

# Sote-tietojärjestelmien olennaiset vaatimukset ja sertifiointi -koulutus 14.6.2024 – Q & A

Koulutuksen aikana esille nousseet  
kysymykset ja niihin vastaukset

Sote-tiedonhallinnan ohjaus  
sotetiedonhallinta@thl.fi

Terveyden ja hyvinvoinnin laitos  
Institutet för hälsa och välfärd  
Finnish Institute for Health and Welfare  
PL / PB / P.O. Box 30  
FI-00271 Helsinki, Finland  
Puh/tel +358 29 524 6000  
thl.fi

## KANTA-LIITTYMINEN JA JÄRJESTELMÄN LUOKKA

Eikö myös Kantaan liittyminen ole velvoitettu jokseenkin kaikilta järjestelmiltä, eli käytännössä B-luokan järjestelmiä ei tulevaisuudessa olisi?

THL: Kantaan liittymisen velvoite kohdistuu palvelunantajiin ja asiakastietojen toimittamiseen Kanta-palveluihin, ei suoraan jokaiseen tietojärjestelmäpalvelun tuottajaan tai tietojärjestelmään. On mahdollista olla nyt ja jatkossakin luokan B järjestelmiä. Esimerkiksi sairaaloissa on usein myös luokkaan B kuuluvia järjestelmiä. Palvelunantajan Kanta-velvoitteiden täyttämiseen tarvitaan kuitenkin luokan A järjestelmä / järjestelmäkokonaisuus. Luokan A3 järjestelmä tai järjestelmäkokonaisuus tarkoittaa järjestelmää, jolla voi täyttää palvelunantajan Kanta-palveluihin liittyvät velvoitteet. Myös osa profiileista on sekä A- että B-luokkaan soveltuvia.

**Valviralle: Koskevatko katselukäyttöön jäävän ja siis luokasta A => B siirtyvää edelleen vanhat, alkuperäiset A-luokan vaatimukset vai miten ? Ajattelen ensimmäisenä vaikkapa erilaisia käyttöoikeuksien ja tietojen näyttämisen rajoituksia - toisaalta niitä ei välttämättä liioin saada toimimaan vanhassa järjestelmässä uusien määritysten mukaisina.**

**Vanhassa tietojärjestelmässä (lokaalisti) tallennettuna olevan käytöltään rajattu asiakastieto ei kuitenkaan muutu maagisesti vähemmän arkaluonteiseksi vain tuon käyttötarkoituksen muutoksella? Mitenkähän asia käytännössä toimii, onko tästä oikeasti kokemuksia?**

THL: Järjestelmän käyttötarkoitus muuttuu, jos järjestelmä on aiemmin ollut Kanta-palveluihin liittyvä mutta ”ei ole enää”. Vaatimuskohtaisesti on hyvä tarkistaa, poistuuko esim. Kanta-palveluihin liittyviä (joita paljon luokassa A) vaatimuksia, jotka eivät enää ole relevantteja, jos järjestelmä siirtyy luokkaan B siksi että järjestelmä ei enää liity Kantaan. Jotkin arkaluonteisen tiedon hallintaan ja pääsynvalvontaan liittyvät vaatimukset voivat toki myös säilyä ennallaan.

Valvira: Järjestelmän käyttötarkoituksen merkitys on keskeinen, kun tarkastellaan järjestelmään kohdistuvia vaatimuksia. Jos käyttötarkoitus muuttuu, tietojärjestelmäpalvelun tuottajan on tarkastettava järjestelmän profiili/profiilitiedot ja tarkemmat vaatimukset. Paikalliseen katselukäyttöön tarkoitettussa järjestelmässä esimerkiksi pääsynhallintaan ja lokitukseen liittyvät vaatimukset ovat tyypillisesti edelleen relevantteja, kun taas Kanta-integraatioon liittyvät vaatimukset eivät enää koske järjestelmää.

## **VALVIRA/ASTORI:**

**Voiko Astorista hakea tietoa vaatimustenmukaisuuden voimassaolon päättymisajalla?**

Valvira: Merkittävien poikkeamien avulla (esim. vanhentunut todistus) hakeminen on mahdollista. Ainakaan rekisterin ensimmäisessä versiossa tietojärjestelmien listaaminen tietoturvaluustodistuksen viimeisen voimassaolopäivän mukaan ei ole mahdollista. Valvira ottaa palautetta ja jatkokehitystoiveita mielellään vastaan.

