Sote-tietojärjestelmien luokittelu, sertifiointi ja omavalvonta: usein kysytyt kysymykset

Versio 22

29.12.2016

Tietopalvelut, Operatiivisen toiminnan ohjaus (OPER)

Terveyden ja hyvinvoinnin laitos (THL)

PL 30 (Mannerheimintie 166)
00271 Helsinki
Telephone: 029 524 6000

www.thl.fi

Sisältö

1 Dokumentin tarkoitus

Tähän dokumenttiin on koottu sote-tietojärjestelmien luokittelussa, sertifioinnissa ja omavalvontasuunnitelmien laadinnassa ja hyödyntämisessä esiin nousseita kysymyksiä ja niihin liittyviä vastauksia. Dokumentti täydentää säädöksiä, määräyksiä ja ohjeita sote-tietojärjestelmien luokittelusta ja sertifiointikriteereistä. Se sisältää ajan tasaisia vastauksia ja tulkintoja esitettyihin kysymyksiin. Tulkintoja voidaan edelleen tarkentaa.

2 Yleisiä kysymyksiä

2.1 Dokumentin sitovuus

Kysymys: Miten sitovia tässä dokumentissa esitetyt asiat ovat?
Vastaus: THL voi antaa erillisiä määräyksiä esimerkiksi järjestelmien luokittelusta ja uusia määräyksiä omavalvonnasta ja järjestelmien olennaisista vaatimuksista. Tässä dokumentissa kuvatut asiat toimivat mahdollisesti myöhemmin annettavien määräysten pohjana. Dokumenttia tullaan päivittämään tarpeen mukaan. Ensisijaisesti noudatettavia ovat aina varsinaiset säädökset ja määräykset.

3 Tietosuojan ja tietoturvallisuuden omavalvontasuunnitelma: kysymyksiä ja vastauksia

3.1 Omavalvontasuunnitelman tekeminen ja tarkennukset organisaatiossa

Kysymys: Mitkä omavalvontasuunnitelman vaatimuksista on täytettävä tai mitkä kuvaukset laadittava minun organisaatiossani?
Vastaus: Omavalvontasuunnitelmaan on sisällytettävä ne kohdat ja kuvaukset, jotka ovat relevantteja sote-palveluja tuottavassa tai Kanta-välittäjänä toimivassa organisaatiossa. Usein on järkevää viitata ulkoisiin dokumentteihin, joissa toimintatavat ja menettelyt on kuvattu, mutta asioita voidaan myös kuvata varsinaisessa omavalvontasuunnitelmassa. Osa relevanteista vaatimuksista voidaan hoitaa ulkoisen tahon toimesta esimerkiksi sopimus- tai palveluhankintamenettelyillä, mutta nekin on voitava todentaa.

Kysymys: Mitkä asiat kannattaa kuvata ja tarkentaa ensimmäisenä omavalvontasuunnitelmassa?
Vastaus: Hyvänä käytäntönä on nähty se, että ensimmäisenä määritellään suunnitelman rajaus (ketä kaikkia ja mitä toimijoita suunnitelma koskee) sekä se, mitkä ovat toiminnassa käytettäviä ja suunnitelman piirissä olevia tietojärjestelmiä. Tietojärjestelmien tunnistaminen ja asettaminen ”kriittisyysjärjestykseen” auttaa yleensä myös tarkentamaan suunnitelman muita kohtia. Rajauksen osalta keskeistä on saada ensin kuvattua ”organisaation omat” vastuualueet ja järjestelmät, jonka jälkeen on mahdollista edetä palveluntuottajien ja sopimusten läpikäyntiin. Sote-palveluntuottajan omavalvontasuunnitelmassa on kuvattava kuinka varmistetaan se, että myös mahdolliset alihankkijat tai välittäjät noudattavat vaatimuksia, ja vaatimusten toteutuminen on oltava todennettavissa. Joka tapauksessa sote-palveluntuottajan omavalvontasuunnitelman kautta on keskeistä pystyä osoittamaan se, kuka vastaa kunkin vaatimuksen täyttämisestä sellaisten vaatimusten osalta, jotka ovat palveluntuottajan toiminnassa relevantteja.

Kysymys: Mitä aiemmin tehtyjä dokumentteja kannattaa käyttää omavalvontasuunnitelman pohjana?
Vastaus: Omavalvontasuunnitelma on mahdollista ”koota” useista eri tarkoituksiin liittyvistä osista ja dokumenteista, tai se on mahdollista koostaa ”linkittämällä” tai viittaamalla muihin eri seikkoja kuvaaviin dokumentteihin. Tietoturvapolitiikka on usein käyttökelpoinen dokumentti omavalvontasuunnitelman laatimisessa, mutta sen tarkkuustasosta ja sisällöstä riippuu missä määrin sen avulla vaatimukset voidaan

täyttää tai todentaa. Myös omassa laatukäsikirjassa (mikäli laatutyötä on tehty) on usein hyödyllistä myös omavalvontasuunnitelmaan liittyvää materiaalia. Esimerkiksi laatuauditointien tai -läpikäyntien liittäminen omavalvontasuunnitelman ja tietoturvallisuusasioiden läpikäyntiin on usein järkevää. Omavalvontaa on mahdollista toteuttaa esimerkiksi samassa rytmissä laatuauditointien kanssa tai laatujärjestelmän vuosikellon mukaisesti. Muita omavalvontasuunnitelmaan liittyviä dokumentteja voivat olla esimerkiksi kokonaisarkkitehtuurikuvaukset kuten tietoturvaperiaatteiden ja tietojärjestemien tai tietojärjestelmäpalvelujen sekä verkkojen ja näihin liittyvien tietoturvallisuuskäytäntöjen kuvaukset.

Kysymys: Voiko omavalvontasuunnitelman jakaa osiin?
Vastaus: Omavalvontasuunnitelman sisällön ei ole välttämätöntä olla yhdessä dokumentissa. Esimerkiksi eri henkilöstöryhmille voi olla omia tiivistelmiään / osioitaan, esimerkiksi järjestelmien ylläpitoyksityiskohdat eivät ole tarpeellisia kaikille ”peruskäyttäjille”.

Kysymys: Mikä on Asiakastietolain mukaisen omavalvontasuunitelman suhde Valviran omavalvontasuunnitelmaan?
Vastaus: Valviraan tehtävä omavalvontasuunnitelma on laajemmin toiminnan kannalta tehtävä. Asiakastietolain mukainen omavalvonta keskittyy asiakas- ja potilastietojen käsittelyyn, tiedonhallintaan, tietojärjestelmien hallintaan sekä tietoturvaan ja tietosuojaan. Nämä omavalvontasuunnitelmat on yleensä järkevää erottaa toisistaan.

Kysymys: Tuleeko omavalvontasuunnitelman olla julkisesti nähtävillä, esim. internetissä vai riittääkö, että suunnitelma on rajatun henkilöstön nähtävillä?
Vastaus: Suunnitelman ei tarvitse olla julkisesti nähtävillä, ja suunnitelma voi sisältää myös sellaisia tietoja joita ei tule luovuttaa ulkopuolisille tai jaella julkisesti. Suunnitelman tulisi kuitenkin olla niiden toimijoiden saatavilla joiden tulee osata toimia suunnitelman mukaisesti. Henkilöstön tulee olla tietoinen omavalvontasuunnitelmasta tai ainakin niistä sen asioista jotka heitä suoraan koskevat. Myös asiakkaat voivat vaatia että pystytään osoittamaan omavalvonnan toteutuminen ja toimivuus. Lain mukaisesti omavalvontasuunnitelman toteutumista on seurattava. Tarkastusviranomaisille tulee pystyä tarvittaessa esittämään omavalvontasuunnitelma ja kuinka sitä koskevat vaatimukset todennetaan.
Omavalvontasuunnitelmassa ja tietoturvallisuuden toteuttamisessa on huomioitava myös esimerkiksi varautuminen ja toipuminen: esimerkiksi tietoverkko-ongelmien toimintaohjeet henkilöstölle tulisi olla tarvittaessa saatavilla muutenkin kuin tietoverkon kautta.

Kysymys: Miten esimerkiksi lääkäriasemalla jossa toimii tulee hoitaa omavalvontasuunnitelma?
Vastaus: Usein on järkevää, että lääkäriasema vastaa omavalvontasuunnitelman laatimisesta, ja asemalla työskentelevien sopimuksissa varmistetaan, että he tuntevat suunnitelman ja osaavat toimia sen mukaisesti, tai vastaavat joistakin suunnitelmaan kuuluvista asioista.

Kysymys: Kuinka pienehkö yritys tai yhdistyspohjainen toimintayksikkö voisi järkevästi tehdä omavalvontasuunnitelman? Ero on suuri verrattuna Kelaan tai esimerkiksi apteekkeihin.
Vastaus: Omavalvontasuunnitelman mukaisten vaatimusten dokumentointi ja omavalvonta. Omavalvontasuunnitelman yleinen mallipohja sisältää erilaisissa tilanteissa ja organisaatioissa huomioitavia seikkoja, joista huolehtiminen on tarpeen omavalvonnassa yleisesti.
Omavalvontasuunnitelman yleinen mallipohja löytyy mm. osoitteesta:
https://www.thl.fi/fi/web/tiedonhallinta-sosiaali-ja-terveysalalla/tiedon-ja-vaatimusten-yhdenmukaistaminen/maaraykset-ja-ohjeet
Potilastiedon arkiston käyttöönoton käsikirjassa yksityisille on saatavilla myös mallipohja, joka on suunnattu yrityksille tai itsenäisille ammatinharjoittajille (kohdasssa ”Mallilomakkeet / Omavalvonnan vaatimukset ja ohjeet yrityksille/itsenäisille ammatinharjoittajille”):
http://www.kanta.fi/web/ammattilaisille/vanhat-materiaalit

Kysymys: Kuka sopii tietosuojavastaavan tehtävään, pitääkö valittu henkilö kouluttaa siihen, onko koulutusta tarjolla ja mitä se maksaa?
Vastaus: Tietosuojavastaavan tehtävään ei ole erityisiä soveltuvuuskriteereitä tai koulutusvaatimuksia, mutta yleinen kuvaus tehtävästä löytyy esimerkiksi osoitteesta http://www.kanta.fi/fi/tietosuojavastaava
Kanta-palvelujen käsikirjassa on kuvattuna mallipohja Tietosuojavastaavan tehtäväkuvan määrittelemiseksi: http://www.kanta.fi/fi/web/ammattilaisille/vanhat-materiaalit
Kanta-sivuilla on myös saatavilla tietoturvan ja tietosuojan verkkokoulu: http://www.kanta.fi/reseptikoulutus/tietoturva.html
Verkosta ja kirjakaupoista on saatavilla tietosuojavastaavien tehtäviä tukevaa kirjallisuutta, mm. ”Tietosuojavastaavan käsikirja 1 ja 2".
Vuosittaisia sosiaali- ja terveydenhuollon tietosuojaseminaareja ja tapahtumia järjestävät mm. Tietosuojavaltuutettu, Suomen Kuntaliitto, STTY:n (Sosiaali- ja terveydenhuollon tietojenkäsittely-yhdistys) tietosuojavastaavien jaosto sekä useat kaupalliset koulutus- ja seminaarijärjestäjät.

Kysymys: Kuinka tarkka esitys omavalvontasuunnitelman liitteeksi pitää tietoturvapolitiikasta yrityksissä tehdä? Voidaanko hyödyntää esimerkiksi järjestöjen jäsenistöilleen tuottamia Tietoturvapolitiikan malleja? Riittääkö se, että yrittäjä liittää sen osaksi omavalvontasuunnitelmaa edellyttäen tietenkin, että on sisäistänyt sen sisältämän sanoman?
Vastaus: Mallipohjia voi hyvin käyttää. Keskeistä on se, että palvelun tuottaja sisäistää asian, ja täydentää mallipohjan oman organisaationsa näkökulmasta siten, että vaatimukset täyttyvät ja voidaan todentaa.

Kysymys: Miten määritellään laissa edellytetty henkilöstön riittävä kokemus?
Vastaus: Henkilöstön kokemus järjestelmän käyttöön kasvaa käytön ja koulutusten myötä. Esimerkiksi uusien järjestelmien käyttöönottotilanteissa ei käyttäjiltä voida edellyttää pitkällistä kokemusta kyseisen järjestelmän käytöstä. Keskeistä on, että uusille työntekijöille järjestetään riittävä koulutus ja perehdytys järjestelmän käyttöön ja myös käyttötaitojen ylläpidosta huolehditaan esimerkiksi koulutusten avulla.

