 Olennaisten vaatimusten luettelo

RYHMÄ		
ASALK	Sähköinen allekirjoitus	Sähköiset henkilö- ja järjestelmäallekirjoitukset
ATUN	Tunnistaminen, sulkulistat ja rajoitukset	Tunnistaminen ja varmenteet, mukaan lukien sulkulistat ja ammattioikeuden rajoitukset
AKVH	Käyttövaltuushallinta	Käyttövaltuuksien määrittely ja tarkistaminen
AVALO	Valvonta ja lokitus	Lokivalvonta ja verkonvalvonta
ATIKO	Tietojen säilytys ja käsittelyn ohjeistus	Käyttöohjeet ja tietojen säilyttäminen
APAKOL	Tietoturva- ja tietosuojatoiminnot ja -tarkistukset	Istunnonhallinta, asiayhteys, luovutusten, suostumusten ja kieltojen hallinta, rekisterien hallinta, tietoryhmä- ja palvelukohtaiset tarkennukset ja muut vaatimukset
ASTUR	Sovellusturvallisuus	Turvalliset kehittämiskäytännöt, hyökkäyksiin varautuminen ja seuranta
AKYM	Järjestelmän käyttöympäristö	Tietoliikenteen ja tallennuksen salaus, verkko- ja hallintayhteydet, palvelin- ja etäpalveluympäristöt, järjestelmäkuvaukset ja sopimusriskit, poikkeustilanteisiin varautuminen

Olennaisten vaatimusten ryhmittely / Digipalvelujen vaatimukset

Määräys 5/2024 liite 2 Olennaisten vaatimusten luettelo

Vaatimusryhmä		
PV	Hyvinvointisovellusten perusvaatimukset	Omatietovarantoon ja Kanta-palveluihin liittyvien hyvinvointisovellusten perusvaatimukset
YT	Hyvinvointitietojen tuottaminen ja käyttö	Omatietovarannotoon liittyvien hyvinvointitietojen tuottamisen ja käytön perusvaatimukset, jotka mukana omatietovarantoon liittyvien hyvinvointisovellusten ja järjestelmien yhteistestauksessa
UUSI: ASP	Asiointi- ja omahoitopalvelujen toiminnallisuudet	Digitaalisten asiointi- ja omahoitopalvelujen keskeisiä toiminnallisuuksia ja vähimmäisvaatimuksia.
SV	Digipalvelujen saavutettavuusvaatimukset	Saavutettavuusvaatimukset, jotka perustuvat digipalvelulakiin sekä yleisiin saavutettavuusvaatimuksiin, ja joita edellytetään hyvinvointisovelluksilta.
KK	Digipalvelujen kuvaukset kansalaiselle	Hyvinvointisovellusten ja muiden digipalvelujen vaatimukset liittyen kansalaisen informointiin ja kansalaiskäyttäjille annettaviin kuvauksiin.
SO	Digipalvelujen säädökset ja ohjaus	Hyvinvointisovellusten ja muiden digipalvelujen vaatimukset liittyen henkilötietojen, lääkinnällisten laitteiden ja muun huomioitavan sääntelyn mukaisuuteen.
TS	Digipalvelujen tietosuojavaatimukset	Henkilötietojen suojaamiseen liittyvät vaatimukset, joita täytettävä hyvinvointisovelluksissa joko hyvinvointisovelluksen valmistajan tai sen asiakkaana toimivan organisaation kautta, ja joiden täyttäminen on suunniteltava myös muissa digipalveluissa.
TV	Digipalvelujen tietoturvavaatimukset	Hyvinvointisovellusten ja muiden digipalvelujen tietoturvallisuuteen liittyvät vaatimukset.

thl

Digipalvelujen vaatimukset -välilehti olennaisten vaatimusten luettelossa sisältää toiminnallisia ja tietoturvallisuusvaatimuksia tietojärjestelmille tai hyvinvointisovelluksille, joissa on **kansalaiskäyttäjien käytettäväksi tarkoitettuja ominaisuuksia**

Olennaisten vaatimusten profiilit

Määräys 5/2024 liitteet 3a-3h

- Kokoavat kansalliset vähimmäisvaatimukset *eri käyttötarkoituksiin* tarkoitetuille järjestelmille
  - Yksi olennaisten vaatimusten profiili kokoaa ne vaatimukset, jotka profiilin mukaisessa käyttötarkoituksessa käytettävässä järjestelmässä on ainakin oltava
- Yhdessä järjestelmässä voi olla useita profiileja
  - Millään järjestelmällä ei ole KAIKKIEN profiilien tai vaatimusten mukainen käyttötarkoitus (esim. apteekit vs. lääkkeiden määrääjät…)
- Kukin profiili sisältää osajoukon olennaisista vaatimuksista
  - Esimerkki: optisen toimialan järjestelmä

Profiilin tunniste	Profiilin nimi	Käyttötarkoitus	Profiilin voimaantulopäivä sertifioinnissa ja ilmoituksissa
	Potilastiedon arkiston profiilit		
3c3	Optisen toimialan järjestelmä	Optisen toimialan palvelujen tuottamisessa käytettävä tietoja Kanta-arkistoon arkistoiva ja sieltä hyödyntävä järjestelmä.	viimeistään 1.6.2024, aiempi ollut voimassa 2021 lähtien

Olennaisten vaatimusten profiilit

Määräys 5/2024 liitteet 3a–3h

- Esimerkki: optisen toimialan järjestelmä

Profiilin tunniste	Profiilin nimi	Käyttötarkoitus	Profiilin voimaantulopäivä sertifioinnissa ja ilmoituksissa
	Potilastiedon arkiston profiilit		
3c3	Optisen toimialan järjestelmä	Optisen toimialan palvelujen tuottamisessa käytettävä tietoja Kanta-arkistoon arkistoiva ja sieltä hyödyntävä järjestelmä.	viimeistään 1.6.2024, aiempi ollut voimassa 2021 lähtien

Kuvaus	Lisätietoja
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.	Järjestelmä voi myös olla toteutettu siten, että se kuuluu luokkaan A1 tai B, riippuen käsitteleekö se Kanta-arkiston tietoja suoraan tai toisen osajärjestelmän kautta. Mikäli järjestelmää käyttävällä palvelunantajalla on myös lääkäritoimintaa, tulee lääkemääräykseen toiminnot toteuttaa Lääkemääryksiä käsittelevän potilastietojärjestelmä -profiilin mukaisesti samassa tai toisessa tietojärjestelmässä.

