Sote-tietojärjestelmien ja hyvinvointi-sovellusten luokittelu, sertifiointi ja olennaiset vaatimukset

Päivitetyt THL:n määräykset

Kanta PH (Personal Health) FHIR rajapintojen - tukiprojekti

30.4.2024

Juha Mykkänen

Terveyden ja hyvinvoinnin laitos

Taustaa ja perusteita

- Asiakastietolain uusi versio 703/2023 astui voimaan 1.1.2024
- Sote-tietojärjestelmiin on kohdistunut **vuodesta 2014 lähtien olennaisia vaatimuksia** asiakastietolain perusteella
- Olennaiset vaatimukset täytettävä **potilastietoja ja sosiaalihuollon asiakastietoja käsittelevissä tietojärjestelmissä** ja asiakastietolain määritelmän mukaisissa **hyvinvointisovelluksissa**
- Keskeisimmät tietojärjestelmät ja kaikki hyvinvointisovellukset on **sertifioitava** suhteessa olennaisiin vaatimuksiin (luokka A)
- THL määräyksillä täsmennetään
  - Järjestelmien ja hyvinvointisovellusten luokittelu
  - Järjestelmiin ja hyvinvointisovelluksiin kohdistuvat olennaiset vaatimukset
  - Sertifiointiin liittyvät menettelyt ja käytännöt
- Määräyksillä tuetaan uuden asiakastietolain ja kansallisten kehittämistavoitteiden toimeenpanoa, huomioiden myös mm. sote-uudistuksen vaikutukset ja kansallisten strategioiden ja ohjelmien tavoitteet
- Lähtökohtana on **nojautuminen aiempiin määräyksiin ja säädöksiin** (aiemmat määräykset vuodelta 2021)
  - Huomioidaan myös aiempien määräysten soveltamisesta esiin nousseet täsmennys- ja täydennystarpeet

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**

Sote-tiedonhallinnan määräykset 2024

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

Riskien hallinta

- erityisesti tietoturvallisuus ja tietosuoja
- käyttäjä-, sote-palvelu- ja tietojärjestelmätoimittaja

Vaatimusten kokoaminen

-vaatimusluettelo = hakemisto standardeista ja määrityksistä, joiden tekemiseen osallistunut satoja asiantuntijoita

Perusvaatimusten täyttymisen varmistaminen

- lainmukaisuuden varmistaminen + perustaso eri käyttötarkoituksiin tehdyille järjestelmille ja sovelluksille (innovoinnin pohjaksi)

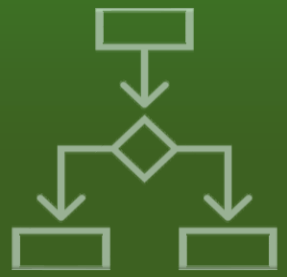
Päällekkäisyyksien välttäminen, esim.

- ei samoja vaatimuksia kuin MDR (potilasturvallisuus), pohja vaikuttavuusarvioille (HTA) ja niiden rakentuminen vakaalle säädöspohjalle, entistä suurempi osa vaatimuksista suoraan kv-standardeista ja malleista, pohja EU-kehitykseen (EHDS)...

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)