3.2 Omavalvonta ja Kanta-palvelut

Kysymys: Liittyykö omavalvontasuunnitelma vain Kanta-palveluihin liittyviin tietojärjestelmiin? Kun dokumentin ensimmäinen varsinainen versio saadaan organisaatioissa tehtyä, lienee tärkeintä kohdistaa sisältöä ennen kaikkea Kanta-alueelle, ts. potilastietojärjestelmiin?
Vastaus: Omavalvontasuunnitelma ei liity pelkästään Kanta-palveluihin, vaan sen kohteena on asiakas- ja potilastietojen käyttö yleisesti. Suunnitelmassa on erikseen kohtia, jotka liittyvät erityisesti Kanta-palvelujen käyttöön, mutta valtaosa asioista koskee myös muita tilanteita ja myös sellaisia järjestelmiä, jotka eivät ole liittyneet Kanta-palveluihin. Kanta-palveluihin ja niiden kautta saataviin tietoihin liittyvät vaatimukset ovat erityisen keskeisiä, koska näiden palvelujen kautta on periaatteessa mahdollista päästä suurempaan joukkoon potilas- ja asiakastietoja, joten niihin liittyvien kohtien suunnittelu organisaatioissa joissa liitytään Kanta-palveluihin on tärkeä lähtökohta myös muille suunnitelman sisällöille.

Kysymys: Mitä uusia vaatimuksia Kantaan siirtyminen tuo omavalvontasuunnitelman sisältöön?
Vastaus: Kanta-palveluihin liittyvillä organisaatioilla on tarkempia vaatimuksia mm. käyttövaltuuksien hallintaan, varmenteiden hallintaan, tunnistamis-, todentamis- ja allekirjoitusratkaisuihin ja käytön seurantaan liittyen. Myös Kanta-palveluihin liittymisessä käytettävien järjestelmien ja teknisten välityspalvelujen on oltava sertifioituja A-luokkaan kuuluvia järjestelmiä, joilla on voimassa oleva vaatimustenmukaisuustodistus. Näitä vaatimuksia on koottu esimerkiksi omavalvontasuunnitelman mallipohjan lukuun 6. Erityisiä Kanta-vaatimuksia kohdistuu mm. seuraaviin asioihin:

- Kanta-palvelujen käytön seuranta ja valvonta ovat erityisesti huolehdittavia seikkoja, koska saatavilla voi olla myös muiden palvelun tarjoajien luovuttamaa jatuottamaa tietoa
- Kanta-palvelujen pääsynhallinnan toteuttaminen
- Sosiaali- ja terveydenhuollon dokumenttien ja rekisterien erottaminen
- Vaatimuksenmukaisuustodistuksen edellyttäminen Kanta-palveluihin liittyviltä tietojärjestelmiltä ja teknisiltä välityspalveluilta
- Häiriötoimenpiteet huomioiden kansalliset häiriö- ja muutosohjeet.

3.3 Omavalvonta ja sosiaalihuolto

Kysymys: Onko omavalvontasuunnitelma tehtävä myös sosiaalihuollossa niiden järjestelmien osalta, joista tiedot eivät lähde potilastiedon arkistoon vaan aikanaan sosiaalihuollon asiakastietojen arkistoon? Siis onko omavalvontasuunnitelma tehtävä esim. sosiaalityössä käytettävän järjestelmän osalta?
Vastaus: Omavalvontasuunnitelma sisältää joitakin asioita, jotka liitttyvät Kanta-palvelujen käyttöönottoon, mutta pääosa asioista on sellaisia joista huolehtiminen on tarpeen kaikessa asiakas- ja potilastietojen käsittelyssä. Omavalvontasuunnitelma ei ole tietojärjestelmäkohtainen vaan toimijakohtainen, mutta siinä on tarpeen myös viitata käytettäviin järjestelmiin ja siihen miten niiden osalta omavalvonnasta huolehditaan.

Kysymys: Käsitelläänkö tulevissa omavalvontasuunnitelmien versioissa myös sosiaalihuollon asioita ja sosiaalihuollon asiakastietojen arkistoon liittyvien ratkaisujen vaatimuksia? Miltä osin nyt huomioidaan omavalvontasuunnitelmassa sosiaalitoimen tietoturva ym. käytännöt?
Vastaus: Jo nykyisten määräysten mukaiset omavalvonnan kohteet sisältävät monia sosiaalihuollon asiakastietoja koskevia kohtia. Kanta-palveluihin (mukaan lukien sosiaalihuollon Kanta-palvelut) liittyviä kohtia tarkennetaan tarvittaessa, kun sosiaalihuollon valtakunnalliset tiedonhallinnan palvelut tulevat vähitellen käyttöön. Myös tietojärjestelmien olennaisten vaatimusten ja toiminnallisuuksien ryhmittelyssä ja vähimmäisvaatimuksia kuvaavissa profiileissaon mukana sosiaalihuollon asiakastietojen arkistoon liittyvien järjestelmen vaatimusten määrittelyjä.

Kysymys: Jos toimintaamme kuuluu sekä sosiaali- että terveyspalveluja, teemmekö yhden yhteisen omavalvontasuunnitelman tietosuojan ja tietoturvallisuuden omavalvontaa varten?
Vastaus: Sosiaali- ja terveyspalveluihin yleensä järkevää tehdä yhteinen tietoturvallisuuden ja tietosuojan omavalvontasuunnitelma, etenkin jos organisaation toimintaan kuuluu molempia ja tiedonhallinnan ja tietosuojan käytäntöjä pyritään yhtenäistämään. Eriyttäminen on perusteltua, jos myös toiminta on eriytettyä.

3.4 Omavalvonta ja tietojärjestelmät

Kysymys: Mistä tiedän, mitkä asiat omavalvonnassa kuuluvat sosiaali- ja terveydenhuollon palveluntuottajan / ammatinharjoittajan vastuulle ja mitkä tietojärjestelmätoimittajan vastuulle?
Vastaus: Kokonaisvastuu omavalvontasuunnitelman laatimisesta, suunnitelman mukaisesta toiminnasta ja toteutumisen seurannasta on sosiaali- ja terveydenhuollon organisaatiolla ja sen toiminnasta vastaavalla johtajalla. Järjestelmätoimittajien roolit voivat vaihdella järjestelmien hankinta- ja ylläpitomallin mukaisesti. Lisäksi joitakin omavalvontaan kuuluvia asioita on mahdollista sopia hoidettavaksi esimerkiksi tietohallintopalveluja tuottavan tahon tai Kanta-välittäjän toiminnassa. Vastuut on kirjattava sopimuksiin. Omavalvontasuunnitelmaan kuvataan, miten asiasta on sovittu järjestelmätoimittajan ja muiden mahdollisten tahojen kanssa. Esimerkiksi hankittaessa järjestelmä palveluna järjestelmätoimittaja voi vastata järjestelmän teknisestä ylläpidosta, versioiden asennuksista, tietoliikenteestä, useista käyttöympäristön vaatimuksista ja niin edelleen.

Kysymys: Mitkä järjestelmät on sisällytettävä omavalvontasuunnitelmaan? Järjestelmät, jotka on liitetty kansallisiin palveluihin (Kanta, potilastiedon arkisto, eResepti, sosiaalihuollon asiakastiedon arkisto) vaiko laajemmin? Millä perusteilla poimitaan mukaan otettavat?
Vastaus: Omavalvontasuunnitelmaan on otettava mukaan ainakin järjestelmät, joiden käyttötarkoituksena on luottamuksellisten tai salassa pidettävien asiakas- tai potilastietojen käsittely (A- ja B-luokkiin kuuluvat järjestelmät). Erityistä huomiota kannattaa kiinnittää A-luokan järjestelmiin, jotka liittyvät Kanta-palveluihin. Suunnitelmaan on mahdollista ottaa mukaan myös muita järjestelmiä, joiden tietosuoja- ja tietoturvakäytäntöjä halutaan ottaa suunnitelman piiriin, esimerkiksi henkilöstön tietoja sisältävissä järjestelmissä voi olla samantyyppisiä vaatimuksia. Omavalvontasuunnitelmasta voidaan myös viitata tarkempiin järjestelmäkohtaisiin kuvauksiin.

Kysymys: Miten varmistetaan ja todennetaan, että tietojärjestelmiä käytetään valmistajan antamien ohjeistusten mukaisesti tai niitä tarkoituksenmukaisesti soveltaen tai täydentäen?
Vastaus: Kun koulutus, ohjeistus ja seuranta on toteutettu siten, että ajantasaiset ohjeistukset ovat saatavilla ja käyttäjät tuntevat ohjeet, ja käyttöön liittyville käyttäjien kysymyksille (myös ohjeisiin liittyen) on määritelty selkeä ja tiedossa oleva toimintatapa, ei pidemmälle menevää todentamista voida nykyisellään edellyttää.

Kysymys: Onko olemassa yksityiskohtaisia ohjeita lokivalvonnan toteuttamisesta eri potilastietojärjestelmissä?
Vastaus: Kanta-määrittelyissä (mm. potilastietojärjestelmien käyttötapaukset ja niiden liite 5) on kuvattu järjestelmien käyttö- ja luovutuslokeihin kohdistuvia vaatimuksia ja ratkaisuja. Lisäksi järjestelmäkohtaisesti järjestelmien valmistajat tai palveluntuottajat voivat tuottaa tarkempia ohjeita, ja valmisteilla on myös uusia kansallisia ohjeita ja määrittelyjä. Lokivalvontaa on tehtävä suunnitelmallisesti (seurantatoimenpiteet ja tarkastukset suunnitellaan etukäteen esimerkiksi toistuvuuden ja laajuuden suhteen). Lokivalvontaa tehdään myös asiakkaiden pyytäessä lokitietoja. Lisäksi jos epäillään tietojen epäasianmukaista käyttöä, lokivalvonnan kautta on voitava tehdä tarkastuksia. Kanta-palveluihin liittyvien tietojärjestelmien sertifiointivaatimuksiin kuuluu tietojen käytöstä koottavien lokien kokoamiseen ja raportointiin kuuluvia toimintoja.

Kysymys: Miten omavalvontasuunnitelmassa tulisi käsitellä sähköisen asioinnin järjestelmiä? Järjestelmästä ei tällä hetkellä siirry Kantaan tietoa, mutta se sisältää toki asiointiin liittyvää potilastietoa. Pitäisikö nämä järjestelmät mainita organisaatioiden omavalvontasuunnitelmassa erikseen tietosuoja / tietoturvanäkökulmasta? Vai riittääkö, että vaadimme järjestelmätoimittajalta dokumentit ko. asioista?
Vastaus: Sähköisen asioinnin palvelut, joita tässä kuvataan kuuluvat asiakastietolain mukaisesti luokan B tietojärjestelmiin, jos niistä ei siirretä tietoja Kanta-palveluihin tai ne eivät hae tietoja Kanta-palveluista. Omavalvontasuunnitelmassa nämä järjestelmät tulee myös olla kuvattuna, suunnitelmahan ei koske pelkästään Kanta-palveluihin liittyviä järjestelmiä. Omavalvontasuunnitelman mallipohjassa tämän tyyppisiä järjestelmiä koskevia asioita on esimerkiksi luvuissa 7 ja 8.2. Osassa kuvattavista asioista voidaan nojautua myös järjestelmätoimittajan dokumentaatioon.

Kysymys: Tietojärjestelmätoimittajan asiakkaat laativat omat omavalvontasuunnitelmansa, joita tarkennetaan esimerkiksi Kanta-palveluihin liittymisen yhteydessä. Missä laajuudessa järjestelmätoimittajan on toimitettava kuvauksia yms. asiakkaidensa omavalvontasuunnitelmiin? Riittäisikö esim. seuraava:

- Yleisluontoinen tietoturvapolitiikka
- Sopimuksien esim. yleisissä käyttöehdoissa kirjaukset tietoturvavastuista, joihin asiakas voi omavalvontasuunnitelmassaan viitata
- Eli asiakas tekee viittaukset yhteisiin sopimuksiin, joista voidaan todentaa esim. vastuujako mm. palvelinympäristön tietoturvasta

- Asiakas voi viitata omavalvontasuunnitelmassaan järjestelmätoimittajan dokumentaatioon
    - Emme toimita tarkkoja kuvauksia toimintamalleista tai esim. tietoturvaratkaisuista tai esim. välittäjänä toimivan toimittajan välittäjätoimintaan kohdistuvasta omavalvontasuunnitelmasta.