Olennaisten vaatimusten profiilit

Määräys 5/2024 liitteet 3a-3h

Useisiin keskeisiin järjestelmien käyttötarkoituksiin pakollisten vaatimusten koonti tarkemmista määrittelyistä ja eri säädöksistä

- 3a Sähköinen resepti (2 profiilia)
- 3b Kanta-asiakastietovarantoon liittyvät järjestelmät (4 profiilia)
- 3c Potilastiedon arkisto (3 profiilia)
- 3d Sosiaalihuollon asiakastiedon arkisto (4 profiilia)
- 3e Kuvantaminen (5 profiilia)
- 3f Todistukset (3 profiilia, julkaistaan myöhemmin vuonna 2024)
- 3g Asiakas- tai potilastietojen käsittelyyn tarkoitetun järjestelmän vähimmäisvaatimukset (1 profiili)
- 3h Kansalaissovellukset ja hyvinvointitiedot (5 profiilia, joista 2 julkaistaan myöhemmin vuonna 2024).

thl

Olennaisten vaatimusten profiilit – THL:n määräys 5/2024 liitteet 3a-3b

- 3a Sähköinen resepti
  - 3a1 Lääkemääräyksiä käsittelevä potilastietojärjestelmä
  - 3a2 Apteekkijärjestelmä
- 3b Kanta-asiakastietovarantoon liittyvät järjestelmät
  - 3b1 Kanta asiakastietovarannosta tietoja hakeva järjestelmä tai palvelu
  - 3b2 Kanta asiakastietovarannosta haettuja tietoja hyödyntävä järjestelmä
  - 3b3 Kanta asiakastietovarantoon tietoja toimittava järjestelmä tai palvelu
  - 3b4 Kanta asiakastietovarantoon toimitettavia tietoja tuottava järjestelmä

Olennaisten vaatimusten profiilit – THL:n määräys 5/2024 liitteet 3c-3d

- 3c Potilastiedon arkisto
  - 3c1 Potilaskertomusjärjestelmä (perusvaatimukset)
  - 3c2 Suun terveydenhuollon järjestelmä
  - 3c3 Optisen toimialan järjestelmä
- 3d Sosiaalihuollon asiakastiedon arkisto
  - 3d1 Sosiaalihuollon rakenteisia asiakastietoja käsittelevä järjestelmä (liittymisvelvoitteen vaatimukset)
  - 3d2 Sosiaalihuollon asiakastiedon arkistoon toimitettavia rakenteisia tietoja tuottava ja käsittelevä sovellus
  - 3d3 Sosiaalihuollon asiakastiedon arkistoon tietoja toimittava sovellus tai palvelu
  - 3d4 Sosiaalihuollon asiakastiedon arkistosta tietoja hakeva sovellus tai palvelu

Olennaisten vaatimusten profiilit – THL:n määräys 5/2024 liite 3e

- 3e Kuvantaminen
  - 3e1 Kuvantamiseen liittyvä potilashallinnon perusjärjestelmä (HIS)
  - 3e2 Kuvantamisen toiminnanohjausjärjestelmä (RIS), Kantaan liittynyt
  - 3e3 Kuvantamisen toiminnanohjausjärjestelmä (RIS), ei Kantaan liittynyt
  - 3e4 Kuvien tallennus- ja jakamisjärjestelmä (PACS)
  - 3e5 Kuvantamisen katselinohjelmisto.

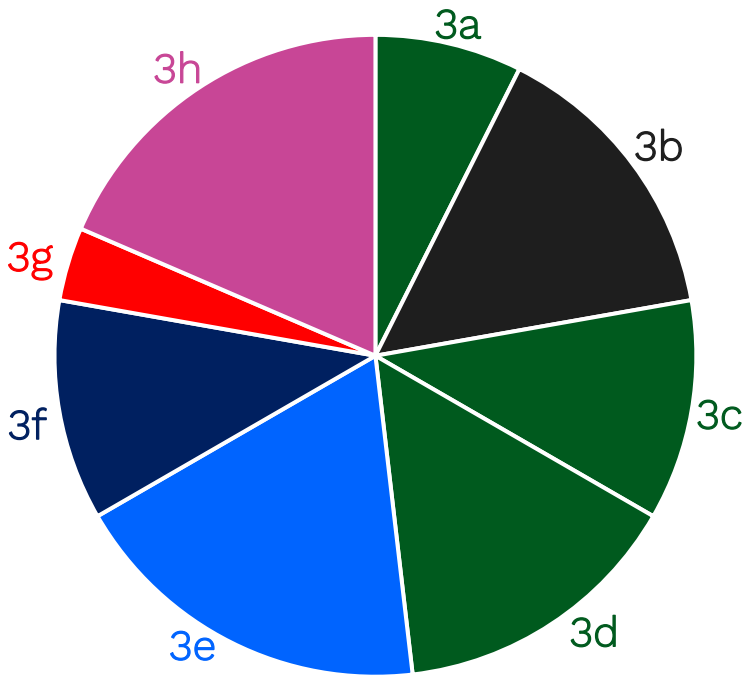
Olennaisten vaatimusten profiilit – THL:n määräys 5/2024 liite 3f+3g

- 3f Todistukset (julkaistaan myöhemmin vuonna 2024)
  - 3f1 Kanta-arkistosta todistuksia tai lausuntoja kyselevä palvelu
  - 3f2 Kanta-arkistosta todistuksia tai lausuntoja vastaanottava palvelu
  - 3f3 Kanta-arkistoon todistuksia tai lausuntoja tuottava palvelu
- 3g Asiakas- tai potilastietojen käsittelyyn tarkoitetun järjestelmän vähimmäisvaatimukset
  - 3g1 Vain yksi profiili, joka sisältää luokkiin B ja A1 kuuluvien järjestelmien vähimmäisvaatimukset
    - Profiilin 3g1 sisältämät perusvaatimukset sisältyvät useimpiin muihin profiileihin

Olennaisten vaatimusten profiilit – THL:n määräys 5/2024 liitteet 3h

- 3h Kansalaissovellukset ja hyvinvointitiedot
  - 3h1 Palvelunantajan digitaalinen asiointipalvelu
  - 3h2 Omatietovarantoon tietoja tuottava hyvinvointisovellus
  - 3h3 Omatietovarannosta hyvinvointitietoja käyttävä hyvinvointisovellus
  - 3h4 Asiakastietoja käyttävä hyvinvointisovellus (julkaistaan myöhemmin vuonna 2024)
  - 3h5 Omatietovarannosta hyvinvointitietoja käyttävä ammattilaisen tietojärjestelmä (julkaistaan myöhemmin vuonna 2024)

Olennaisten vaatimusten profiilit



- 3a Sähköinen resepti (2)
- 3b Kanta-asiakastietovarantoon liittyvät järjestelmät (4)
- 3c Potilastiedon arkisto (3)
- 3d Sosiaalihuollon asiakastiedon arkisto (4)
- 3e Kuvantaminen (5)
- 3f Todistukset (3)
- 3g Asiakas- tai potilastietojen käsittelyyn tarkoitetun järjestelmän vähimmäisvaatimukset (1)
- 3h Kansalaissovellukset ja hyvinvointitiedot (5)

Tietojärjestelmäpalvelun tuottajan on kuvattava, minkä profiilien mukaiset vaatimukset järjestelmä täyttää

Palvelunantaja voi tarkistaa eri tietojärjestelmissä toteutetut profiilit mm. Valviran tietojärjestelmärekisteristä

Yhdellä järjestelmällä voi olla useiden profiilien mukaisia käyttötarkoituksia

Mitä profiileja järjestelmässä on?