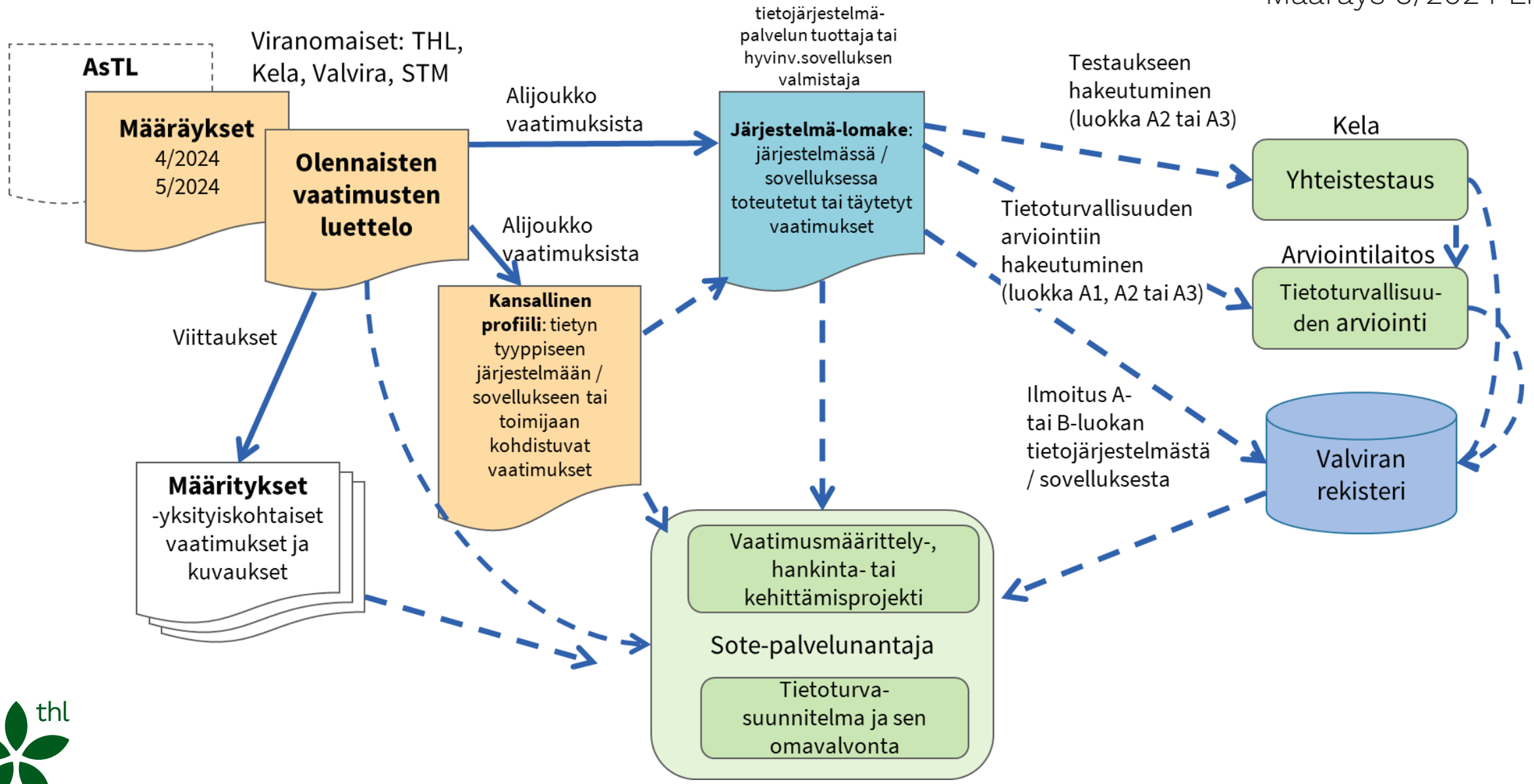
- Vaatimukset ja viittaukset määrityksiin, joilla varmistetaan järjestelmän **yhteentoimivuus** Kanta-palvelujen ja muiden järjestelmien kanssa, pohjana toiminnalliset vaatimukset ja profiilit
- Asiakastietolaki 703/2023, 86 § - Yhteentoimivuuden testaaminen
- **Sertifiointi: yhteistestaus** Kelan kanssa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