Vastaus: Lain mukaan "Valmistajan on annettava tietojärjestelmän yhteydessä järjestelmän käyttäjälle yhteentoimivuuden, tietoturvallisuuden ja tietosuojan sekä toiminnallisuuden kannalta tarpeelliset tiedot ja ohjeet järjestelmän käyttöönotosta, tuotantokäytöstä ja ylläpidosta." (AsTL 19 c §). Sopimuksiin kirjautut vastuut ovat erityisen tärkeä seikka omavalvonnan kannalta. Koska omavalvonnan kokonaisvastuu on sote-palvelujen tuottajilla, tulisi ainakin sellaiset omavalvontaseikat joista on sovittu järjestelmätoimittajan vastaavan asiakkaan puolesta toimittaa riittävän tarkasti kuvattuna asiakkaille. Vaatimuksena on, että omavalvonnan vaatimusten toteutuminen on pystyttävä todentamaan esimerkiksi sote-palvelunantajaan kohdistuvan tarkastuksen yhteydessä. Omavalvonnan tarkastusoikeus ja todentamisvastuu ulottuu myös sote-palveluntuottajan tietojärjestelmätoimittajiin, eli riittävän tarkkojen kuvausten toimittaminen (vaatimus todennettavissa kuvauksen perusteella) tai todentamisen järjestäminen tarvittaessa (esim. osana sopimusta) ovat tässä asiassa perusvaihtoehtoja.
Omavalvontasuunnitelman määräyksen ja mallipohjan Tietojärjestelmät-kohdissa mainitut asiat kuvaavat yleisen vähimmäisvaatimustason eri järjestelmistä, mutta sopimuksista ja järjestelmän kriittisyydestä riippuen voi olla tarpeen kuvata muutakin.
Tietojärjestelmän valmistajalta ei edellytetä erillistä omaa omavalvontasuunnitelmaa, ellei tämä toimi myös välittäjäroolissa (esimerkiksi tarjoa kokonaispalvelua siten että järjestelmätoimittaja myös hoitaa ylläpito- ja virhetilanneselvitystehtäviä niin että sen henkilöstöllä on pääsy salassa pidettäviin asiakas- ja potilastietoihin).
Dokumentaation julkisuus on eri asia kuin sen toimittaminen asiakkaille. Dokumentaatiota voi toimittaa myös siten, että sen luottamuksellisena säilymisestä on sovittu.

3.5 Omavalvonnan toteuttaminen

Kysymys: Mitkä ovat organisaation johdon kannalta tärkeimpiä syitä varmistaa omavalvonnan toimivuus?
Vastaus: Omavalvontasuunnitelman ja omavalvonnan toteuttamisen kautta:

- varaudutaan oman toiminnan kannalta keskeisiin tietoturvallisuus- ja tietosuojariskeihin, jotka toteutuessaan voivat pahimmillaan vaarantaa koko organisaation toiminnan
- lisätään asiakkaiden ja sidosryhmien luottamusta organisaation menettelytapoihin
- parannetaan henkilöstön työhyvinvointia sekä oikeusturvaa
- parannetaan asiakastietojen tietoturvallisuutta ja kykyä toimia suunnitelmallisesti, kun asiakkaat käyttävät lakisääteisiä tiedonsaanti- ja tarkastusoikeuksiaan
- täytetään organisaation vastaavan johtajan lakisääteistä velvoitetta tietosuojan ja tietoturvallisuuden omavalvonnan järjestämisestä
- täyttetään vaatimuksia tietoturvallisuuden ja tietosuojan toteuttamisen todennettavuudesta esimerkiksi viranomaistarkastusten yhteydessä
- luodaan tilintekokyvykkyyttä ja kykyä vastata myös tuleviin säädösvaatimuksiin täyttäen esimerkiksi monia EU:n tietosuoja-asetuksen tavoitteita.

Kysymys: Millä tavalla omavalvonnan toteuttamisesta tai itseauditoinneista syntyvä materiaali on dokumentoitava?
Vastaus: Säädösten mukaan omavalvonnan toteuttaminen suunnitelman mukaisesti on dokumentoitava. Dokumentointiin ei kohdisteta yksityiskohtaisia vaatimuksia säädösten kautta. Dokumentointitapa on järkevää kuvata osana suunnitelmaa. Dokumentointi helpottaa parannustoimenpiteiden suunnittelua ja mahdollistaa tarvittaessa tarkastuksessa edellytettävän toteuttamisen todentamisen.
Omavalvontasuunnitelman pohjalta voidaan toteuttaa itseauditointi tai myös ulkoinen auditointi, jonka tulokset kootaan auditointiraporttiin. Tämä ei kuitenkaan ole ainoa tapa dokumentoida omavalvontaa, vaan

myös suunnitelman eri osien ja kuvausten päivitykset ja eri osiin liittyvät tarkemmat kuvaukset (esimerkiksi koulutuspäiväkirjat, toimintakertomukset, tietotilinpäätösten osat) voivat toimia dokumentoinnissa.

Kysymys: Millä tavalla omavalvonnan toteuttamisessa syntynyt materiaali on säilytettävä tai arkistoitava?
Vastaus: Omavalvonnan toteuttamisessa syntyneen materiaalin säilyttämiseen ei ole yksityiskohtaisia säädösperusteisia ohjeita. Materiaalin säilyttäminen voidaan suunnitella esimerkiksi oman laatukäsikirjan tai tiedonohjaussuunnitelman mukaisesti. Tyypillinen suositus on säilyttää esimerkiksi ”rutiinimateriaalia” 5 vuotta tai tarkastuksen tai väärinkäytösepäilyjen yhteydessä syntynyttä materiaalia 12 vuotta.

4 Sote-tietojärjestelmien luokittelu: kysymykset ja vastaukset

Tässä osiossa käsitellään kysymyksiä, jotka liittyvät asiakastietolaissa määriteltyjen sosiaali- ja terveydenhuollon tietojärjestelmien luokkien A ja B määräytymiseen.

4.1 Vastuu luokittelusta ja luokitteluperusteet

Kysymys: Kuka luokittelun tekee?
Vastaus: Lain mukaan valmistaja on vastuussa sosiaali- ja terveydenhuollon tietojärjestelmän luokittelusta. Valmistajan lukuun luokittelun voi tehdä myös tietojärjestelmäpalvelun tuottaja, joka myy esimerkiksi ulkomaista tietojärjestelmätuotetta tai tarjoaa siihen tukipalveluja.

Kysymys: Mitkä järjestelmät kuuluvat Valviralle ilmoitettaviin A- tai B-luokan tietojärjestelmiin? Koskeeko ilmoittamisvelvollisuus sekä A-luokan että B-luokan järjestelmiä?
Vastaus: Asiakastietolain mukaisesti tietojärjestelmät, joiden käyttötarkoitus (tai yksi käyttötarkoituksista) on sosiaalihuollon asiakastietojen tai terveydenhuollon potilastietojen käsittely, on ilmoitettava Valviralle. Nämä tiedot ovat sivullisilta salassa pidettäviä. Yleisiä toimisto-ohjelmistoja tai vastaavia yleiskäyttöisiä ohjelmistoja ei ilmoiteta rekistereihin. Ilmoituksen menettelytapoja kuvataan tarkemmin THL:n määräyksessä 2/2016 sekä Valviran Tietojärjestelmät-sivulla:
https://www.thl.fi/fi/web/tiedonhallinta-sosiaali-ja-terveysalalla/tiedon-ja-vaatimusten-yhdenmukaistaminen/julkaisut/maaraykset
http://www.valvira.fi/terveydenhuolto/terveysteknologia/tuotteen_markkinoille_saattaminen/tietojarjestelmat

Kysymys: Mitkä järjestelmät kuuluvat A-luokan tietojärjestelmiin, joilta edellytetään Kanta-yhteistestausta, tietoturva-auditointia sekä vaatimustenmukaisuustodistusta ja joiden tiedot ja vaatimustenmukaisuustodistus on toimitettava Valviralle?
Vastaus: A-luokkaan kuuluvat järjestelmät, jotka liittyvät suoraan tai välityspalvelun kautta Kanta-palveluihin tai tuottavat asiakirjoja, jotka välitetään Kanta-palveluihin. A-luokkaan kuuluvat myös välityspalvelut joiden kautta järjestelmät liittyvät Kanta-palveluihin silloin, kun niiden tuottajalla on mahdollisuus päästä käsiksi asiakas- ja potilasasiakirjojen sisältöihin.

Kysymys: Mistä voi tarkistaa, mitkä järjestelmät kuuluvat luokkaan A?
Vastaus: Sekä A- että B-luokkaan kuuluvat käyttöönotettavat järjestelmät tai niiden uudet versiot on ilmoitettava Valviran rekisteriin. Rekisteri tulee Valviran sivuille verkkoon saataville viimeistään vuoden 2017 alussa. Rekisteri sisältää tiedot A-luokkaan kuuluvista järjestelmistä, joiden on läpäistävä sertifiointiprosessi. Tietojärjestelmien valmistajien ja tietojärjestelmäpalvelujen tuottajien on luokiteltava omat järjestelmänsä ja kunkin järjestelmän osalta on pystyttävä ottamaan kantaa siihen mihin luokkaan se kuuluu. Myös Kelan sivuilta löytyy tietoa sertifioiduista A-luokan tietojärjestelmistä, kunnes Valviran rekisteri on käytettävissä:
http://www.valvira.fi/terveydenhuolto/terveysteknologia/tuotteen_markkinoille_saattaminen/tietojarjestelmat
http://www.kanta.fi/web/ammattilaisille/sertifioidut-jarjestelmat-ja-valittajat

4.2 Esimerkkejä järjestelmien luokittelusta

Kysymys: Millaisia esimerkkejä järjestelmien luokittelusta on saatavilla?
Vastaus: Esimerkkejä järjestelmien luokittelusta:
Luokka A:

- Potilastietojärjestelmätuote (esim. sähköinen potilaskertomusjärjestelmä), joka toimittaa tietoja Kanta-palveluihin) tai hakee tietoja Kanta-palvelusta
- Apteekin tietojärjestelmä, joka on liitetty Kanta-palveluihin
- Tietojärjestelmä, jolla tehdään Kanta-palveluhin välitettäviä sähköisiä lääkemääräyksiä tai sähköisiä potilasasiakirjoja tai joka hyödyntää niitä Kanta-palvelusta tai välityspalvelun kautta
- Potilastietojärjestelmä, joka tuottaa Kanta-palveluihin välitettävän potilasasiakirjan CDA-muodossa ja välittää sen toisen potilastietojärjestelmän tai välityspalvelun kautta Kanta-palveluihin
- Tietojärjestelmä, joka hakee tietoja Kanta-palveluista mutta ei lähetä sinne uusia dokumentteja
- Tekninen Kanta-välityspalvelu, jota hyödynnetään Kanta-liityntäpisteen toteuttamisessa toisen järjestelmän liittämiseksi Kanta-palveluihin
- Erillisenä hankittava tai myytävä tietojärjestelmäpalvelu, joka välittää muilta järjestelmiltä tietoa Kanta-palveluihin tai välittää muille järjestelmille tietoja Kanta-palveluista (huom. ks. myös myöhemmät kysymykset näiden järjestelmien luokittelusta)
- Järjestelmä, jota markkinoidaan Kanta-palveluihin liittyvänä järjestelmänä
- Järjestelmä, jota markkinoidaan Kanta-palvelujen käyttötapauksissa kuvatuilla toiminnallisuuksilla, jotka toteutuvat Kanta-palveluihin liittymisen kautta (myös siinä tapauksessa, että tekninen liittyminen toteutetaan ulkoista tietojärjestelmäpalvelua, teknistä Kanta-välityspalvelua tai toisen toimittajan tuotetta käyttäen)
- Erikseen hankittava palvelu tai komponentti, jonka avulla voidaan toteuttaa muiden järjestelmien liittäminen Kanta-palveluihin ja olennaisten tietoturvallisuusvaatimusten täyttäminen kokonaan tai osittain

Luokka B

- Sosiaalihuollon asiakastietojärjestelmä, joka ei välitä tietoja Kanta-palveluihin
- Terveydenhuollon potilastietojärjestelmä, joka ei vielä ole liittynyt Kanta-palveluihin mutta tulee liittymään niihin tulevaisuudessa (jolloin siirtyy luokkaan A)
- Sähköisen asioinnin palvelu tai asiointijärjestelmä, jossa käsitellään asiakas- tai potilastietoja, mutta joka ei liity Kanta-palveluihin
- Terveydenhuollon potilastietojärjestelmä tai sosiaalihuollon asiakastietojärjestelmä, jota ei myydä tai markkinoida Kanta-palveluihin liittyvänä järjestelmänä, ja joka tuottaa yksittäisiä tietoelementtejä, joista toinen tietojärjestelmä tai palvelu koostaa asiakirjoja, jotka välitetään toisen tietojärjestelmän kautta Kanta-palveluihin
- Järjestelmä, joka hyödyntää erillistä tietojärjestelmäpalvelua tai ohjelmistoa Kanta-liittymään ja jonka osalta liittymäpalvelun kautta hoidetaan kaikkien A-luokan järjestelmien olennaisten vaatimusten toteuttaminen ja todentaminen, ja jota ei myydä tai markkinoida Kanta-palveluihin liittyvänä tai sellaisilla toiminnallisuuksilla, jotka toteutuvat Kanta-palveluihin liittymisen kautta.