## **STANDARDIT, LAATUJÄRJESTELMÄT SERTIFIOINNISSA:**

**Huomioidaanko sertifiointiprosessissa mm. tietoturvaan liittyviä standardeja? Eli jos toimijalla on tietoturva- ja laatustandardeja jo hankittuna, se keventää sertifiointiprosessia?**

THL: Laatustandardin mukainen laatujärjestelmä on erittäin hyvä tapa täyttää myös asiakastietolain laatuvaatimus. Myös monet yksityiskohtaisemmista vaatimuksista viittaavat standardeihin, joihin ne suoraan perustuvat tai joiden avulla vaatimuksesta löytyy tarkempaa tietoa (sisällöstä tai soveltuvasta täyttämistavasta).

Sertifiointiprosessi voi keventyä, jos siihen kuuluvien vaatimusten täyttyminen on jo esimerkiksi jossain todennettu, näiden asioiden ilmaisemiseen on mm. oma paikka järjestelmälomakkeessa (Perustiedot-sivu, kohta 11). Tietoturva-vaatimusten ja mm. digipalvelujen vaatimusten lähteissä on viittauksia standardeihin, joiden mukaisesti vaatimuksen toteuttaminen on hyvä tapa vaatimuksen täyttämiseen.

## **DIGIPALVELUT:**

**Ymmärsinköhän "hyvinvointisovelluksen" määritelmän väärin - eli esim. pelkästään hv-alueen omaan portaaliin/PHR-tietovarantoon tai APTJ:hen liittyvä (yleisen kielenkäytön mukainen hv-) sovellus ei siis sisälly määritelmään ? Onko tässä tapahtunut jokin tuore muutos, koska minulla on hatara mielikuva määritelmän viimeksi perustuneen yleisesti "terveystietojen käsittelemiseen" (sen jälkeen, kun sidonnaisuudesta kirjaimellisesti Kanta Omatietovarantoon luovuttiin).**

THL: Lain määritelmän (ja määräyksissä tarkoitettu) mukainen hyvinvointisovellus on pelkästään Kanta-palveluihin liittyvä: hakee tai tuottaa hyvinvointitietoja omatietovarantoon, tai hakee muista Kanta-palveluista asiakkaan käyttöön asiakastietoja. Määritelmä ei tietääksemme ole perustunut ”terveystietojen käsittelemiseen”.

**Hmmm. Onko "palvelunantajan digitaalinen asiointipalvelu" siis erikoistapaus, joka ei välttämättä ole "hv.sovellus" aikaisemman määritelmän mukaisesti mutta silti vaatimusten piirissä?**

THL: Palvelunantajan digitaalinen asiointipalvelu voi täyttää laissa olevan ”tietojärjestelmä” määritelmän, jos se on asiakastietojen käsittelyyn tarkoitettu ja esim. tallentaa asiakastietoja palvelunantajan omaan henkilökisteriin. Tällaiset järjestelmät ja palvelut ovat vaatimusten piirissä. ”Digipalvelu” termiä käytetään sekä hyvinvointisovelluksista että tällaisista asiointipalveluista, joissa on kansalaisille suunnattuja ominaisuuksia ja käyttöliittymiä. Profiilien kuvauksissa asiaa on kuvattu tarkemmin.

**Onko termiä "käyttö" tarkemmin määritelty hv.sovellusten kontekstissa ?  
Täyttyykö se jo pelkästään tietojen hakemisella Kannasta vai vasta jos hakutulokselle "tehdään jotain" tai "hyödynnetään tietoja johonkin" ? Entä onko vaikkapa haettujen CDA-muotoisten asiakastietojen prosessointi asiakkaalle helppolukuiseen muotoon "käyttöä"?**

THL ja Kela: Myös tietojen hakeminen ja haettujen tietojen prosessointi asiakkaalle toiseen muotoon on tietojen käyttöä. Tämä on myös riskinäkökulmasta luontevaa. Myös tällaisiin käyttökohteisiin löytyy relevantit olennaiset vaatimukset esim. ”Digit.palvelujen vaatimukset” - osiosta olennaisten vaatimusten luettelosta ja järjestelmäomakkeesta.