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 kokonaisuus

Määräys 5/2024 Liite 1

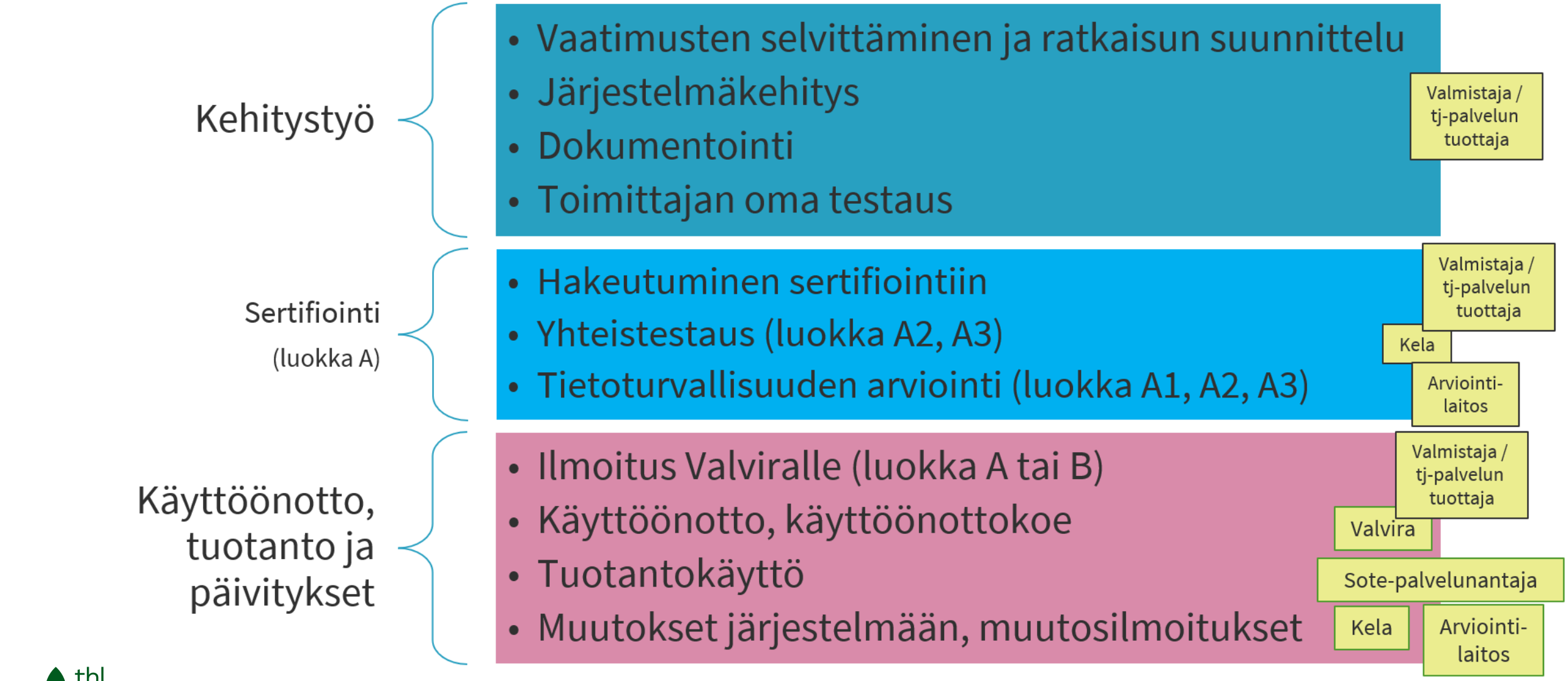


Olennaisten vaatimusten profiilit

Määräys 5/2024 liitteet 3a-3h

- Useisiin keskeisiin järjestelmien käyttötarkoituksiin pakollisten vaatimusten koonti tarkemmista määrittelyistä ja eri säädöksistä
  - 3a Sähköisen reseptin profiilit (2 profiilia)
  - 3b Kanta-asiakastietovarantoon liittyvien järjestelmien profiilit (4 profiilia)
  - 3c Potilastiedon arkiston profiilit (3 profiilia)
  - 3d Sosiaalihuollon asiakastiedon arkiston profiilit (4 profiilia)
  - 3e Kuvantamisen profiilit (5 profiilia)
  - 3f Todistusten profiilit (3 profiilia) (julkaistaan erikseen vuonna 2024)
  - 3g Asiakas- tai potilastietojen käsittelyyn tarkoitetun järjestelmän vähimmäisvaatimukset (sis. luokka B tai A1) (1 profiili)
  - UUSI: 3h Kansalaissovellusten ja hyvinvointitietojen profiilit (5 profiilia)