Ei luokittelua eikä ilmoituksia (tietoturvasta kuitenkin huolehduttava säädösten mukaisesti):

- Yleiset tekstinkäsittely- tai toimisto-ohjelmat, joita käytetään myös asiakas- ja potilastietojen kirjaamiseen.
- Suojatussa ympäristössä toimiva sairaalan tai muun palveluntuottajan hallinnollinen tukijärjestelmä, jonka keskeisenä käyttötarkoituksena ei ole asiakas- tai potilastietojen käsittely, vaikka se saattaa sisältää joitakin asiakastietoja, esimerkkejä: ateriatilausjärjestelmä, materiaalihallinnon järjestelmä tai käyttövaltuuksien hallintajärjestelmä, jonka kautta ei käsitellä salassa pidettäviä asiakas- tai potilastietoja ja jonka nimenomainen käyttötarkoitus ei ole asiakas- tai potilastietojen käsittely.
- Asiakas- tai kuntalaskutusjärjestelmä, jonka käyttötarkoituksena ei ole salassa pidettävien asiakas- tai potilastietojen käsittely.
- Yleiset tietokanta-, sovelluspalvelin-, integrointialusta- tai muut infrastruktuurituotteet, elleivät ne toimi itsenäisesti teknisenä Kanta-välityspalveluna.
- Viestintään käytetyt järjestelmät tai sovellukset, joiden käyttötarkoituksiin ei kuulu asiakas- tai potilastietojen hallinta tai käsittely.
- Tietojärjestelmä tai tietojärjestelmäpalvelu, joka käsittelee anonymisoitua tai ei-tunnisteellista tai väestötason yhteenvetoina käsiteltävää asiakas- tai potilastietoa, esimerkiksi päätöksentukipalvelu, potilasryhmittelypalvelu tai johtamisen tai raportoinnin järjestelmä, joka ei sisällä asiakkaiden yksilöintitietoja. Mikäli järjestelmän käyttötarkoituksena kuitenkin on asiakas- tai potilastietojen käsittely ja tiedoista on tunnistettavissa yksittäinen asiakas, järjestelmä kuuluu luokkaan B. Lääketieteellisen päätöksentuen palveluissa on huomioitava myös lääkintälaitesäädösten vaatimukset ohjelmistoista (nämä vaatimukset ja luokittelut eivät suoraan vastaa asiakastietolain luokittelua A- ja B-luokan järjestelmiin).
- Yleinen asianhallintajärjestelmä, jota valmistaja ei ole erityisesti suunnitellut sosiaali- tai terveydenhuollon asiakas- tai potilasasiakirjojen ja niissä olevien tietojen käsittelyyn, ja joka ei sisällä ominaisuuksia joilla se olisi yhteydessä valtakunnallisiin sote-tietojärjestelmäpalveluihin.
- Haitta- tai vaaratapahtumien raportointiin ja käsittelyyn käytettävä järjestelmä, joka ei sisällä tunnisteellista asiakas- tai potilastietoa.
- Kehitteillä olevaan Omakanta Omatietovarantoon liittyvä palvelu tai järjestelmä, joka ei liity muihin Kanta-palveluihin (näiden palvelujen luokittelua ja vaatimuksia tarkennetaan tulevissa säädöksissä).

4.3 Luokittelu järjestelmäkokonaisuuksissa, joissa Kanta-yhteydet hoidetaan tietyn palvelun tai komponentin kautta

Kysymys: Miten luokitellaan järjestelmäkokonaisuus, jossa Kanta-yhteydet hoidetaan tietyn palvelun tai komponentin kautta?
Vastaus: Luokitteluun vaikuttavat ainakin seuraavat seikat:

- järjestelmän, osajärjestelmän tai tietojärjestelmäpalvelun käyttötarkoitus
- olennaisten vaatimusten sisältö
- järjestelmän, osajärjestelmän tai tietojärjestelmäpalvelun ”myyntinimi” tai tuotenimi sekä se, onko osa myynnissä ja markkinoinnissa ilmaistuja toiminnallisuuksia Kanta-palvelujen kautta toteutuvia
- järjestelmän eri komponenttien välinen työnjako
- käyttöympäristön suojaustasovaatimukset.

Lain mukaan vaatimusten on täytyttävä käytettäessä tietojärjestelmää sekä itsenäisesti että yhdessä muiden siihen liitettäväksi tarkoitettujen tietojärjestelmien kanssa.

Järjestelmät tai tietojärjestelmäpalvelut, joita voi ostaa, hankkia tai koota asiakas- tai potilastietojen käsittelyä varten on luokiteltava siten, että järjestelmän käyttäjät tai niiden hankintaa harkitsevat voivat tarkistaa myös Valviralle ilmoitettuja tietoja vasten mihin luokkaan järjestelmä (järjestelmän nimi- ja versiotietojen perusteella) kuuluu tai käyttää eri luokkiin kuuluvien olennaisten vaatimusten määrittelyjä hyväkseen vaatimusmäärittelyissä ja hankinnoissa. Mikäli järjestelmän markkinointimateriaalissa tai dokumentaatiossa kuvataan sen liittyvän Kanta-palveluihin, on sellaiset vaatimukset joita luokan A järjestelmälle asetetaan pystyttävä todentamaan.

Jos järjestelmä toteuttaa Kanta-palvelujen määrittelyissä (esimerkiksi käyttötapaukset, toiminnalliset määrittelyt tai rajapintamäärittelyt) kuvattuja toiminnallisuuksia, se kuuluu luokkaan A, ellei jostain erityisestä syystä muuta johdu. Näiden määrittelyjen mukaiset toiminnallisuudet ovat luokkaan A kuuluvien tietojärjestelmien olennaisia toiminnallisia vaatimuksia.

Esimerkiksi laaja ”yhtenä tuotteena myytävä” potilastietojärjestelmäkokonaisuus, joka hoitaa Kanta-liittymisen tietyn erillisen palvelun kautta kuuluu luokkaan A, mikäli Kanta-yhteys ja Kanta-palvelujen kautta saatavat tai niihin välitettävät tiedot ovat keskeinen osa sen toimintaa. Tämä ei estä Kanta-liittymiseen käytetyn osan myyntiä myös omana tuotteenaan (ja tarvittaessa myös sen ilmoittamista erikseen). Osasto- tai alayksikkökohtaisissa erillisjärjestelmissä pätevät samat perussäännöt. Mikäli järjestelmä ”tuottaa Kanta-asiakirjoja” tai toteuttaa Kanta-käyttötapauksia, se kuuluu luokkaan A. Mikäli järjestelmä vain hyödyntää muiden järjestelmien tai palvelujen kautta Kanta-palveluista saatavia tietoja tai tuottaa asiakas- ja potilastietoja joista jokin muu järjestelmä koostaa esimerkiksi Kanta-palveluihin lähetettävät asiakirjat vastaten muidenkin A-luokan vaatimusten täyttymisestä, se voidaan luokitella luokkaan B.

Mikäli käytössä on palvelu tai komponentti, joka on aiemmin läpäissyt auditoinnin ja yhteistestauksen tietyn toisen sitä hyödyntävän järjestelmän kanssa, on testauksessa tai auditoinnissa mahdollista jättää todentamatta uudelleen ne vaatimukset, jotka on jo hyväksytysti testattu ja auditoitu aiemmin ja jotka toimivat täysin vastaavalla tavalla myös uuden testattavan järjestelmän kanssa. Tämä voi myös alentaa testauksen ja auditoinnin kustannuksia.

Tietojärjestelmän valmistaja vastaa järjestelmän luokittelusta ja suunnittelusta sekä lain edellyttämistä selvityksistä ja ilmoituksista.

4.4 Järjestelmän siirtyminen luokasta toiseen tai luokittelu useisiin luokkiin

Kysymys: Voiko järjestelmä tai sen uusi versio siirtyä luokasta toiseen?
Vastaus: Kyllä voi, esimerkiksi sellaisen version käyttöönoton yhteydessä jonka myötä myös järjestelmä voidaan liittää Kanta-palveluihin. Tämä edellyttää kunkin luokan vaatimusten mukaista ilmoitusta jossa myös ilmaistaan luokasta toiseen siirtyminen ja perustelut tai kuvaus siitä, mitkä järjestelmän ominaisuudet ovat muuttuneet siten että siirtyminen on tarpeen.

Kysymys: Voiko järjestelmän yksi versio olla sekä luokassa A että luokassa B?
Vastaus: Kyllä voi, mikäli järjestelmää voidaan käyttää sekä Kantaan liittyvänä että ilman Kanta-liityntää. Tällöin on kuitenkin suositeltavaa, että järjestelmä sertifioidaan ja rekisteröidään A-luokkaan. Mikäli järjestelmää käytetään ilman ”ilman Kanta-liityntää” tai se on konfiguroitavissa tällaiseen käyttöön, on järjestelmä mahdollista ilmoittaa myös selkeästi molempiin luokkiin ja nimetä ilmoituksessa selkeästi fraasein ”(ilman Kanta-liityntää)” tai ”(sisältäen Kanta-liitynnän)”.

5 Tietojärjestelmiä koskevat olennaiset vaatimukset: yleiset kysymykset ja suhde laatujärjestelmän, välityspalvelun ja omavalvonnan vaatimuksiin

Kysymys: Mitkä olennaiset vaatimukset koskevat A-luokan ja B-luokan järjestelmiä?
Vastaus: Asiakastietlain nojalla on määritelty, että sekä A- että B-luokan järjestelmiä koskevat olennaiset toiminnalliset vaatimukset (ks. luku 6.1). Asiakastietolain nojalla on myös määritelty kansalliset tietoturvallisuuden auditointivaatimukset A-luokan tietojärjestelmille, jotka liittyvät Kanta-palveluihin. Osa tietoturvavaatimuksista on sellaisia, joihin on syytä kiinnittää huomiota myös B-luokan järjestelmissä, vaikka näissä järjestelmissä ei edellytetäkään ulkoista tietoturvallisuuden auditointia. Kanta-palveluihin liittyvien A-luokan järjestelmien on myös täytettävä yhteentoimivuuden vaatimukset, jotka todennetaan Kanta-palvelujen kanssa suoritettavan yhteistestauksen kautta. Tiedonhallinnan muut velvoitteet ja yleiset säädökset asiakas- ja potilastietojen käsittelyssä koskevat sekä A- että B-luokan järjestelmiä.

Kysymys: Kuka päättää mikä on tietojärjestelmän olennainen muutos?
Vastaus: Valmistaja vastaa aina vaatimustenmukaisuudesta ja sen arvioinnista, onko järjestelmään tehty esimerkiksi versiopäivityksen yhteydessä olennaisia muutoksia. Sertifiointiprosessin mukaisesti A-luokan järjestelmän muutosilmoitus toimitetaan Kelalle ja arviointilaitokselle, jotka arvioivat onko kyseessä olennainen muutos, joka edellyttää uudelleen sertifiointia. Uusien kansallisten määrittelyjen versioiden yhteydessä voi olla tieto siitä, aiheuttaako määrittely esimerkiksi aiemman version perusteella toteutettuun järjestelmään uudelleentestaus- tai tietoturvallisuuden uudelleenarviointitarpeen.

Kysymys: Mikä on tietojärjestelmiin kohdistuvien olennaisten vaatimusten suhde sote-palveluntuottajien omavalvontasuunnitelmaan?
Vastaus: Sekä A- että B-luokan tietojärjestelmien huomiointi on tarpeen sote-palveluntuottajan omavalvontasuunnitelmassa tietoturvallisuuteen ja tietosuojaan liittyen. Osana omavalvontaa tulee varmistaa, että käytettävät A- ja B-luokan tietojärjestelmät on ilmoitettu asianmukaisin tiedoin Valviran rekisteriin tietojärjestelmistä ja että A-luokkaan kuuluvien järjestelmien vaatimustenmukaisuustodistus on voimassa ja ajan tasalla. Sote-palveluntuottajan omavalvontasuunnitelmassa on syytä pitää järjestelmittäin kirjaa käytettävien järjestelmien vaatimustenmukaisuustodistuksen tai hyväksyttyjen testausten voimassaolosta (A-luokan järjestelmissä) ja siitä, että tuotantokäytössä olevat järjestelmät on asianmukaisesti ilmoitettu Valviran rekisteriin. Tietoja voi selvittää Valviran rekisterin, Kanta-sivujen sekä valmistajien tai tietojärjestelmäpalvelujen tuottajien kautta.

Kysymys: Asiakastietolain pykälä 19c edellyttää, että tietojärjestelmän valmistajalla on oltava laatujärjestelmä, jota sovelletaan tietojärjestelmän suunnitteluun ja valmistukseen. Laki ei kuitenkaan tarkemmin määrittele minkälainen ko. laatujärjestelmän pitää olla. Yleisesti terveydenhuollon laitteiden suunnittelun ja valmistuksen laatujärjestelmille sovelletaan standardia ISO 13485. Se on kuitenkin varsin raskas, eikä nyt kyseenä olevassa tapauksessa olisi muuten välttämätön. Mitä elementtejä asiakastietolain mukaisen laatujärjestelmän tulee vähintään sisältää?
Vastaus: Laatujärjestelmän sisältö on sovitettava laitteen tai tietojärjestelmän käyttötarkoituksen ja kriittisyyden mukaisesti. Kaikkia laitteille tarkoitettuja laatujärjestelmän ominaisuuksia ei edellytetä kaikilta ohjelmistoilta. Kattavia valtakunnallisia ohjeita eri käyttötarkoituksiin tai A- ja B-luokkiin kuuluvien tietojärjestelmien laatujärjestelmälle ei ole toistaiseksi määritelty. Laatujärjestelmän kehittämisessä on huomioitava myös lääkintälaitedirektiivin ja sen pohjalta annettujen säädösten velvoitteet, jos järjestelmä luokitellaan lääkintälaitteeksi.