Yhdellä järjestelmällä voi olla useiden profiilien mukainen käyttötarkoitus:

Esimerkiksi yksittäinen laaja, luokkaan A3 kuuluva sosiaali- ja terveydenhuollon asiakas- ja potilastietojärjestelmä voi (osajärjestelmineen) olla:

- (3g1 Asiakas- tai potilastietojen käsittelyyn tarkoitettu järjestelmä)
- 3a1 Lääkemääräyksiä käsittelevä potilastietojärjestelmä (PTJ)
- 3c1 Potilaskertomusjärjestelmän perusvaatimukset täyttävä
- 3d1 Sosiaalihuollon rakenteisia asiakastietoja käsittelevä järjestelmä (liittymisvelvoitteen vaatimukset)
- 3e1 Kuvantamiseen liittyvä potilashallinnon perusjärjestelmä (HIS)
- 3f3 Kanta-arkistoon todistuksia tai lausuntoja tuottava palvelu
- 3h1 Palvelunantajan digitaalinen asiointipalvelu

Järjestelmälomake

Määräys 5/2024 Liite 4 Järjestelmälomake

- Lomakepohja, **tietojärjestelmäpalvelun tuottaja** tai **hyvinvointisovelluksen valmistaja** täyttää
- Muodostaa **asiakastietolain edellyttämän selvityksen olennaisten vaatimusten täyttämisestä**
- Käytännön työkalu **sertifiointiin ja rekisteröintiin**
- Järjestelmän / hyvinvointisovelluksen **perustietojen** kuvaus
- **Käyttötarkoituksen** tiivis kuvaus
- Tieto siitä, minkä kansallisten **profiilien** mukainen käyttötarkoitus järjestelmällä / sovelluksella on
  - Niiden kansallisesti julkaistujen profiilien luettelo, joiden mukaiset vähimmäisvaatimukset täytetään
- Käyttötarkoituksen tarkempi kuvaus suhteessa olennaisiin vaatimuksiin
  - **Toiminnot** jotka ovat osa käyttötarkoitusta
  - **Tietosisällöt** jotka ovat osa käyttötarkoitusta
  - **Tietoturvavaatimukset**, jotka täytetään järjestelmässä tai hyvinvointisovelluksessa
- 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 (lähteet saa näkyviin myös lomakkeessa)**
- **PÄIVITETTY** versio määräyksen 5/2024 liitteessä 4

”Rasti ruutuun”

Määräys 5/2024 Liite 4 Järjestelmälomake

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

Ryhmä Toiminnot	Id	Otsikko	Selite	Toteutetaan järjestelmässä / sovelluksessa	Lisätietoja
				ei merkintää / tyhjä = vaatimusta ei toteuteta tai täytetä **X** = vaatimus toteutetaan tai täytetään **M** = toteutus muuttunut verrattua aiempaan järjetelmälomakkeeseen/versioon, lisätiedot kuvattava **U** = ulkoinen, toteutetaan toisen järjestelmän tai rajapinnan kautta, lisätiedot kuvattava **es** = ei sovellettavissa, vaatimuksessa kuvattu soveltamisehto ei täyty, lisätiedot kuvattava	[täytä tarvittaessa, esim. mikäli toteutetaan erikseen sertifioidulla toisella järjestelmällä / sovelluksella tai tietyn rajapinnan kautta, kyseisen järjestelmän / sovelluksen tai rajapinnan nimi]
KH		**Käyttäjä- ja käyttöoikeushallinta**			
	KH01	Ammattilaiskäyttäjien hallinta	Ammattilaiskäyttäjien määrittely organisaation järjestelmään tai käyttäjähakemistoon		

Järjestelmälomakkeeseen liittyviä kokemuksia ja palautteita

- ”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**.”
- ”Järjestelmälomakkeessa voisi olla selkeämmin dokumentoitu, mitkä vaatimukset ovat tietyn tyyppiselle / tietyn luokan järjestelmälle valideja.” ← profiilit, tukimateriaalissa oleva koontitaulukko
- ”**Lähdelinkit** ovat hyödyllisiä.” ← lisätty lomakkeeseen, myös sertifiointi- ja tarkennustiedot kustakin vaatimuksesta
  - löytyvät otsikkorivin +-merkin takaa
- ”Lomake vaikuttaa hyvinkin hyödylliseltä. Ruksittujen ominaisuuksien **kuvailu esimerkiksi vapaamuotoisena tekstinä olisi varsin hankalaa**. Lisätietokenttä toimintorivin ohessa on hyvä olla olemassa.” ← mukana lomakkeessa
- ”THL voisi ohjeistaa, **kuinka vanha lomake** hyväksytään yhteistestaukseen/tietoturvallisuuden arviointiin.” ← määräystekstissä ohjeistettu: lomakkeen tietojen on vastattava järjestelmäversiota, joka on menossa yhteistestattavaksi, tietoturvallisuuden arviointiin tai Valviran rekisteröintiin / rekisteritietojen päivitykseen

Oikeellisuus tärkeää - täytä huolellisesti ja ajantasaisesti!

Sertifiointiprosessi

Luokka A

Sertifioinnin kokonaisuus

- Asiakastietolain mukainen sertifiointi koskee luokan luokan A (A1, A2, A3) tietojärjestelmiä ja asiakastietolain tarkoittamia (Kanta-palveluihin liittyviä) hyvinvointisovelluksia
  - Sertifioinnista vastaa tietojärjestelmäpalvelun tuottaja / hyvinvointisovellusten valmistaja, ei käyttäjäorganisaatiot
- Olennaisten vaatimusten täyttämisen ja sertifioinnin muodostettava **eheä kokonaisuus** sote-palvelun antajien toiminnan ja näiden tietoturvasuunnitelmien kanssa
- Sertifiointiin hakeutuva tietojärjestelmäpalvelun tuottaja / hyvinvointisovelluksen valmistaja 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 ja olennaisten vaatimusten viranomaistoimijat

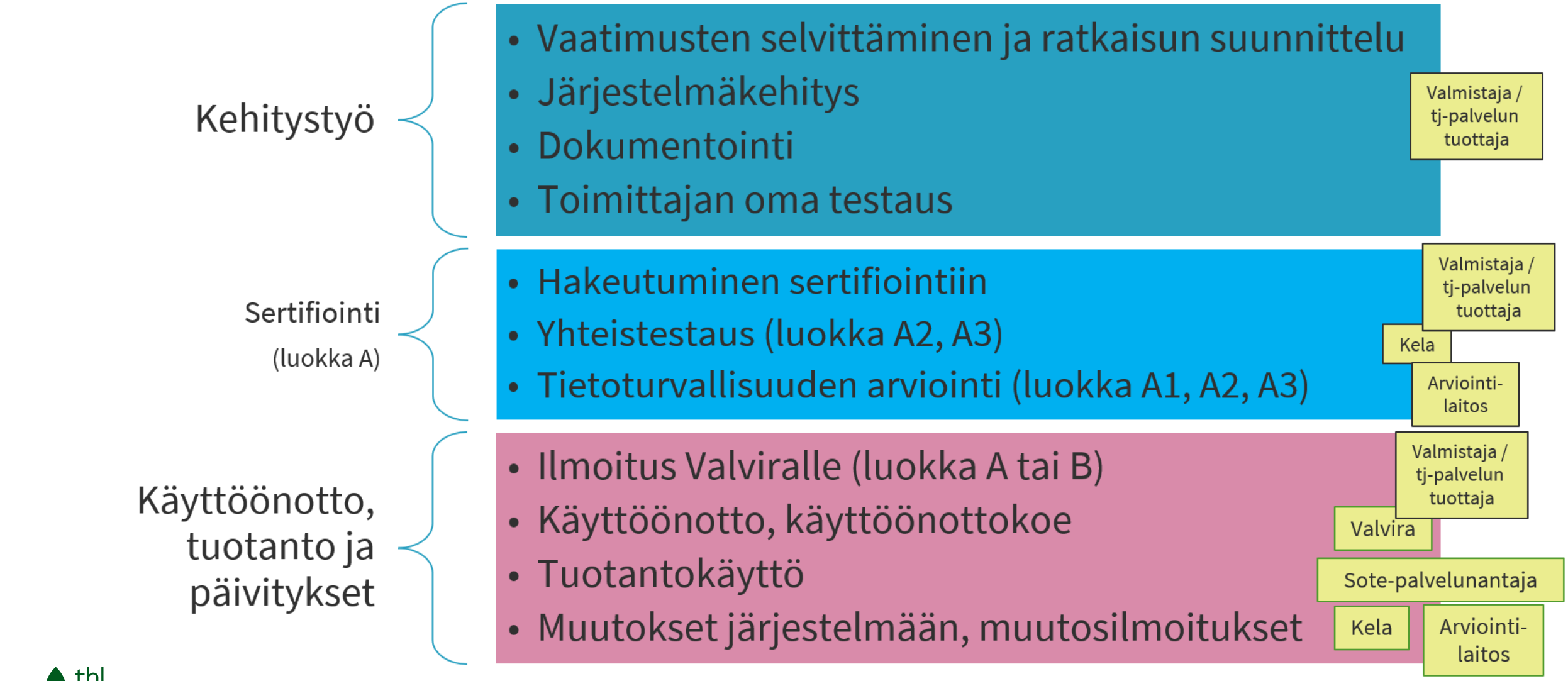
Sertifiointi- ja rekisteröintiprosesseissa ovat mukana:

- **Kela / Kanta-palvelut**: Kelan palvelu, jonka vastuulla on Kanta-palveluiden toteuttaminen, ylläpito ja kehittäminen
  - **Kanta-yhteistestaus**: suunnittelee ja koordinoi **yhteistestauksen** (luokka A2 tai A3)
- **Tietoturvallisuuden arviointilaitos**: Traficomin hyväksymä taho, joka suorittaa sertifiointiprosessin osana olevan tietoturvallisuuden arvioinnin, tuottaa tietoturvallisuustodistuksen ja ottaa vastaan ilmoituksia järjestelmiin tai sovelluksiin tehtävistä muutoksista (luokka A1, A2 tai A3)
- **Valvira**: valvontaviranomainen, joka ylläpitää **rekisteriä** tietojärjestelmistä ja valvoo ja edistää tietojärjestelmien ja hyvinvointisovellusten vaatimustenmukaisuutta (luokka B, A1, A2 tai A3)

Ohjauksessa lisäksi:

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

Sertifiointi suhteessa kehitystyöhön ja käyttöönottoihin



Määräys 5/2024 Liite 1

Sertifiointiprosessin päätoimenpiteet valmistajan / tietojärjestelmäpalvelun tuottajan näkökulmasta

1. Tuote- ja järjestelmäkehitys
   - Käyttötarkoituksen määrittely
   - Säädösten ja olennaisten vaatimusten huomiointi, mm.
     - minkä profiilien mukaiset käyttötarkoitukset on → profiileista tulevat vaatimukset
     - 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 tietoturvallisuuden arviointilaitokseen ja tarvittaessa Kelaan
   - Liittyminen ja ilmoittautuminen Kelan asiakastestipalveluun ja yhteistestaukseen
   - ilmoittautuminen ja tietoturvallisuuden arviointiin
   - olennaisten vaatimusten järjestelmälomake
3. Yhteistestausprosessi
   - Ks. Kelan materiaali
4. Tietoturvallisuuden arviointi
   - Arviointivalmiudet, dokumentaatio, arviointitilaisuus / tilaisuudet
5. Tietoturvallisuustodistus
   - HUOM. todistus voidaan myöntää ensimmäisessä A2/A3 sertifioinnissa 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 (→ Kohta 1...)

Sertifiointiprosessi uusien säädösten mukaisesti

- Perusprosessi samanlainen kuin aiemmissakin säädöksissä
- Luokkien B, A1, A2 ja A3 velvoitteet vastaavia kuin aiemmissakin säädöksissä
- Järjestelmän käyttötarkoituksen ja riskitason huomiointi todentamisessa terävöitynyt edelleen vuodesta 2021
- Ennen vuotta 2021 käytetty termi ”vaatimustenmukaisuustodistus” muuttui jo vuonna 2021 muotoon ”tietoturvallisuustodistus”, jolloin myös tietoturvallisuustodistuksen voimassaoloaika muuttui viidestä kolmeen vuoteen
- Viimeisetkin ennen vuoden 2021 määräyksiä saadut todistukset uusittava uudempien määräysten mukaisiksi tietoturvallisuustodistuksiksi ennen 1.11.2024 (vuoden 2021 määräysten mukainen määräaika)
- Vaatimustenmukaisuuden uudistamiseen tullut täsmennyksiä – yhden järjestelmän yhteistestausten ja tietoturvallisuustodistuksen
- Vuoden 2021 määräyksissä mukana ollut ”rajoitettu käyttötarkoitus” ei enää mukana vuoden 2024 määräyksissä (yksinkertaistaminen, Valviran rekisteröinti eri asia kuin valvontaprosessi)
- Luokasta B luokkaan A (erityisesti A1) siirtymisen kriteerit ja määräajat ennallaan verrattuna määräykseen 4/2021
- Tietoturvavaatimusten todentamisiin tarkennuksia ja täsmennyksiä

Tietoturvallisuuden arviointilaitokset

- Traficom hyväksyy tietoturvallisuuden arviointilaitokset ja valvoo niitä
  - Arviointilaitosten hyväksyntä perustuu lakiin tietoturvallisuuden arviointilaitoksista 1405/2011
- Traficom ohje arviointilaitoksille
  - "Luokkaan A kuuluvan tietojärjestelmän tai hyvinvointisovelluksen tietoturvallisuuden arvioinnin voi suorittaa vain arviointilaitos, jonka pätevyysalueena on VAHTI tai Katakri."
- Asiakastietolain mukaisiin tietoturvallisuuden arviointeihin hyväksyttyjä arviointilaitoksia tällä hetkellä kaksi: KPMG IT Sertifiointi Oy ja Nixu Certification Oy

Tietoturvallisuuden arvioinnin menettelyt osana sertifiointia

- Arvioinnin kriteeristönä ovat määräyksen 5/2024 mukaiset tietoturvallisuusvaatimukset
  - Tietoturvavaatimusten *lähteet* täsmentävät vaatimuksia, suorat tarkat lähdeviitteet suoraan sovellettavia
- Pohjatyö, relevanttien vaatimusten tunnistaminen, toteutus ja huomiointi järjestelmän kannalta, dokumentointi
- Yhteydenotto arviointilaitokseen / sertifiointihakemus, sitoumus
- Sopimus arviointilaitoksen kanssa
  - Tietoturvallisuuden arviointi ja mahdolliset seuranta-auditoinnit ovat maksullisia
  - Huom. määräykset mahdollistavat esim. arvioinnin laajuuden, järjestelmän luokan ja riskitason huomioinnin arviointien hinnoittelussa
- 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
- Laki ja määräykset eivät edellytä seuranta-auditointeja, mutta **muutosilmoitukset** ja **todistuksen uusiminen** ennen aiemman vanhenemista tärkeää huolehtia