Sertifiointi suhteessa kehitystyöhön ja käyttöönottoihin



Määräys 5/2024 Liite 1

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

- Perusasioita ja –jäsennyksiä ei ole muutettu, pääosa tietojärjestelmien vaatimuksista samoja kuin aiemmin!
- Selkeyttää edelleen 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 järjestelmissä / profiileissa
- Linkitys Valviran tietojärjestelmärekisterin uudistamiseen

Määräysten lausuntokierroksen tuloksia

- Lausuntoaika päättyi joulukuussa 2023
- Lausuntoja tuli lausuntopalvelun kautta 16 organisaatiolta, lisäksi kommentteja määräysaiheisiin kirjaamoon ja suorilla yhteydenotoilla
- Yli 300 yksityiskohtaista kommenttia, kaikki käsitelty, pääosa aiheutti muokkauksia
- Runsaasti yksittäisiin vaatimuksiin kohdistuneita erinomaisia täsmennys- ja selkeytysehdotuksia!
- 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, viranomaistoimijoiden yhteistoiminta

Hyvinvointisovellukset ja muut digipalvelut

- Lausuntokierroksella **useita aiheeseen kohdistuvia erinomaisia lausuntoja ja ehdotuksia** sovellustoimittajilta ja tietojärjestelmätoimittajilta sekä Kelalta
- Yksittäisiä lausuntoja, jotka koskivat laissa olevia menettelyjä, joista osaa pidettiin liian vaativina vedoten siihen, että ”ei ole sattunut mitään ikävää”…
- Asiakkaiden käyttämien ja tietoja välittävien sovellusten kautta on kuitenkin toteutunut tai löytynyt merkittäviä tietosuoja- ja tietoturvariskejä ilman valvontaa tai riittäviä hyväksymismenettelyjä
- Muutamia esimerkkejä →

- ”Knight report”
  - *“The entirety of the app ecosystem examined in the report contained “pervasive authorization vulnerabilities” that enabled Knight to access more than 4 million patient and clinician records with just a single patient login account.”*
  - *” While the report found that the EHR platforms examined in the study had good security in place, third-party clinical data aggregators and mobile apps were a completely different story: with “widely systemic” vulnerabilities that allowed access to EHR data.”*
- *Tangari et al. 2021.* Analyzing security issues of android mobile health and medical applications. *J Am Med Inform Assoc. 2021 18;28(10):2074-2084.*
  - *”downloaded more than 20 000 mHealth apps from the Medical and Health & Fitness categories on Google Play”*
  - *”1.8% of mHealth apps package suspicious codes (eg, trojans), 45.0% rely on unencrypted communication, and as much as 23.0% of personal data (eg, location information and passwords) is sent on unsecured traffic”*
- Happtique / puutteellinen sertifiointi
  - *”Among the security issues uncovered by Smith were usernames and passwords stored in plain text and data stored and sent in plain text.”*
  - *“The fact neither company has reached out to me and [company] decides to tell me what seems to be nothing more than misinformation - means to me neither company cares.”*

☹

Merkittävimmät muutokset ja täydennykset 1/2

- **lokimerkintöjen ja käyttölokien** hallinnan yhtenäistämiseen liittyvien kansallisten vaatimusten toimeenpano aikatauluineen on sisällytetty olennaisiin vaatimuksiin (ei erillistä määräystä)
- määräysten suhdetta apteekkien tietojärjestelmiin ja verkkopalveluihin on selkeytetty
- tietoturvallisuuden arvioinnin ja yhteistestausten tulosten suhdetta tietojärjestelmien rekisteröintiin on täsmennetty, erityisesti **vaatimustenmukaisuutta uudistettaessa**
- Kelan **yhteistestauskokonaisuudet** on aiempaa selkeämmin linkitetty olennaisiin vaatimuksiin

Merkittävimmät muutokset ja täydennykset 2/2

- **tietoturvavaatimusten** suorat ja toteutusta tukevat **lähteet** on sisällytetty olennaisten vaatimusten luetteloon
- vaatimusten linkityksiä **kansainvälisiin standardeihin** lisätty ja selkeytetty, erityisesti tietoturva- ja digipalveluvaatimuksissa
- kansalaiselle suunnattujen digipalvelujen ja asiointipalvelujen vaatimuksia on otettu aiempaa selkeämmin omaksi osiokseen olennaisten vaatimusten kokonaisuudessa
  - aiempi hyvinvointisovellusten määräys poistuu, vaatimukset on integroitu osaksi laajempaa olennaisten vaatimusten ja sertifioinnin kokonaisuutta