Kysymys: Milloin sote-palvelujen tuottajaa koskevat palveluntuottajia koskevan omavalvontasuunnitelman lisäksi myös Kanta-välityspalvelujen sertifioinnin tietoturva-auditoinnin vaatimukset tai Kanta-välittäjää koskevat omavalvonta vaatimukset?
Vastaus: Mikäli sote-palveluntuottaja vastaa myös teknisen Kanta-välityspalvelun toteuttamisesta, sitä koskevat myös välityspalvelun sertifiointivaatimukset. Jos sote-palvelujen tuottaja vastaa Kanta-liityntäpisteen toiminnasta ja hallinnoinnista, sen omavalvontasuunnitelmassa on huomioitava myös välittäjätoimintaan liittyvät (esimerkiksi käyttöympäristöön liittyvät) vaatimukset. Kanta-välityspalvelujen sertifiointia sekä liityntäpisteissä toimivien ulkoisten välittäjien sertifioinnin ja omavalvonnan toimintatapoja on tarkennettu ohjeessa 3/2015, joka löytyy osoitteesta:
https://www.thl.fi/fi/web/tiedonhallinta-sosiaali-ja-terveysalalla/tiedon-ja-vaatimusten-yhdenmukaistaminen/julkaisut/ohjeet

Kysymys: Milloin järjestelmätoimittajaa (valmistaja tai tietojärjestelmäpalvelun tuottaja) koskevat järjestelmän sertifioinnin lisäksi myös omavalvontasuunnitelmaan liittyvät vaatimukset?
Vastaus: Järjestelmätoimittaja voi tuottaa järjestelmän lisäksi teknistä **Kanta-välityspalvelua**. Jos tämä palvelu on käytettävissä erikseen järjestelmästä, sen itsenäinen käyttö edellyttää erillistä vaatimustenmukaisuustodistusta. Teknisen Kanta-välityspalvelun toteuttajalta ei edellytetä automaattisesti omavalvontasuunnitelmaa, ellei tämä toimi myös välittäjänä.
Mikäli tietojärjestelmäpalvelua tarjoava taho toimii myös **välittäjänä**, jonka henkilöstöllä on mahdollisuus päästä käsittelemään salaamattomia asiakas- ja potilastietoja, on omavalvonnassa huomioitava myös Kanta-välityspalveluihin kohdistuvat vaatimukset. Välittäjiltä edellytetään omavalvontasuunnitelmaa, ja välittäjien, jotka eivät ole sote-organisaatiorekisterissä olevia sote-palveluntuottajia, on hakeuduttava välittäjärekisteriin sote-palveluntuottajan valtuutuksella. Lisätietoja ja tarkempia kriteerejä löytyy edellisen kysymyksen linkin kautta.

Jos Kanta-palveluihin liittyvää järjestelmää **tarjotaan palveluna** (esim. nk. palveluvälittäjätoiminta) sillä tavoin, että järjestelmän käyttöympäristö on tietojärjestelmäpalvelun tuottajan vastuulla ja tietojärjestelmäpalvelun tuottajan henkilöstöllä on pääsy käyttöympäristön asiakas- tai potilastietoihin, on tietojärjestelmäpalvelun tuottajan pystyttävä selkeästi osoittamaan, mikä taho vastaa omavalvontaan ja käyttöympäristöön liittyvien vaatimusten toteuttamisesta ja tarvittaessa todentamisesta. Palveluvälittäjän on tehtävä omavalvontasuunnitelma, ja suunnitelman eri kohtien vastuut ovat myös sopimuksin määriteltävissä.

Kysymys: Milloin konesalipalvelun tuottajaa koskevat välityspalvelun sertifiointivaatimukset ja tietoturva-auditointi?
Vastaus: Mikäli konesalipalveluja tuottavan tahon henkilöstö voi päästä käsiksi salaamattomiin asiakas- ja potilastietoihin, on omavalvonnassa ja sertifioinnissa huomioitava myös Kanta-välityspalveluihin sekä järjestelmien käyttöympäristöön kohdistuvat vaatimukset. Kaikki relevantit välityspalvelun omavalvontavaatimukset on täytyttävä joko a) sote-palveluntuottajan omavalvonnan, b) välittäjän omavalvonnan, c) teknisen välityspalvelun toteuttajan sertifioituun tuotteeseen liittyvän toiminnan, tai d) tietojärjestelmäpalvelun tuottajan tai valmistajan sertifioituun tuotteeseen liittyvän toiminnan kautta. Osana tätä ketjua on kuvattava, miten on varmistettu että konesalipalvelujen tuottaja ei pääse käsiksi salaamattomiin potilas- tai asiakastietoihin tai miten muulla tavoin tähän liittyvät vaatimukset täytetään. Vaatimusten todentaminen ja mahdollinen tietoturva-auditointi konesalipalvelujen osalta koskee niitä vaatimuksia, jotka ovat konesalipalvelun kannalta olennaisia kuten ylläpitohenkilöstöön ja käyttöympäristöön kohdistuvat vaatimukset.

Kysymys: Voiko teknistä Kanta-välityspalvelua käyttää myös muihin tarkoituksiin kuin Kanta-liityntäpisteen toteuttamiseen?
Vastaus: Kyllä voi. Palvelun käyttötarkoitus voi kattaa muutakin kuin Kanta-välityksen. Välityspalvelut rakennetaan usein yleiskäyttöisille alustoille joita voi hyödyntää muuhunkin kuin Kanta-liityntöihin. Samantyyppisiä asiakas- ja potilastietojen tietoturvallisuusvaatimuksia kohdistuu myös muuhun käyttöön,

mutta esimerkiksi alueellisen käytön mahdolliset erityispiirteet eivät ole välityspalvelun tietoturva-auditoinnin kohteena. Välityspalvelun tai järjestelmän muut kuin sertifiointiin liittyvät käyttökohteet tai -tarkoitukset eivät saa vaarantaa sertifioidun ratkaisun turvallisuutta. Jos tällaista riskiä havaitaan esimerkiksi sertifioidun välityspalvelun merkittävien muutosten yhteydessä, pitää arvioida palvelun uudelleenauditointitarve.

6 Sote-tietojärjestelmien olennaiset toiminnalliset vaatimukset

6.1 Selvitys toiminnallisten vaatimusten täyttymisestä ja B-luokan olennaiset vaatimukset

Kysymys; Mitä järjestelmiä ja valmistajia toiminnallisten vaatimusten määräys (THL määräys 2/2016) koskee? Koskeeko määräys myös B-luokan järjestelmiä?
Vastaus: Määräys koskee:
- Kanta-palveluihin liittyviä järjestelmiä ja Kanta-välityspalveluita, jotka kuuluvat käyttötarkoituksensa ja ominaisuuksiensa perusteella asiakastietolain mukaiseen luokkaan A, sekä muita Kanta-palveluihin liittyviä tietojärjestelmäpalveluita
- muita sosiaali- ja terveydenhuollon järjestelmiä, joiden käyttötarkoituksena on asiakas- ja potilastietojen käsittely, eli asiakastietolain mukaiseen luokkaan B kuuluvia järjestelmiä.

Kysymys: Onko Valviralle tehtävä ilmoitus tietojärjestelmästä (erityisesti luokkaan B kuuluva, asiakas- ja potilastietojen käsittelyyn tarkoitettu järjestelmä, joka ei liity Kanta-palveluun) sama asia kuin asiakastietolain edellyttämä selvitys olennaisten toiminnallisten vaatimusten täyttämisestä?
Vastaus: Järjestelmien ilmoitusvelvollisuus koskee tuotantokäyttöön otettavia A- ja B-luokkaan kuuluvia tietojärjestelmiä. Selvitys olennaisten toiminnallisten vaatimusten täyttämisestä koskee B-luokan järjestelmien osalta 1.1.2017 alkaen käyttöönotettavia järjestelmiä tai uusia versioita järjestelmistä. Kyseessä on eri asia, mutta molempien velvoitteiden täyttäminen samalla järjestelmälomakkeella ja samalla ilmoituksella Valviraan on suositeltavaa ja järkevää. Valviraan tehtävä ilmoitus edellyttää sekä Valviran ilmoituslomakkeen että määräyksen 2/2016 mukaisen järjestelmälomakkeen toimittamista.

Kysymys: Mitä olennaisten vaatimusten täyttäminen B-luokan järjestelmissä edellyttää?
Vastaus: B-luokan järjestelmissä on a) kuvattava järjestelmän käyttötarkoitus ja toiminnallisten vaatimusten täyttäminen asiakastietolain ja THL:n määräyksen 2/2016 mukaisesti, b) tarkistettava, mitkä valtakunnalliset olennaisten vaatimusten vähimmäisvaatimukset (kuten toiminnallisten vaatimusten profiilit) järjestelmää koskevat, c) ilmoitettava järjestelmä Valviran rekisteriin sosiaali- ja terveydenhuollon tietojärjestelmistä säädösten mukaisesti.

Kysymys: Miksi B-luokan järjestelmiä koskevat vain yllä kuvatut vaatimukset, ja mitä se tarkemmin kuvattuna tarkoittaa?
Vastaus: Luokkaan B kuuluu hyvin suuri joukko eri käyttötarkoituksiin käytettäviä järjestelmiä, ja niiden tarkempi käyttötarkoitus ohjaa sitä, millaisia vaatimuksia järjestelmille on asetettava. Yhtä yhtenäistä vaatimusmäärittelyä kaikkien erilaisten B-luokkaan kuuluvien järjestelmien vähimmäisvaatimuksiksi ei ole koottu kansallisesti. B-luokan järjestelmiltä ei edellytetä Kanta-palveluihin liittyvää sertifiointia, ulkoista tietoturva-auditointia tai siitä saatavaa vaatimustenmukaisuustodistusta. B-luokan järjestelmän tietojärjestelmäpalvelun tuottajan on ilmoitettava järjestelmä Valviran rekisteriin ennen tuotantokäyttöönottoa tai viimeistään 1.1.2017 mennessä. Ilmoituksen yhteydessä on myös kuvattava toiminnallisten vaatimusten määräyksen (THL määräys 2/2016) mukaisesti järjestelmän käyttötarkoitus. Osana ilmoitusta ja kuvausta tehdään järjestelmän toimintojen ja tietosisältöjen erittely. Jos B-luokan järjestelmä tuottaa Kanta-palveluihin

välitettäviä tietoja tai hyödyntää Kanta-palveluista haettavia tietoja, sitä voivat koskea vähimmäisvaatimukset joita on kuvattu profiileissa ”Kanta-arkistosta haettuja tietoja hyödyntävä sovellus” ja ”Kanta-arkistoon toimitettavia tietoja tuottava sovellus”.

Kysymys: Koskeeko toiminnallisten vaatimusten määräys 2/2016 jo käytössä olevia sertifioituja järjestelmiä?
Vastaus: Kyllä koskee. Jo käytössä olevasta järjestelmästä edellytetään määräyksen mukaista järjestelmälomaketta ja ilmoitusta. Määräys ei kuitenkaan edellytä vaatimustenmukaisuustodistuksen uudistamista elleivät muut uusimisen edellytykset täyty. Toisin sanoen jos järjestelmään ei ole tehty sellaisia olennaisia muutoksia jotka edellyttävät uutta testausta tai tietoturva-auditointia, sertifiointia ei tarvitse tehdä uudelleen.

Kysymys: Koska selvitys toiminnallisten vaatimusten täyttymisestä tulee tehdä?
Vastaus: Järjestelmistä tehtävissä ilmoituksissa ja Valviran ylläpitämän rekisterin julkaisussa noudatetaan asiakastietolain mukaisia määräaikoja. Ilmoitus on tehtävä ennen järjestelmän ottamista tuotantokäyttöön tai viimeistään 31.12.2016. Myös Kanta-palveluihin jo liittyneiden järjestelmien osalta ilmoitus on tehtävä viimeistään 31.12.2016. Takaraja koskee myös niitä A-luokan tietojärjestelmiä, joille on suoritettu aiempi hyväksytty yhteistestaus ja tietoturvallisuuden auditointi ennen toiminnallisten vaatimusten määräyksen voimaantuloa.