Tietoturvavaatimusten todentaminen

Määräys 4/2024 Luku 7.3, Määräys 5/2024 luku 10.2

- Todentamisessa käytetään Traficomin ohjeiden mukaisia hallinnollisia ja soveltuvin osin myös teknisiä todentamistapoja
- Todentaminen tehdään Määräyksen 5/2024 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: tarkistus järjestelmää tai sovellusta käyttämällä (toiminnallisella testauksella) ominaisuuden olemassaolosta ja asianmukaisuudesta osana tietoturvallisuuden arviointia
  - HT: tekninen tietoturva- ja haavoittuvuustestaus ja turvallisuustason arviointi osana tietoturvallisuuden arviointia
- D: dokumentaation läpikäynti
- (täydentävä): H: haastattelu osana tietoturvallisuuden arviointia, jolla voidaan syventää ja täydentää arviointia
  - ei yksin riittävä vaatimuksen todentamistavaksi

Muutokset aiempiin säädöksiin ja määräysten lausuntokierroksen tulokset

Olennaisten vaatimusten (5/2024) ja sertifioinnin (4/2024) keskeisimmät selkeytykset ja päivitykset

- Aiempien säädösten pohjalta sertifioitu luokassa A jo aiemmin n. 60 ja rekisteröity luokkaan B yli 300 tietojärjestelmää
- Perusasioita ja –jäsennyksiä ei ole muutettu, pääosa tietojärjestelmien vaatimuksista samoja kuin aiemmin!
- Määräykset 4/2024 ja 5/2024 selkeyttävät ja yhtenäistävät olennaisten vaatimusten rakennetta ja hyödynnettävyyttä **päivittynyt asiakastietolaki** ja **kansalliset kehittämispolut** huomioon ottaen, mm.
  - Uudet ja päivittyvät **määritykset:** mm. sosiaalihuollon asiakastietojen vaiheistus , kansallinen lääkityslista, koodistojen hyödyntämisen perusvaatimukset, uudistetut luovutuslupa-, informointi-, puolesta asiointi- ym. määritykset, ohjelmistot ja laitteet merkinnän tekijänä, lokitietojen tuottaminen → **yhteentoimivuus ja tiedon laatu**
  - Asiakastietolain ja määritysten **voimaantuloajat** ja **vaatimustenmukaisuuden uudistamisen aikataulut** (3 vuoden välein koonti) pohjana myös vaatimusten **voimaantulolle ja vaatimustenmukaisuuden ylläpidolle** järjestelmissä / profiileissa
- Linkitys **Valviran tietojärjestelmärekisterin** uudistamiseen

Määräysten lausuntokierroksen tuloksia

- Lausuntoja tuli lausuntokierroksella 16 organisaatiolta, lisäksi kommentteja määräysaiheisiin kirjaamoon ja suorilla yhteydenotoilla
- Yli **300** yksityiskohtaista kommenttia, kaikki käsitelty, useimmat aiheuttivat täsmennyksiä tai muokkauksia lausuntoversioon
- Runsaasti yksittäisiin vaatimuksiin kohdistuneita erinomaisia täsmennys- ja selkeytysehdotuksia – **kiitokset kommentoijille**!
- Eniten sisällöllisiä kommentteja kohdistui seuraaviin aiheisiin
  - Yksityiskohtaisten tietoturvavaatimusten täsmennys- ja päivitystarpeet
  - Sertifiointiprosessin ja järjestelmälomakkeen täsmennykset
  - Digipalvelujen vaatimukset
  - Apteekkien tietojärjestelmät ja verkkopalvelut
- Useita kommentteja myös huomioitavaksi jatkotyöhön
  - esim. STM tuleva säädösten kehitys, viranomaisten yhteistoiminta, EU-valmistelut…

Merkittävimmät muutokset ja täydennykset 1/2

- Kelan **yhteistestauskokonaisuudet** on aiempaa selkeämmin linkitetty olennaisiin vaatimuksiin (määräys 5/2024 liitteet 2 ja 3)
- tietoturvallisuuden arvioinnin ja yhteistestausten tulosten suhdetta tietojärjestelmien rekisteröintiin on täsmennetty, erityisesti **vaatimustenmukaisuutta uudistettaessa** (määräys 4/2024 luku 10)
- **lokimerkintöjen ja käyttölokien** hallinnan yhtenäistämiseen liittyvien kansallisten vaatimusten toimeenpano aikatauluineen on sisällytetty olennaisiin vaatimuksiin - ei erillistä määräystä (määräys 5 liitteet 3)
- määräysten suhdetta **apteekkien tietojärjestelmiin ja verkkopalveluihin** on selkeytetty (soveltamisen rajaukset apteekkien järjestelmissä) (koonti: määräys 5/2024 liite 1 luku 6.6)

Merkittävimmät muutokset ja täydennykset 2/2

- **tietoturvavaatimusten** suorat ja toteutusta tukevat **lähteet** on sisällytetty olennaisten vaatimusten luetteloon (määräys 5/2024 liite 2)
- vaatimusten linkityksiä **kansainvälisiin standardeihin** lisätty ja selkeytetty, erityisesti tietoturva- ja digipalveluvaatimuksissa (määräys 5/2024 liite 2)
- kansalaiselle suunnattujen **digipalvelujen** (asiointipalvelut ja hyvinvointisovellukset) vaatimuksia on otettu aiempaa selkeämmin omaksi osiokseen olennaisten vaatimusten kokonaisuudessa
  - aiempi erillinen Omatietovarantoon liittyneiden hyvinvointisovellusten määräys poistunut, myös nämä vaatimukset on integroitu osaksi olennaisten vaatimusten ja sertifioinnin kokonaisuutta, lisäksi perusvaatimukset palvelunantajien asiointipalveluille
  - Digitaalisten palvelujen vaatimukset osin omina vaatimusryhminään, profiilit keskeisille digipalveluille (määräys 5/2024 liitteet 2 ja 3, määräys 5/2024 liite 1 luku 6.5)

Nostoja merkittävimmistä täydennyksistä aiempiin määräyksiin

Nosto / esimerkki: yhtenäisten käyttölokitietojen tuottamisen aikataulu – määräyksen 5/2024 profiileissa olevat ajankohdat

Ks. olennaiset vaatimukset AVALO02, TLOK01, TLOK02, KS01, KS02

- 1.1.2027 tuotannossa:
  - lääkemääräyksiä tuottavat tietojärjestelmät, ja apteekkijärjestelmät (profiilit 3a1-3a2),
  - potilaskertomusjärjestelmät, suun terveydenhuollon sekä optisen toimialan järjestelmät (profiilit 3c1-3c3),
  - sosiaalihuollon kansallisten vaatimusprofiilien mukaiset järjestelmät (profiilit 3d1-3d4)
  - kuvantamiseen liittyvät potilashallinnon perusjärjestelmät (profiili 3e4)
- 1.1.2029 tuotannossa:
  - kuvantamisen toiminnanohjausjärjestelmät ja soveltuvin osin kuvien tallennus- ja jakamisjärjestelmät (PACS) ja kuvantamisen katselinohjelmistot (profiilit 3e5-3e7)
  - palvelunantajien digitaaliset asiointipalvelut ja omatietovarannosta hyvinvointitietoja käyttävät ammattilaisten tietojärjestelmät (profiilit 3h1 ja 3h5)
  - muut kuin yllä mainitut Kanta-tietovarannoista tietoja hakevat tai niihin tietoja tuottavat järjestelmät (profiilit 3b1-3b4)
- 1.1.2030 tuotannossa
  - muut asiakas- ja potilastietojen käsittelyyn tarkoitetut tietojärjestelmät (profiili 3g1)