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)
  - 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

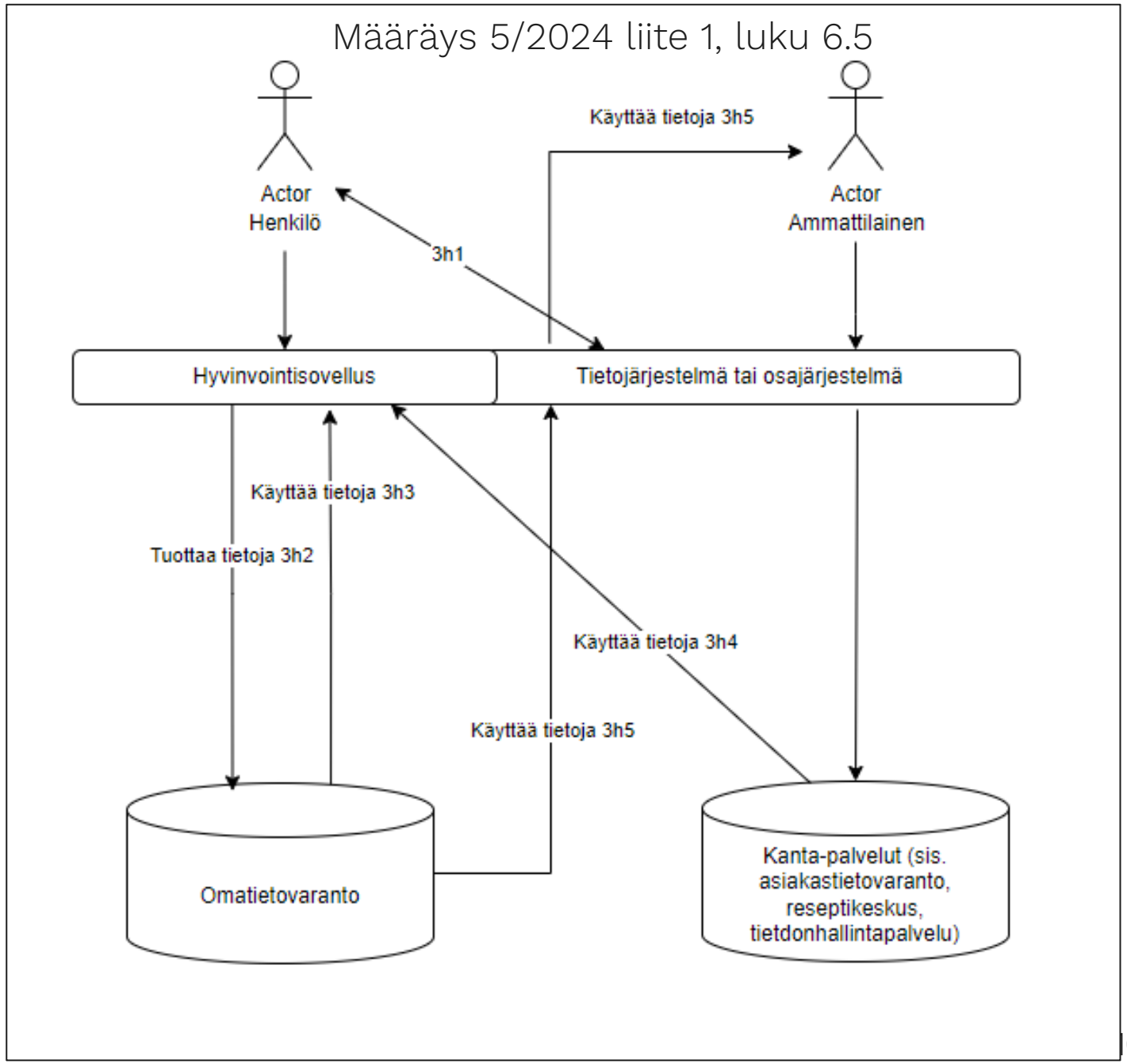
Digipalvelujen käyttäjät, profiilit ja tietovarannot