Kysymys: Onko tuotannossa olevan B-luokan tietojärjestelmän olennaisten vaatimusten täyttämisestä toimitettava selvitys Valviralle 31.12.2016 mennessä, vaikka järjestelmään ei kohdistuisi määräyksen 2/2016 mukaisia olennaisia toiminnallisia vaatimuksia?
Vastaus: Mikäli kyseessä on sellainen B-luokan järjestelmä, johon ei kohdistu valtakunnallisten vähimmäisvaatimusprofiilien mukaisia vaatimuksia, on ilmoitus ja selvitys olennaisten vaatimusten täyttämisestä toimitettava viimeistään järjestelmän seuraavan päivitysversion yhteydessä, asiakastietolain siirtymäsäännösten perusteella. Ilmoitus on kuitenkin tehtävä joka tapauksessa ennen järjestelmän tai sen version tuotantokäyttöönottoa uudessa käyttöympäristössä tai päättyvän palvelusopimuksen uusimista tai käyttöönottoa sellaisessa käyttäjäorganisaatiossa, joka ei ole aiemmin ollut järjestelmän käyttäjä, vaikka kyseessä olisi jo toisessa ympäristössä käytetty versio. Järjestelmien käyttäjien omavalvonnan ja viranomaisvalvonnan näkökulmasta on suositeltavaa tehdä ilmoitus Valviran rekisteriin heti kun mahdollista.

Kysymys: Tarvitseeko jo sertifioidut järjestelmät sertifioida toiminnallisten vaatimusten määräyksen vuoksi uudelleen?
Vastaus: Toiminnallisten vaatimusten johdosta ei automaattisesti edellytetä uutta sertifiointia. Kanta-palveluihin liittyvät, aiemmin hyväksytyt järjestelmät on sertifioitava ennen kuin tietojärjestelmän aiempi hyväksyntä vanhenee tai kun järjestelmään tehdään olennaisia muutoksia.

Kysymys: Mikä on toiminnallisten vaatimusten vähimmäissisältö ja mitä valmistajan pitää vähimmillään tehdä toiminnallisiin vaatimuksiin liittyen?
Vastaus: Tietojärjestelmän valmistajan tai tietojärjestelmäpalvelun tuottajan tulee kuvata järjestelmän käyttötarkoitus, toiminnot ja sisällöt määräyksen mukaisella lomakkeella (järjestelmälomake) ja huolehtia omasta järjestelmätestauksestaan järjestelmän käyttötarkoituksen mukaisten toiminnallisten vaatimusten mukaisesti

- kun (luokan A tai luokan B) sote-tietojärjestelmä ilmoitetaan Valviran lakisääteiseen rekisteriin sote-tietojärjestelmistä
- kun Kanta-palveluun liittyvä (luokan A) järjestelmä ilmoitetaan Kelan yhteistestaukseen
- kun Kanta-palveluun liittyvä (luokan A) järjestelmä ilmoitetaan ulkoiseen tietoturva-auditointiin
- myös (luokan A) uudelleentestauksissa / uudelleenauditoinneissa, kun järjestelmään on tehty olennaisia muutoksia

Tietojärjestelmän valmistajan / tietojärjestelmäpalvelun tuottajan tulee ottaa kantaa, onko järjestelmällä jonkin kansallisen profiilin mukainen käyttötarkoitus ja toteuttaa profiilin mukaiset vähimmäisvaatimukset ja määrittelyt ennen tuotantokäyttöä / säädettyjen aikataulujen mukaisesti.

Kysymys: Mitä Kanta-yhteistestaukseen hakeutuminen edellyttää toiminnallisten vaatimusten osalta?
Vastaus:Kanta-yhteistestaukseen hakeutuvista A-luokkaan kuuluvista tietojärjestelmistä on Kelalle toimitettava THL:n määräyksen 2/2016 mukainen järjestelmälomake sekä testausraportti Kelan ohjeiden mukaisesti. Testausraportin lisäksi voidaan edellyttää tietojen yhdenmukaisuutta lääkerekisterin ja kansallisen koodistopalvelun kanssa sekä järjestelmän käyttäjähallinnan toteuttamista ja Valviran rooli- ja attribuuttitietojen käyttöä kansallisten vaatimusmäärittelyjen mukaisesti. Testauksesta lisätietoja ja tarkempaa ohjeistusta on osoitteessa: http://www.kanta.fi/web/ammattilaisille/testaus

Kysymys: Mitä tarkoitetaan järjestelmän käyttöönottopäivämäärällä Valviran ilmoituslomakkeessa?
Vastaus: Käyttöönottopäivämääräksi voi ilmoittaa päivämäärän, jona järjestelmä otetaan tai on otettu tuotantokäyttöön ensimmäisessä tuotantoympäristössä Suomessa, tai järjestelmän tuotantokäyttöön tarkoitetun version julkaisupäivämäärän.

6.2 Toiminnallisten vaatimusten profiilit

Kysymys: Mikä on toiminnallisten vaatimusten profiilien merkitys ja käyttö?
Vastaus: Profiilien avulla ilmaistaan eri käyttötarkoituksiin käytettävien sote-tietojärjestelmien kansalliset vähimmäisvaatimukset. Kukin profiili ottaa kantaa siihen, mitkä toiminnot ja tietosisällöt tulee toteuttaa järjestelmässä, joka täyttää tietyn käyttötarkoituksen (profiilin) mukaiset olennaiset vaatimukset. Profiilit nojautuvat THL:n määräyksen 2/2016 mukaisessa luokituksessa kuvattuihin järjestelmätoimintoihin ja tietosisältöihin. Tietojärjestelmässä tai tietojärjestelmäkokonaisuudessa, jolla on profiilia vastaava käyttötarkoitus, on toteutettava viitattujen määrittelyjen mukaisesti vähintään profiilissa pakolliseksi määritellyt toiminnot ja ominaisuudet.
Yksi järjestelmä voi toteuttaa usean profiilin mukaiset vaatimukset mutta myös sellaisia toimintoja ja sisältöjä, joita profiileissa tai luokituksessa ei ole määritelty. Valviraan tehtävissä ilmoituksissa ilmaistaan, minkä kansallisten profiilien mukaiset vaatimukset järjestelmä toteuttaa.

Kysymys: Miten toimitaan määräyksen mukaisen selvityksen ja järjestelmälomakkeen kanssa, jos järjestelmä ei täytä mitään vaadituista profiileista?
Vastaus: Määräyksen mukainen järjestelmälomake sekä asiakastietolain edellyttämä selvitys ja ilmoitus Valviralle on tehtävä riippumatta siitä täyttääkö järjestelmä yhdenkään kansallisen profiilin mukaiset vähimmäisvaatimukset.

Kysymys: Mitkä ovat profiilin uuden version vaikutukset profiilin aiemman version mukaiseen järjestelmään?
Vastaus: Aikaisemmin tehty ilmoitus säilyy vaikka ilmoitukseen sisältyvästä profiilista tulee uusi versio. Kun järjestelmästä tehdään myöhemmin uusi ilmoitus, tulee siirtyä noudattamaan uutta/viimeisintä profiilia siirtymäsäännösten ja voimaantuloaikojen mukaisesti, mikäli vanhan profiiliversion voimassaololle on säädetty päättymispäivä.

Kysymys: Mikä merkitys on profiilien toiminnoissa ja tietosisällöissä olevilla päivämäärillä tai teksteillä?
Vastaus: Profiileissa ilmaistut päivämäärät pohjautuvat valtakunnallisesti säädettyihin tai kansallisissa kehittämissuunnitelmissa kuvattuihin aikatauluihin. Jos profiilin voimaantulopäivämäärä ja vaatimuksen kohdalla ilmaistu päivämäärä ovat menneisyydessä, tarkoittaa se sitä, että vaatimus on jo voimassa. Tällöin profiilin mukaisen käyttöön otettavan tietojärjestelmän tai jo käytössä olevan järjestelmän uuden version tulee toteuttaa vaatimus. Osassa vaatimuksia on ilmaisu ”liittymisen yhteydessä”, joka tarkoittaa sitä että vaatimus on toteutettava ennen kuin profiilin mukainen järjestelmä otetaan tuotantokäyttöön Kanta-

palveluihin liittyneenä. Joissakin profiileissa vaatimuksia on myös tarkennettu ”järjestelmän käyttötarkoituksen mukaisesti”. Tällöin tietty toiminto tai vaatimus on toteutettava määrittelyjen mukaisesti, mikäli se järjestelmään kuuluu, mutta on myös olemassa järjestelmiä tai moduuleja, joissa toiminnon toteuttaminen ei ole välttämätöntä tai vaatimus on toteutettavissa esimerkiksi toisen liittyvän järjestelmän kautta.

Kysymys: Millä perusteella on saatavilla kansallisia vähimmäisvaatimusten profiileja? Miksi tietyn tyyppiselle erillisjärjestelmälle ei ole profiilia?
Vastaus: Profiili kohdistetaan joukkoon järjestelmiä, joille on määriteltävä yhdenmukaiset vähimmäisvaatimukset valtakunnallisella tasolla. Myös uusia profiileja voidaan tehdä kun on tunnistettu ehdokkaita uusille profiileille. Profiileja voi ilmestyä eri aikaan kuin uusia määräyksiä tai luokituksia, ja profiileja on myös mahdollista määrätä erikseen sitoviksi.

6.3 Toiminnallisiin vaatimuksiin liittyvät vastuut

Kysymys: Kuka vastaa, että tietojärjestelmä on vaatimusten mukainen?
Vastaus: Valviralle tehdyn ilmoituksen ja siihen liittyvien kuvausten kautta valmistaja tai tietojärjestelmäpalvelun tuottaja vakuuttaa, että järjestelmä asianmukaisesti asennettuna, ylläpidettynä ja käyttötarkoituksen mukaisesti käytettynä täyttää Asiakastietolain 19 a § kautta säädetyt olennaiset vaatimukset. Ilmoittaja vastaa siitä, että ilmoitetut toiminnot ja tietosisällöt vastaavat järjestelmään toteutettuja. Mikäli järjestelmä kuuluu A-luokkaan, on lomakkeen tietojen vastattava myös yhteistestauksen ja tietoturvallisuuden auditoinnin tuloksia.

Kysymys: Kuka täyttää toiminnallisten vaatimusten mukaisen järjestelmälomakkeen ja mihin se toimitetaan?
Vastaus: Järjestelmälomakkeen täyttää ja lähettää tietojärjestelmän valmistaja tai tietojärjestelmäpalvelun tuottaja. Järjestelmälomake tulee olla täytettynä hakeuduttaessa yhteistestaukseen tai auditointiin. Valviralle toimitettavan ilmoituslomakkeen (Ilmoitus tietojärjestelmän käyttöönotosta - ilmoituslomake, pdf) yhteydessä on aina toimitettava lisäksi määräyksen 2/2016 mukainen järjestelmälomake (järjestelmälomake, xls), joka tulee lähettää ilmoituslomakkeen lisäksi Valviran asiointipostilaatikkoon (AsTL-asiat(at)valvira.fi).

Kysymys: Mitä asioita kuuluu sote-palveluntuottajan vastuulle olennaisissa vaatimuksissa?
Vastaus: Sosiaali- ja terveydenhuollon palvelun antajan tai apteekin tulee varmistaa, että sen toiminnassa tuotantokäyttöön otettavan tietojärjestelmän tiedot löytyvät Valviran ylläpitämästä rekisteristä (rekisteri tulee saataville 1.1.2017 mennessä), josta pystyy myös tarkistamaan omista tai hankittavista järjestelmistä tehdyt ilmoitukset. Rekisterin kautta saa tietoa myös A-luokassa hyväksytysti suoritetuista testauksista ja auditoinneista, vaatimustenmukaisuustodistusten ja testaustulosten päivittymisestä ja ajantasaisuudesta. Lisätietoja on Valviran sivuilla: http://www.valvira.fi/terveydenhuolto/terveysteknologia/tuotteen_markkinoille_saattaminen/tietojarjestelmat

Kysymys: Jos tuotannossa olevalla A- tai B-luokan tietojärjestelmällä ei enää ole valmistajaa, joka vastaisi olennaisten vaatimusten täyttämisestä, voiko järjestelmää käyttää ja kuka vastaa ilmoittamis- ja todentamistoimenpiteistä?
Vastaus: Tuotannossa olevalla A- tai B-luokan järjestelmällä on oltava vastuutaho, joka vastaa järjestelmän ylläpidosta, ilmoittamisesta ja olennaisten vaatimusten täyttämisestä. Mikäli alkuperäinen valmistaja on esimerkiksi mennyt konkurssiin mutta järjestelmällä on joku muu taho joka vastaa järjestelmän toiminnasta, ylläpidosta ja kehittämisestä, voi tämä taho tehdä myös järjestelmää koskevat ilmoitukset ja huolehtia olennaisten vaatimusten toteuttamisesta ja tarvittaessa todentamisesta. Tällainen taho voi olla myös järjestelmän käyttäjäorganisaatio.