**Olettaen että hv.sovelluksia (ja niihin rinnastettavia) alkaisi tulla suuremmissa määrin mukaan, onko antaa arviota siitä kestäkö sertifiointin prosessi, yhteistestaukset, ulkoisten arviointilaitosten kapasiteetti jne. merkittävästi suuremman määrän käsiteltäviä kohteita?**

THL: Toivottavasti. Sertifiointinissa vaikuttaa olevan vaihtelevasti kuormitusta, välillä ruuhkaa ja välillä vähemmän käynnissä olevia. Prosessia sujuvoittaa merkittävästi se, että täytetyt vaatimukset kuvataan selkeästi ja oikein järjestelmäomakkeessa ja dokumentointi on hoidettu hyvin.

Kela: Tällä hetkellä emme ole tunnistaneet riskiä sen suhteen, että yhteistestaukseen olisi lähiaikoina tulossa merkittäviä määriä hyvinvointisovelluksia ja yhteistestaus ruuhkautuisi. Periaatteessa, jos samanaikaisesti tulisi useita hyvinvointisovelluksia tekemään yhteistestausta, se varmaan vaikuttaisi yhteistestauksen keston. Samoin uusien tietosisältöjen yhteistestaus kestää usein vähän pidempään kuin vanhojen.

Yleensä yhteistestausten kesto vaihtelee järjestelmäkohtaisesti ja näin mahdollisesti myös hyvinvointisovellusten kohdalla.

Hyvinvointisovellusten yhteistestauskäytännöt vakiintuvat vähitellen, mutta pääpiirteissään hyvinvointisovellusten yhteistestaus ei merkittävästi eroa tietojärjestelmien yhteistestauksesta.

Toimittajan on hyvä perehtyä yhteistestausprosessiin ja ohjeistuksiin ajoissa, sillä uudelle toimittajalle yhteistestauksen työtiloihin ja toimintatapoihin tutustuminen voi myös viedä aikaa. Tarvittaessa yhteistestauksesta saa tukea prosessin käynnistämiseen. Jos yhteistestauksen aikana ilmenee hyvinvointisovelluksen toteutuksessa asioita, joihin toimittajan pitää tehdä vielä uutta sovelluskehitystä, se myös vaikuttaa yhteistestauksen keston.

Valvira: Asiakastietolain 81 §:n mukaan hyvinvointisovellusta ei saa ottaa tuotantokäyttöön, ellei siitä ole ajantasaisia tietoja Valviran tietojärjestelmärekisterissä. Sertifiointin lisäksi hyvinvointisovelluksen valmistajan on hyvä varata riittävä aika myös rekisteröintiprosessille.

**Jatkokommentti: Niimpä eli "kuorma" prosessissa on kaikille yhteinen. Ja kohta saamme ehkä/vielä mukaan EU-ulottuvuudenkin.**

**MUITA:**

Edelleen jääkö siis säätelyyn aukkopaiikka siihen, ettei hyväksytyn tietojärjestelmän (ohjelmistona ajateltuna) asennetun instanssin käyttöä tietyssä organisaatiossa erikseen "sertifioida" ? Hyväksymisprosessiin sisältyvä tietojärjestelmän testikäyttö ja testiympäristö on kuitenkin eri asia kuin tuotanto, varsinkin pitemmällä aikajänteellä katsellen (muutokset koodistoissa, Kanta-tietosisällöissä jne.). Olisiko mahdollisuuksia tomerammin puuttua vaikkapa siihen, miten ja millä aikataululla tietojärjestelmän asiakasorganisaatiot ottavat (jo toteutettuja tai tilaavat toteutuksen) Kanta-toiminnallisuuksia käyttöönsä - on jotenkin surullista, että esim. "potilastietojen 2016-tasonnosto" on edelleen yhtään mitenkään agendalla.

THL: Suomen lainsäädännön mukainen sertifiointi on tuotesertifiointia, jossa yksi järjestelmä voidaan ottaa käyttöön monissa paikoissa tai käyttöympäristöissä hyväksynnän jälkeen. Jokaisessa organisaatiossa erikseen sertifiointi lisäisi myös kustannuksia. "Tasonnosto" -aiheeseen liittyvät keskeisten terveystietojen vaatimukset ovat voimassa edelleen.

Valvira: Jos terveydenhuollon palvelunantaja on laiminlyönyt lakisääteisen veloitteen toteuttamisen, siitä voi ilmoittaa paikalliselle aluehallintoviranomaiselle, joka valvoo sosiaali- ja terveydenhuollon järjestämisen ja tuottamisen lainmukaisuutta ja antaa siihen liittyvää ohjausta. palvelunantajia. Ilmoituksen voi tehdä myös Valviralle.