Nostoja: apteekkien järjestelmät ja verkkopalvelut

- Lausuntokierroksella useita aiheeseen kohdistuneita lausuntoja apteekkitoimijoilta ja apteekkien tietojärjestelmätoimittajilta
- Selkeytykset lopullisiin määräyksiin palautteiden pohjalta ja viranomaisyhteistyössä (mm. viranomaisyhteistyöryhmä THL, STM, Kela, FIMEA, Valvira, Traficom)
- Koonti määräyksen 5/2024 liite 1 luku ”6.6 Lääkemääräysten käsittely sekä apteekkien tietojärjestelmät ja verkkopalvelut”
  - Lääkkeen toimittamista varten laaditut asiakirjat uuden lain mukaisesti asiakasasiakirjoja, muutos ei kuitenkaan ole oleellisesti muuttanut lääkemääräysten käsittelyä tai laajuutta
  - Apteekkitietojärjestelmien vaatimukset vakiintuneet jo aiemmissa säädöksissä (luokka A3)
  - STM lakivalmistelun mukaiset rajaukset: vain lääkkeiden toimittamisessa käytetyt järjestelmät tietojärjestelmävaatimusten piirissä, verkkoapteekit edellyttävät laajempaa sääntelyä
  - Apteekkien muut henkilö- ja asiakasrekisterit eri asia kuin asiakastietolain asiakastiedot
  - Lääkemääräystietojen yhteisrekisterinpito → ei esim. luovutusilmoitus- ym. vaatimuksia

Nostoja: digipalvelut määräyksissä 1/2

- **Määritelmät** - Määräys 4/2024 luku 2
  - Monet (nykyiset) asiointipalvelut täyttävät laissa olevan **tietojärjestelmän** määritelmän, jos tuottavat tai käsittelevät asiakastietoja – **digitaalinen asiointipalvelu**
  - **Hyvinvointisovellukset** on laissa määritelty pelkästään Kanta-palveluihin liittyvinä: sekä hyvinvointitietoja käsitteleviä että Kanta-palveluista asiakastietoja asiakkaan käyttöön tuovia
  - **Digipalvelu** / digitaalinen palvelu – yhteinen termi yllä oleville – tietojärjestelmä tai hyvinvointisovellus, jossa on kansalaisen käytettäväksi tarkoitettuja ominaisuuksia
- **Luokittelu** (onko sertifioitava) - Määräys 4/2024
  - Laki edellyttää kaikkien Kanta-palveluihin liittyvien hyvinvointisovellusten sertifiointia (luokka A, oletusarvoisesti A2 jos ”stand-alone” hyvinvointisovellus)
  - Tietojärjestelmät (myös jos ne ovat tai jos niihin sisältyy asiointipalveluja)
    - Sertifioidaan (luokka A), jos ne liittyvät Kanta-palveluihin tai jos niihin muista syistä kohdistuu tarve suorittaa tietoturvallisuuden arviointi (tietoturvallisuus, riskitaso, tietojen laajamittainen käyttö)
    - Muussa tapauksessa ei sertifioida (luokka B)
  - Sekä tietojärjestelmät että hyvinvointisovellukset on rekisteröitävä Valviran ylläpitämään tietojärjestelmärekisteriin

Nostoja: digipalvelut määräyksissä 2/2

- **Vaatimukset** - Määräys 5/2024 liite 2 Olennaisten vaatimusten luettelo, välilehti ”Digit. palvelujen vaatimukset”
  - Joukko vaatimuksia, joita kohdistuu erityisesti hyvinvointisovelluksiin ja asiointipalveluihin
  - Jos asiointipalvelu on tietojärjestelmä tai osa sitä, vaatimuksia myös luettelon muissa osioissa
  - Kaikki vaatimukset viittaavat lähdedokumentteihin (esim. lait, kansalliset määritykset, standardit)
  - Pääosa vaatimuksista perustuu aiempiin määräyksiin ja tarkempiin määrityksiin
  - Osa vaatimuksista ja profiileista täsmentyy edelleen tulevien määrittelyjen myötä
- **Profiilit** - Määräys 5/2024 liite 3h – Kansalaisen digipalvelujen ja hyvinvointitietojen profiilit
  - 3h1 Palvelunantajan digitaalinen **asiointipalvelu**
  - 3h2 Omatietovarantoon tietoja tuottava **hyvinvointisovellus**
  - 3h3 Omatietovarannosta hyvinvointitietoja käyttävä **hyvinvointisovellus**
  - 3h4 Asiakastietoja käyttävä hyvinvointisovellus
  - 3h5 Omatietovarannosta hyvinvointitietoja käyttävä ammattilaisen tietojärjestelmä

Julkaistaan myöhemmin koska on tulossa määrityksiä jotka vaikuttavat profiilien vaatimuksiin