Kysymys: Koska Valviran asiakas- ja potilastietojärjestelmien rekisteri on käytettävissä ja mikä sen merkitys on?
Vastaus: Vuoden 2017 alusta alkaen Valvira ylläpitää julkista rekisteriä asiakas- ja potilastietoja käsittelevistä hyväksytyistä tietojärjestelmistä. Ainoastaan Valviran rekisteriin ilmoitettujen tietojärjestelmien käyttöönotto on sallittua. Ennen Valviran rekisterin ilmestymistä Kanta-palveluihin liittyvien tietojärjestelmien voimassa olevien aiempien hyväksyntöjen tilanteen voi tarkistaa Kanta-sivustolta.

7 Sote-tietojärjestelmien olennaiset tietoturvallisuuden vaatimukset ja auditointikriteerit

Tässä osiossa on tietoturvallisuuden olennaisiin vaatimuksiin, auditointikriteereihin ja yksittäisiin sertifiointivaatimuksiin kohdistuneita kysymyksiä ja vastauksia. Kysymyksissä esiintyvät numerot viittaavat vaatimusnumeroihin dokumentissa ”Määräys 1/2015, Liite 1: Tietoturvavaatimukset A-luokkaan kuuluville järjestelmille ja järjestelmien käyttöympäristöille”:

Kysymys: Vaatimus #2 vaatii että potilaskertomuksen muuttumattomuus tulee taata myös muussa kuin asiakirjamuodossa. Mikä on riittävä muuttumattomuuden takaamisen tapa? Riittääkö että tiedot on tallennettu tietokantaan eikä niitä pääse ohjelman käyttöliittymän kautta käsittelemään ilman että lokeihin jää jälki?
Vastaus: #2: "Muuttumattomuus" muussa kuin asiakirjamuodossa riippuu järjestelmän toteutustavasta ja on sovitettava siihen. On pyrittävä huolehtimaan vähintäänkin siitä, että jäjitettävyys saadaan aikaan esimerkiksi lokien kautta mikäli muutoksia tehdään sovelluksella. Lisäksi on varmistettava, etteivät sivulliset pääse asiattomasti muuttamaan järjestelmään talletettuja tietoja.

Kysymys: Vaatimus #2: lisäkentässä mainitaan: ”Tarkastetaan, että allekirjoitetun asiakirjan sisältö on yhtenevä sen kanssa, mitä merkinnän tekijä on nähnyt.” Mihin tällä viitataan? Liittyykö tämä asiakirjan noutoon arkistosta, ja kuinka asiakirjan muuttumattomuus taataan?
Vastaus: Kohdassa 2A viitataan asiakirjan lähettämiseen arkistoon. Tulee siis varmistua siitä, että teksti, jonka käyttäjä on esimerkiksi potilaan hoitokertomukseen kirjannut siirtyy sellaisenaan KanTa-palveluihin. Auditoinnin yhteydessä tarkastetaan, että jos lähetettävän asiakirjan sisältöä säilytetään paikallisessa tietokannassa ennen asiakirjan muodostusta ja lähetystä, tulee sen muokkaaminen käyttöoikeuksin estää tai tehdä tarvittava versiohistoria kaikista asiakirjan muutoksista. Vaatimuksessa ei siis tarkasteta tai puututa asiakirjan sisältöön vaan varmistetaan, että asiakirjat säilytetään muuttumattomina paikallisessa tietokannassa ja allekirjoitetaan ennen lähetystä KanTa-palveluihin. Asiakirjan muuttumattomuus taataan muilla keinoilla kuin edellyttämällä asiakirjan alkuperäisen sähköisen allekirjoituksen tarkistamista asiakirjan hakevassa järjestelmässä.

Kysymys: Vaatimus #5 lisätiedot ja VAHTI-ohjeet kuvaavat, että salasana on lukittava viiden virheellisen kirjautumisyrityksen jälkeen. Onko tämä ehdoton vaatimus, mikäli toimintaympäristössä tästä voi aiheutua merkittävää haittaa potilasturvallisuudelle (esimerkiksi pienellä palveluntarjoajalla, jolla ei ole ylläpitohenkilökuntaa tai ympärivuorokautista teknistä palvelusopimusta tietojärjestelmäpalvelun tuottajan kanssa)?
Vastaus: #5: Lisätiedot-kohtien tiedot eivät ole todentamisessa säännönmukaisesti käytettäviä kriteerejä. Vaatimus on kompensoitavissa, mikäli sen toteuttamisesta syntyisi merkittävää haittaa potilasturvallisuudelle. Kompensaationa tulee kuvata, millaisilla ohjeilla tai menettelyillä pyritään välttämään virheelliset kirjautumiset ja salasanojen ”arvaamiseen” liittyvä väärinkäyttö. Järjestelmissä ja paikallisissa hallintakäytännöissä tulee kuitenkin varautua siihen, että vaatimuksen VAHTI-mukaista tulkintaa tullaan kiristämään jatkossa.

Kysymys: 4Y D: ”Tarkastetaan kuvaukset roolien, käyttäjätietojen ja käyttöoikeuksien hallinnan periaatteista ja ohjeet niiden toteuttamisesta käyttäjäorganisaatioille.”Meillä ei ole erillisiä ohjeita miten käyttäjäorganisaatiossa pitää laatia käyttäjäryhmiä. On kyllä ohjeita ja koulutusta miten ohjelma käytetään. Se on organisaatiosta kiinni miten ne haluavat rakentaa ja ylläpitää käyttäjäryhmiä. Mielestämme käyttäjäryhmien toteutus on organisaatioiden oma asia. Järjestelmässä pitää vain tukea käyttäjäryhmiä.

Vastaus: Vaatimusten mukaisesti järjestelmän on tuettava eri rooleissa.toimivien käyttäjien roolin mukaista toimintaa. Esimerkiksi jokaisen sähköisen reseptin käyttötapauksen esiehdoissa on määritelty, minkä käyttäjäryhmän mukaiset oikeudet käyttäjällä pitää olla, jotta hän voi suorittaa ko. käyttötapauksen. Sähköisen reseptin lääkemääräysten ja toimitusten osalta oikeudet on kuvattu myös Sähköisen lääkemääräyksen määrittelydokumentissa ”Lääkemääräyksiin ja toimitussanomaan liittyvät oikeudet”: http://www.kanta.fi/documents/12105/3448591/eResepti_Maarittely_Liite1V2.6.pdf/1a1e59cd-55df-4ec5-9ccf-1512c0fa78ab . Eri toimintojen mukaisia käyttäjäryhmävaatimuksia on myös Potilastietojärjestelmien vaatimusmäärittelyissä sekä arkiston että reseptin osalta. Potilasasiakirjamerkintöjen tekemisen oikeudet on todettu mm. potilasasiakirja-asetuksessa (mm. 4 § Potilasasiakirjoihin sisältyvien tietojen käyttöoikeudet ja 6 § Oikeus tehdä merkintöjä potilasasiakirjoihin). Jos määriteltyjen roolien mukaiset käyttöoikeudet määritellään vasta käyttöympäristössä, järjestelmässä on oltava kuvaus ja/tai ohje siitä, kuinka oikeuksien määrittely käyttöympäristössä tehdään siten, että vaatimukset täyttyvät.

Kysymys: #6: Tarkoittaako kriteerissä 6 Y kuvattu validointi Kanta-palvelusta haettavien asiakirjojen sähköisen allekirjoituksen validointia? Onko Kantasta tietoja hakevan sovelluksen validoitava asiakirjan sähköinen allekirjoitus?
Vastaus: Kohdassa 6Y viitataan käytettävien varmenteiden vertaamiseen sulkulistaan. Asiakirjan sisältöön tai allekirjoittamiseen ei tässä vaatimuksessa puututa. Kanta-palvelusta haettavien asiakirjojen alkuperäisen tai Kanta-allekirjoituksen validointia ei edellytetä tietoja hakevalta järjestelmältä?

Kysymys: #7: mitä rajoituksia pitää tarkistaa automaattisesti – koskeeko vaatimus vain lääkkeenmääräämisen rajoituksia jotka on vaadittu Valviran ohjeissa tai muitakin rajoituksia? Voitteko antaa esimerkkejä?
Vastaus: #7: Kyse on Valviralta haettavista rajoitustiedoista sähköiseen lääkemääräykseen liittyen. Osa rajoituksista voidaan toteuttaa ohjelmallisesti (mukaan lukien lääkevalmisteisiin kohdistuvat). Ei-ohjelmallisesti toteutettavia rajoitustietoja koskee myös vaatimus niiden näyttämisestä käyttäjälle ja lokitusvaatimus. Näistä on tietoja mm. osoitteessa:
http://www.valvira.fi/documents/14444/37132/Ammattioikeuden_rajoitustietojen_valittaminen.pdf
Ohjeita myös päivitetään mm. web-reseptiin liittyen.

Kysymys: #7: Millaisia tietoja on kirjattava potilastietojärjestelmän käyttölokiin rajoituksista, jotka eivät ole ohjelmallisesti tarkistettavia vaan pelkästään käyttäjälle näytettäviä? Riittääkö että käyttölokiin merkitään vain tieto rajoitusten tarkistamisesta tai siitä että rajoituksia on, vai pitääkö rajoitusteksti kirjata käyttölokiin?
Vastaus: #7: Pelkkä käyttölokikirjaus rajoituksen olemassaolosta ei riitä, vaan lokiin on kirjattava riittävän tarkat tiedot rajoituksesta kuten rajoitusteksti. Käyttötapausmäärittelyjen mukaisesti ”Jos lääkkeenmääräjällä on rajoitustieto, pitää se kirjata valvontaa varten perusjärjestelmän lokeihin...”

Kysymys: #10: ”Pääkäyttäjillä on oikeus tarkistaa oman organisaationsa tietoja Kantasta virhetilanteissa. Tietojärjestelmäpalvelun tuottajalla on oikeus tarkistaa virhetilanteissa sen organisaation tietoja Kantansa, jonka lukuun järjestelmäasiantuntijat selvityksen aikana toimivat. Tietojärjestelmiin on toteutettava käyttövaltuudet siten, että Kanta-oikeudet rajataan ed mainituissa virhetilanneselvityksissä ainoastaan omien tietojen hakuun. Kaikki selvityksessä tehdyt haut tulee näkyä lokeista.” Alleviivattu ominaisuus ei ole toteutettu järjestelmään, eli vain terveydenhuollon ammattihenkilöt pystyvät tällä hetkellä suorittamaan hakuja potilastiedon arkistosta. Onko tämä ongelma? Vai onko olemassa joku toinen vaatimus joka määrää että tämä ominaisuus on oltava?

Vastaus #10**:** Kyse on siitä että mikäli tietojenkäsittely ei tapahdu asiakkaan asioiden hoitamiseksi (vaan esim. virhetilanteen selvittämiseksi), pitäisi päästä vain oman organisaation tietoihin, jos Kanta-palvelun käyttöä tarvitaan virhetilanteen selvittämiseksi. Ks. myös alla oleva vastaus.

Kysymys: #10: Mitä tietoja kyseinen vaatimus koskee ja minkälaiset oikeudet järjestelmäasiantuntijoilla on / tulisi olla Kantaan? Minkä perusteella/parametreilla järjestelmäasiantuntijat voivat tehdä hakuja Kantaan ja mitä tietoa näistä hauista palautuu? Miksi luovutushaut rajataan pois kohdassa #10? Ongelmahan voi liittyä juuri luovutuksella saatavaan tietoon.
Vastaus: #10: Vaatimus tarkoittaa, että esimerkiksi virhetilanteiden selvittelytilanteissa tukihenkilö voi tarvittaessa päästä tarkastelemaan oman organisaationsa (tai sen organisaation tietoja jonka lukuun selvittelyä tehdään) asiakas- tai potilastietoja myös Kanta-palveluista, mikäli virhetilanteen selvittely sitä vaatii. Luovutuksella saatavia muiden organisaatioiden tai rekisterien tietoja ei saa päästä katsomaan, ja asianmukaiset lokimerkinnät myös näissä selvittelytilanteissa tarvitaan. Vaatimusmuotoilu on tarkennusten kautta syntynyt viranomaisten yhteinen linjaus - valmistelussa oli sekä ehdotuksia siitä että luovutushautkin pitäisi olla mahdollisia kuin myös se, että organisaation omatkin tiedot pitäisi kieltää Kanta-palveluihin liittyvissä selvittelyissä. Tietojen käytön vain organisaation omiin tietoihin on ratkaisu, jolla pienennetään "vahinkojen vaikutusaluetta" mikäli virhetilanteissa tai selvittelyoikeuksia saaneiden toimesta sattuisi kaikesta huolimatta tapahtumaan väärinkäytöksiä, ja se vastaa pitkälti aiempaa käytäntöä jossa virhetilanteita selvittelevä henkilöstö on voinut nähdä oman organisaationsa tietoja virhetilanteiden selvittämisessä, vaikka tehtävä työ ei suoraan liitykään asiakkaan hoito- tai asiakassuhteeseen. Hakutilanteet ja -toiminnot voivat liittyä Kanta-käyttötapausten mukaisiin toimintoihin. Vaatimus ei suoraan liity siihen, tapahtuuko tunnistautuminen ammattilaisen tai esimerkiksi järjestelmäasiantuntijan toimikortilla.