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)



Nostoja: hyvinvointisovellukset ja asiointipalvelut

- Selkeämmin erikseen profiilit omatietovarantoon tietoja tuottaville, hyvinvointitietoja hyödyntäville ja asiakastietoja hyödyntäville hyvinvointisovelluksille
- Palautetta saatiin 3h-profiilien vaatimuksista ja kuvauksista epätarkkuudesta → tarkennettu profiilien ja vaatimusten sisältöjä, lisätietoja ja lähteitä
- Samoin täsmennetty tai korjattu joukko epätarkkoja vaatimuksia (pääosin vanhoista OTV hyväksymiskriteereistä)
- Profiiliin 3h1 Palvelunantajan digitaalinen asiointipalveluun liittyvä kommentti:
  - Onko tämä profiili vain paikallisen asiakastiedon (palvelun tarjoaman rekisterinpitäjän omistaman tiedon) näyttämistä kansalaiselle?
    - Täydennetty profiilin kuvausta: Palvelussa käsiteltävät henkilö- ja asiakastiedot ovat palvelua tarjoavan palvelunantajan rekisterinpitoon kuuluvia ja ne voivat olla tallennettuna muualla kuin Kanta-palveluissa (sekä tuottaminen että näyttäminen)
- Hyvinvointisovelluksissa erityisesti pyritty madaltamaan kynnystä *Omatietovarantoon tietoja tuottavien* sovellusten toteuttamisen helpottamiseksi

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 uhkaympäristö huomioiden
- Määräysten **lukumäärä vähenee** ja olennaisten vaatimusten **integraatio paranee**
  - Hyvinvointisovellusten ja digipalvelujen vaatimukset osaksi samaa kokonaisuutta tietojärjestelmävaatimusten kanssa, olennaisten vaatimusten selkeämpi linkitys yhteistestauskokonaisuuksiin, tietoturvavaatimusten lähteet, jne.
- Menettelyjen ja vaatimusten voimaantuloissa huomioidaan **jatkuvuus**: esim.
  - 2023 tai alkuvuonna 2024 käynnistetyt sertifioinnit mahdollista suorittaa loppuun aiempien menettelyjen ja vaatimusten pohjalta
  - uusien vaatimusten voimaantuloajat kehittämis-, hankinta- ja sertifiointisyklit huomioiden
- Määräykset **julkaistaan mahdollisimman pian** – käännökset juuri valmistuneet, viimeiset vaatimus- ja profiiliyksityiskohdat viimeisteltävänä
- Julkaisu Finlex-palvelussa ja THL:n sivuilla

Tulossa myös

- Tukimateriaalit
  - Päivitetty **riskiarviotyökalu** (mm. järjestelmien riskitason, tietojen käytön laajamittaisuuden arvioinnin ja tietojärjestelmän luokittelun tukemiseen)
  - Olennaisten vaatimusten ja profiilien **koontitaulukko**
    - Helpottaa vaatimusten kokoamista esim. järjestelmiin tai järjestelmäkokonaisuuksiin, joilla laaja käyttötarkoitus / useita profiileja
- **Olennaisten vaatimusten ja sertifioinnin koulutustilaisuus**
  - **kevätkaudella / alkukesästä, tarkka ajankohta ilmoitetaan THL tapahtumakalenterissa ja tulevissa tapahtumissa**
- Tietoturvasuunnitelman koulutustilaisuus 4.6.2024
- Seuraavia säädösten uudistuksia jo näköpiirissä
  - STM käyttöoikeusasetus, asiakastietolain seuraava versio, Euroopan terveysdata-avaruuden (EHDS) huomiointi ja voimaantulo…

Kiitokset!
Kysymyksiä?

sotetiedonhallinta@thl.fi

Terveyden ja
hyvinvoinnin laitos