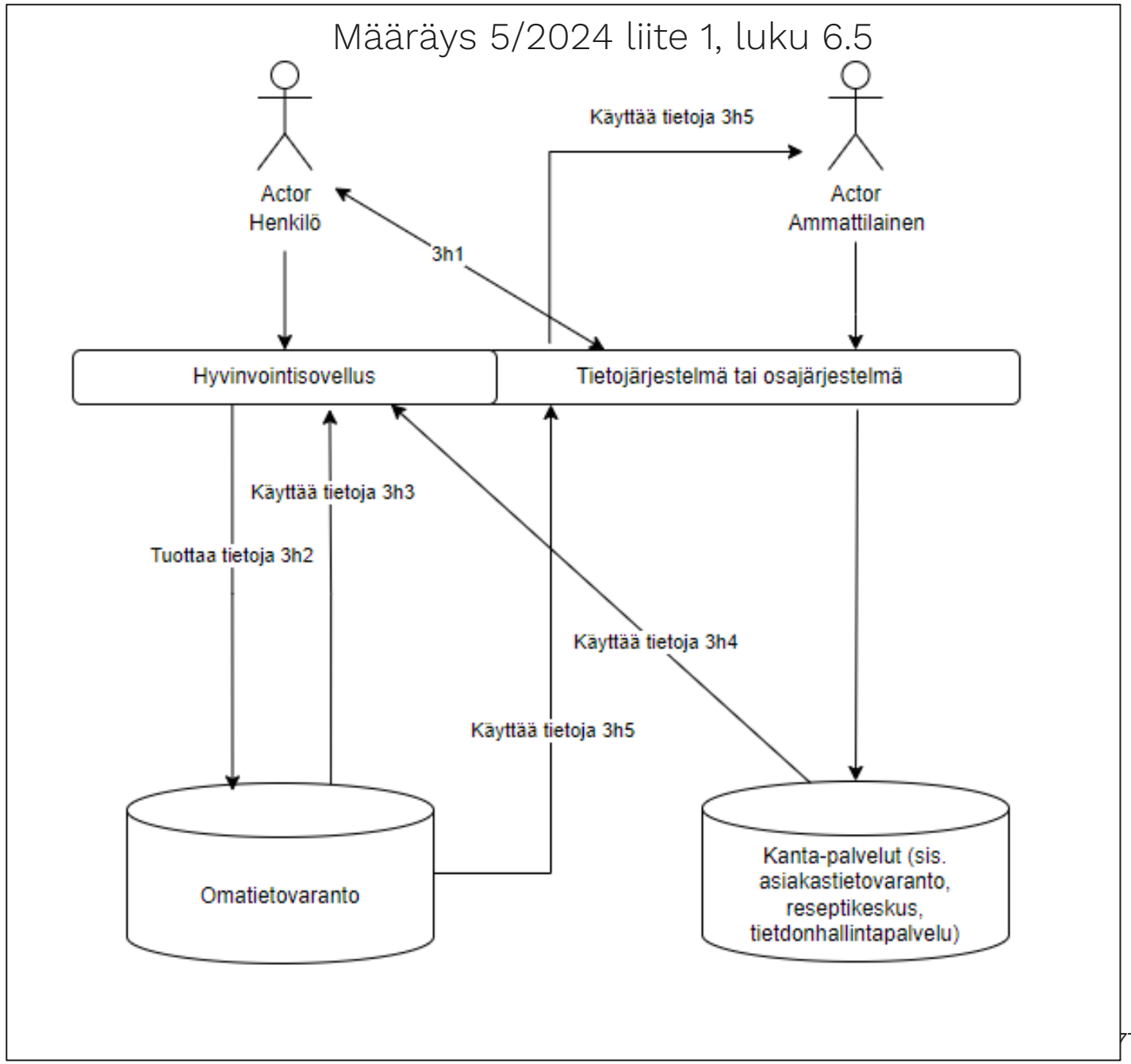
Digipalvelujen käyttäjät, profiilit ja tietovarannot

Määräys 5/2024, liite 3h
Kansalaisen digipalvelujen ja hyvinvointitietojen profiilit

3h1 Palvelunantajan digitaalinen asiointipalvelu
3h2 Omatietovarantoon tietoja tuottava hyvinvointisovellus
3h3 Omatietovarannosta hyvinvointitietoja käyttävä hyvinvointisovellus
3h4 Asiakastietoja käyttävä hyvinvointisovellus
3h5 Omatietovarannosta hyvinvointitietoja käyttävä ammattilaisen tietojärjestelmä

HUOM. yksi järjestelmä / sovellus voi toimia yhdessä tai useammassa roolissa (myös muut kuin nämä profiilit)

HUOM. yksi ratkaisu voi olla tietojärjestelmä, hyvinvointisovellus, tai molempia (asiakastietolain määritelmät)



Erityiskysymyksiä: poikkeamat, vaatimusten voimassaolo, EU-kehitysnäkymiä

Poikkeamat vaatimustenmukaisuudesta

Määräys 5/2024 luku 10.4

- Merkittäviä poikkeamia (AsTL 82 §, 41 §) ovat poikkeamat, jotka tuotantokäytössä aiheuttaisivat

1. Riskejä potilas- tai asiakasturvallisuudelle
2. Merkittäviä riskejä tietosuojalle, tietoturvallisuudelle tai sote-palvelujen toiminnalle
3. Merkittäviä tai pitkäaikaisia heijastusvaikutuksia tai lisäpoikkeamia useille palvelunantajille tai useille muille järjestelmille / sovelluksille
4. Laajamittaisia häiriöitä tietojen oikeellisuudelle, eheydelle tai yhteentoimivuudelle (erityisesti Kanta-palvelujen kautta)
5. Tietoturvallisuustodistuksen vanheneminen (tarkennuksin)
6. *Käyttötarkoitukseen kuuluvan (esim. profiiliin kuuluvan) pakollisen vaatimuksen toteuttamatta tai noudattamatta jättäminen*
7. *Hyväksytyn sertifioinnin puuttuminen sertifioitavaksi kuuluvasta vaatimuksesta / luokka A (tarkennuksin)*
8. Pakollisen vaatimuksen perustuminen vanhentuneeseen määrittelyversioon (tarkennuksin, mm. jos määrittelyversio ei enää voimassa tuotannossa tai tueta Kanta-palveluissa)
9. Säädöksissä asetettujen tai viranomaisten asettamien määräaikojen noudattamattomuuden järjestelmään edellytetyille korjauksille (tarkennuksin)

Poikkeamat vaatimustenmukaisuudesta

Määräys 5/2024 luku 10.4

- Merkittävistä poikkeamista ilmoitettava AsTL 82 § ja 90 § 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 muun muassa tehdä tarkastuksia (89 §), antaa määräyksen velvollisuuden täyttämiseksi tai puutteiden korjaamiseksi (93 ja 94 §), asettaa käyttökiellon (94 §) sekä tehostaa antamaansa määräystä uhkasakolla (96 §)
- Tietojärjestelmäpalvelun tuottaja tai palvelunantaja **eivät saa ottaa tuotantokäyttöön** järjestelmää, johon Valviran tietojärjestelmärekisteristä löytyvien tietojen perusteella kohdistuu merkittävä poikkeama, joka estää tuotantokäyttöönoton

thl

Vaatimusten ja profiilien voimassaolo

Määräys 5/2024 liite 1, luku 6.1, Määräys 5/2024 luku 12

- *Profiilin voimaantulopäivä sertifioinnissa ja ilmoituksissa:* profiilin mukaisia vaatimuksia sovelletaan yhteistestauksessa, tietoturvallisuuden arvioinnissa ja Valviran tietojärjestelmärekisteriin tehtävissä ilmoituksissa, 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 ja määräyksissä (esim. lokivaatimukset) tuotantokäytön voimaantuloaikoja mm. eri tietosisältöjen tai toimintojen vaiheistukseen
- Viitattujen määritysten (erityisesti Kanta-vaatimukset) voimassaolo huomioitava vaatimusten toteuttamisessa
  - THL tai Kela julkaisevat tiedot siitä, mitkä ovat voimassa olevia määrittelyjä ja määrittelyversioita, ja mitä määrittelyversioita edellytetään esim. yhteistestauksessa ja tuotantokäytössä
- Määräykset eivät vaikuta asiakastietolaissa asetettuihin velvoitteisiin tai määräaikoihin esim. Kanta-liittymisten suhteen, ks. asiakastietolaki 67 § ja 102 §

Tulossa: European Health Data Space

- EU-asetus, suoraan Suomessa sovellettavaa lainsäädäntöä
  - Merkittäviä tavoitteita kansalaisten oikeuksiin, terveystietojen liikkumiseen ja markkinoiden yhtenäistämiseen liittyen
- Kompromissiteksti EU:n kolmikannassa jo hyväksytty, lopulliset tekstit todennäköisesti syksyllä 2024
- Soveltaminen alkaa 2 vuotta julkaisusta, joitakin siirtymäaikoja
- Tämän päivän aiheeseen liittyviä sisältöjä (asetuksessa myös paljon muuta):
  - Sähköisten potilastietojärjestelmien ja niihin liittyvien hyvinvointisovellusten olennaiset vaatimukset
  - Sähköisten potilastietojärjestelmien harmonisoidut komponentit: yhteentoimivuus- ja lokikomponentti
  - EU-vaatimustenmukaisuus harmonisoiduille komponenteille
  - Potilastietojärjestelmien kanssa yhteentoimivien hyvinvointisovellusten vaatimustenmukaisuusmerkki
  - Itsesertifiointi, EU-testausympäristö, EU-vaatimustenmukaisuusvakuutus
  - Eurooppalainen terveystietojen vaihtoformaatti (EEHRxF)
  - Jäsenmaissa (edelleen) muihin kuin harmonisoituihin komponentteihin kohdistuvia vaatimuksia ja sertifiointikäytäntöjä
- Suomi aktiivisesti mukana toimeenpanosäädösten valmisteluhankkeessa (Xt-EHR) ja toisena vetäjänä ”Certification and labelling framework” työpaketissa

Yhteenveto

Yhteenveto

- Olennaisten vaatimusten ja sertifioinnin menettelyt ja pääosa olennaisista vaatimuksista **nojautuvat aiempiin säädöksiin, määräyksiin ja määrityksiin**
  - Järjestelmän **käyttötarkoituksen** mukaiset vaatimukset edelleen olennaisten vaatimusten lähtökohtana
  - Tietoturvallisuuden ja tietosuojan varmistaminen nykyinen riskiympäristö huomioiden
- Määräysten **lukumäärä vähentynyt** ja olennaisten vaatimusten **integraatio parantunut**
  - Hyvinvointisovellusten ja muiden digipalvelujen vaatimukset osaksi samaa kokonaisuutta tietojärjestelmävaatimusten kanssa, olennaisten vaatimusten selkeämpi linkitys yhteistestauskokonaisuuksiin, tietoturvavaatimusten lähteet, jne.
- Menettelyjen ja vaatimusten voimaantuloissa lähtökohtana **jatkuvuus**, esim.
  - 2023 tai alkuvuonna 2024 käynnistetyt sertifioinnit mahdollista suorittaa loppuun aiempien menettelyjen ja vaatimusten pohjalta
  - uusien vaatimusten voimaantuloajat kehittämis-, hankinta- ja sertifiointisyklit huomioiden
- Tärkeää tarkistaa ja varmistaa että kaikki järjestelmää koskevat olennaiset vaatimukset on täytetty (ja tarvittaessa sertifioitu) voimassa oleviin vaatimuksiin ja määrityksiin perustuen
  - Myös Kanta-palveluihin liittyvien vaatimusten yhteistestausten perustuminen voimassa oleviin määritysversioihin

Lopuksi

- Hyödynnä käytännön työkalut: mukana mm.
  - **olennaisten vaatimusten luettelo**
    - ajantasainen koonti kansallisista vaatimuksista
    - = toisiinsa liittyvien määritysdokumenttien hakemisto: mistä säädöksistä ja määrittelyistä löytyy aiheen XYZ vaatimukset…
  - **profiileissa** kooste eri käyttötarkoitusten vähimmäisvaatimuksista
  - **järjestelmälomake**, jossa toivottuja lisätietoja mukana
  - **muutosilmoitus**- ja **luokitteluohjeet**
  - tukimateriaalina **riskiarviotyökalu**
  - tukimateriaalina kaikki olennaiset vaatimukset ja profiilit sisältävä **koontitaulukko**
    - erityisesti laajempiin järjestelmiin, joissa monien profiilien mukaisia käyttötarkoituksia
- Pidä vaatimustenmukaisuus ajan tasalla!

Kiitokset!
Kysymyksiä?

sotetiedonhallinta@thl.fi

Terveyden ja
hyvinvoinnin laitos

Lisämateriaalia

Määräysten perusteena olevat THL vastuut säädöksissä

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 97§]

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 76§]

Määräykset **asiakasasiakirjojen tietorakenteista, tietosisällöistä, koodistoista** [AsTL 20§]

Koodistopalvelun ylläpito ja asiakasasiakirjojen tietorakenteiden ylläpito ja jakelu [AsTL 65§]

Määräykset **toiminnallisuutta, yhteentoimivuutta, tietoturvaa ja tietosuojaa koskevista tietojärjestelmien olennaisista vaatimuksista** [AsTL 84§]

Määräykset **tietojärjestelmien luokittelusta** ja **vaatimustenmukaisuuden menettelyistä** ja merkittävistä **poikkeamista** [AsTL 79§, 85§, 82§]

Määräykset **tietosuojan ja tietoturvallisuuden** ja järjestelmien käytön **tietoturvasuunnitelmasta** [AsTL 77§]

Määräysten voimaantulo ja siirtymä aiemmista säädöksistä

Määräys 4/2024 Luku 12

- Määräysten mukaiset menettelyt ovat astuneet voimaan määräysten tultua voimaan (10.5.2024)
- Aiempien säädösten mukaiset tietoturvallisuustodistukset säilyneet voimassa
  - Uusittava kuitenkin ennen aiemman vaatimustenmukaisuuden umpeutumista tai 1.11.2024 mennessä (jos vanhempi kuin 2021 säädösten mukainen todistus)
  - Aiemmin hyväksytyt järjestelmät toimivat tuotannossa ja voidaan ottaa käyttöön voimassaoloaikana
  - Uusiminen AJOISSA, vireille viimeistään 6kk ennen aiemman vaatimustemukaisuuden päättymistä
- Käynnissä olevat sertifiointiprosessit (ennen 10.5.2024 käynnistetty) voidaan suorittaa loppuun prosessin käynnistyessä voimassa olleiden vaatimusten mukaisesti vuoden 2024 loppuun mennessä
  - Asiasta erillinen merkintä myönnettävään todistukseen, uuden lain mukainen 3v voimassaoloaika
- Jos ei tarvita uutta sertifiointia mutta uusien määräysten johdosta on tarpeen päivittää tiedot Valviran tietojärjestelmärekisteriin, tiedot päivitettävä 1.11.2024 mennessä tai Valviran määräämällä tavalla
  - esim. luokan B järjestelmässä myös uuden määräyksen mukaisia vaatimuksia, profiilitietojen päivitykset joiden vaatimukset jo hyväksytysti todennettu, jne.

Kolmansien osapuolten palveluihin liittyvät tietosuoja-, tietoturva- ja varautumisvaatimukset

Määräys 5/2024 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
- Vaatimukset hyvin pitkälti vastaavia kuin vuoden 2021 määräyksissä
  - EU- ja ETA-tasoinen tietojen liikkuvuusperiaate lähtökohtana
  - 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. skenaario jossa tietoliikenneyhteydet rajoitettu Suomen sisäpuolelle) huomioitu 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 5/2024 Liite 1 luku 6.3

- Monet tietojärjestelmät entistä vähemmän irrallisia / ”itsenäisiä” monoliitteja
- Määräyksissä huomioitu **osajärjestelmien** rooli
  - Osana laajempaa kokonaisuutta toimiva osajärjestelmä on mahdollista luokitella, sertifioida ja rekisteröidä – osajärjestelmällä oma luokittelu, riskitaso, järjestelmälomake, profiilijoukko jne.
  - 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