Kysymys: #12: Mitä tarkoittaa ”tekninen loki” ja miten se täsmälleen on määriteltävä?
Vastaus: #12: "Tekninen loki" yleisesti viittaa järjestelmien ja alustojen lokitietoihin, joita käytetään mm. teknisten virheiden selvittelyssä ja jotka ovat erillisiä Kanta-palveluihin liittyvistä käyttö- ja luovutuslokeista. Tässä vaatimuksessa tarkoitetaan nimenomaisesti Kanta-viestinvälitykseen liittyviä lokitietoja (muut kuin käyttö- ja luovutuslokitiedot).

Kysymys: #13: Onko käyttölokiin tallennettava tiedot kaikkien potilaslistoissa näytöllä näkyvien henkilöiden tiedoista?
Vastaus: #13: Tässä vaiheessa ei edellytetä lokimerkintöjen tekemistä kaikista potilaslistoissa esiintyvistä henkilöistä, mikäli henkilöiden tarkempia tietoja ei käytetä. Lokivaatimusten myöhemmän täsmentämisen yhteydessä vaatimusta voidaan tarkentaa.

Kysymys; #16: Y Verkkoliikenteen tietoliikenneprofiili - Verkkoliikenteen normaali tietoliikenneprofiili (baseline) on tiedossa; on olemassa menettely, jolla normaalista tietoliikenneprofiilista eroava liikenne pyritään havaitsemaan; järjestelmän osalta on pystyttävä kuvaamaan, millaista verkkoliikennettä normaali käyttö aiheuttaa. Pitääkö baseline olla tiedossa tuotantoympäristöstä?
Vastaus: Tarkkoja lukuja tietystä tuotantoympäristöstä ei edellytetä, mutta tulisi kuvata arvio siitä, millainen verkkoliikenteen määrä ja luonne on tyypillisessä tai joissakin tyypillisissä käyttöympäristöissä.

Kysymys: #16: Riittääkö vain käytetyt portit vai pitääkö olla tiedossa profiili ”dekaditasolla” esim. yöllä hiljaista ja virka-aikaan satoja käyttäjiä. Millä tasolla normaali käyttö pitää pystyä kuvaamaan, esim. https-liikennettä palvelinsaliin vai pitäisikö olla kuvattuna summittainen liikennemäärä per käyttäjä?
Vastaus: Käytettyjen tietoliikenneporttien erittely ei riitä, vaan kuvattaviin seikkoihin kuuluu myös, mikäli tietoliikenteen määrä vaihtelee tyypillisessä käytössä esimerkiksi eri vuorokauden aikoina. Kuvauksessa tulisi olla mukana vähintäänkin arvio käyttäjämäärän normaalista vaihtelusta ja eri käyttäjämäärien vaikutuksista verkkoliikenteeseen.

Kysymys: #16: Poikkeavan liikenteen havainnointi: pitääkö olla kyky havaita esim. porttiskannaus / bruteforce / palvelunestohyökkäys?
Vastaus: Järjestelmän luonteesta ja kriittisyydestä riippuu se, kuinka tärkeää on havaita esimerkiksi palvelunestohyökkäykset ja porttiskannaukset. Kaikkia A-luokan järjestelmiä koskeviin vaatimuksiin ei kuulu kyky järjestelmätasolla havaita hyökkäyksiä. Tulisi kuitenkin pystyä kuvaamaan, kuinka esimerkiksi järjestelmän ongelmatilanteissa voidaan pyrkiä selvittämään onko kyseessä palvelunestohyökkäys, ja kuinka verkkokäyttöisessä sovelluksessa tai sen käyttöympäristössä on varauduttu tai tulisi varautua porttien skannausta vastaan.

Kysymys: #19: Kuinka lääkemääräysten toimitustiedon tulostuksen ja tallennuksen suhteen toimitaan, jos järjestelmässä tai Kanta-palveluissa on häiriötilanne, joka estää toimitustiedon tallentamisen Reseptikeskukseen - onko toimitukseen liittyvä tarra tulostettava tällöinkin vasta sitten, kun toimitustieto on tallennettu onnistuneesti Reseptikeskukseen?
Vastaus #19: Häiriötilanteessa toimitustieto voidaan tulostaa apteekissa paikallisesti tallennetun, myöhemmin Reseptikeskukseen tallennettavan lääketoimituksen pohjalta.

Kysymys: #27: Mitä tarkoitetaan ”kansallisesti ylläpidettävillä perustiedoilla”? Koodistopalvelussa ylläpidetään koodistoja kuten tietosisältöjä tai lomakemäärittelyitä, joita ei voida nykyisellään päivittää järjestelmiin muuten kuin ohjelmakoodia muuttamalla. Muu vaatisi pitemmälle menevää ja mutkikasta geneeristä toteutusta.
Vastaus: #27: Vaatimuksena ei tietenkään ole että järjestelmä automaattisesti mukautuisi lomake- tai tietosisältö- (tai edes koodisto-)määrittelyihin, vaan että tapa jolla koodistopalvelusta näitä hyödynnetään on kuvattu (kuvauksena voi siis olla myös kuvaus esim. siitä miten seurataan koodistopalvelun sisältöjä ja tehdään niiden pohjalta päivityksiä).

Kysymys: #40Y Turvallisen ohjelmoinnin periaatteet järjestelmätoteutuksissa: onko täytettävä ja todennettava kirjaimellisesti kaikki lisätietoja-kohdan mukaiset vaatimukset?
Vastaus: #40Y: Vaatimus ja sen kontrollit koskevat tässä vaiheessa sitä, kuinka eri alakohtien sisältöjen mukainen ohjelmistokehitysmalli on kuvattu ja suunniteltu toteutettavaksi. Tämän mallin mukaiseen toimintaan tulee todennäköisesti jatkossa kohdistumaan myös kuvaamista tiukempia todentamistapoja. Pitkään aiemmin kehitetyissä järjestelmissä on todennäköisesti osia, joissa kaikkia lisätietoja-kohdan mukaisia kriteerejä ei ole pitkäaikaisessa kehitystyössä huomioitu koko kehityshistorian aikana. Vaatimusten mukaisten seikkojen kuvaaminen on lähtökohta sille, että järjestelmän kehittämisessä huolehditaan jatkossa entistä tarkemmin kansallisen turvallisuusauditointikriteeristön mukaisesta ohjemistokehityksestä.

Kysymys: #43Y Järjestelmässä tulee olla menettely, jolla luvaton käyttö ja luvattomat käyttöyritykset voidaan havaita. Tarkoitetaanko järjestelmällä alustaa (windows server/iis/sql) vai A-luokan potilastietojärjestelmää?
Vastaus: #43Y: Vaatimukset kohdistuvat A-luokan järjestelmään ja sen käyttöympäristöön. Jos käytettävä alusta on osa järjestelmää ja vaatimuksiin vastataan alustan kautta, vaatimukset voidaan täyttää myös tällä tavoin. Jos alusta ja palvelimet eivät ole osa järjestelmää vaan osa käyttöympäristöä ja alustan ominaisuuksia käytetään vaatimusten täyttämiseen, tulee järjestelmän osalta kuvata kuinka vaatimuksiin käyttöympäristössä vastataan tai kuinka niihin tulee vastata. Luvattomien käyttöyritysten estämisen ja havaitsemisen vaatimukset sinällään koskevat järjestelmän loppukäyttäjille tarjottavien sisäänkirjautumispalvelujen ja -näyttöjen lisäksi myös järjestelmän suoritusympäristön palvelinohjelmistoja.

Kysymys: #43Y: Minkälaista havaintokykyä vaaditaan? Jos käyttöoikeudet on rajattu, ettei käyttäjä pääse tekemään luvattomia asioita niin täytyykö olla kyky havaita tällainen toiminta?
Vastaus: #43Y: Tunnistus- ja autentikointimekanismien osalta luvattomista käyttöyrityksistä tulisi syntyä lokitiedot joiden tarkistamisesta huolehditaan. Järjestelmissä tai käyttöympäristössä voi myös olla edistyneempiä havainnointi- ja hälytysmekanismeja ja esimerkiksi samasta osoitteesta tulevien toistuvien

luvattomien käyttöyritysten havainnointi ja automaattinen estäminen, mutta nämä eivät nykyisellään sisälly kaikille järjestelmille pakollisiin aina todennettaviin vaatimuksiin. Käyttövaltuuksien hallinta on tehtävä kunkin käyttäjän osalta tarkoituksenmukaisesti siten, että hyväksytysti tunnistautuneet käyttäjät saavat tehdä omaan rooliinsa kuuluvia toimenpiteitä ja nähdä oman roolinsa mukaisia tietoja järjestelmässä.

Kysymys: Tarkastetaanko käyttöympäristövaatimuksia kuten 46, 47 ja 49 silloin, kun auditoidaan perusjärjestelmää ilman käyttöympäristöä? Onko kohdissa mainitut järjestelmän dokumentointivaatimukset toistettu muualla?
Vastaus: #46, 47, 49: Nämä vaatimukset todennetaan siltä osin kuin järjestelmä ottaa niihin kantaa ja/tai antaa niihin ohjeistuksia. Osa vaatimuksista voi yleensäkin pääosin toteutua järjestelmän kautta tai sitten käyttöympäristössä tehtävillä toimenpiteillä jotka eivät ole suoraan tai pelkästään järjestelmän kautta hoidettavia. Omavalvontasuunnitelmaan ja olennaisiin vaatimuksiin liittyvät määräykset ja vaatimukset on pyritty synkronoimaan siten, että osalle vaatimuksista on myös omavalvontasuunnitelmassa vastaavia kohtia. Järjestelmän osalta on syytä kuvata ja ohjeistaa, missä määrin eri vaatimukset ratkaistaan järjestelmän kautta, missä määrin konfigurointi- tai asennusohjeilla ja missä määrin pitää hoitaa kunkin käyttöympäristön omilla toimenpiteillä, joiden tarkat vastuut voivat sisältyä myös omavalvontasuunnitelmiin.

Kysymys: ”48Y D/H: Tarkastetaan että mahdolliset hallintayhteydet on toteutettu salatulla yhteydellä, esim. VPN, SSH, SSL/TLS tai hallintayhteyksille on oma suojattu verkkonsa.” Miten tulee toimia esimerkiksi "remote desktop" eli rdp yhteyksissä asiakkaiden järjestelmäympäristöihin? Näissä yhteyksissä välitetään ”pelkkä kuva”, mutta liikenne ei ole salattu. Yhteyksiä on yleensä rajoitettu ip-osoitteiden mukaan. Lisäksi asiakkailla voi olla henkilöitä, jotka tekevät kotona etätöitä.

Vastaus: Hallintayhteyksissä tulee käyttää salattua yhteyttä. Esimerkiksi VPN-yhteyden asentaminen suojaamaan remote desktop käyttöä tai Secure RDS -yhteyksien käyttäminen SSL-protokollan kanssa on mahdollista. IP-osoitteiden rajoittamisella voidaan toimia siirtymäaikana sellaisissa järjestelmissä, jotka ovat aiemmin liittyneet Kanta-palveluihin, mutta salattujen hallintayhteyksien käyttöä vaaditaan, ja niiden toteuttamiseen on olemassa myös edullisia vaihtoehtoja. Esimerkkejä: https://technet.microsoft.com/en-us/magazine/ff458357.aspx , http://www.howtogeek.com/175087/how-to-enable-and-secure-remote-desktop-on-windows/

Järjestelmän normaalien toimintojen etäkäytössä ovat voimassa samat perusvaatimukset kuin paikalliskäytössä. Järjestelmän osalta tulisi kuvata, kuinka järjestelmässä suojataan myös etätyössä tapahtuva tietoliikenne siten että sivulliset eivät pääse tietoihin, tai kuinka tällainen suojaus on toteutettava järjestelmän käyttöympäristössä jota ylläpitää joku muu kuin järjestelmän valmistaja. Jos tämä vastuu jää järjestelmän käyttäjälle tai käyttöympäristön ylläpitäjälle, siitä on tiedotettava myös näille tahoille.

8 Määräajat ja voimassaolot: kysymyksiä ja vastauksia

Kysymys: Järjestelmämme jonka on suunniteltu liittyvän Kanta-palveluihin ei ole vielä käynyt läpi yhteistestausta eikä sertifiointiprosessia. Ovatko tietoturvan sertifiointivaatimukset sille voimassa?
Vastaus: Ovat, säädösten ja määräysten mukaisesti. Yhteistestaus, tietoturva-auditointi ja vaatimustenmukaisuustodistus tarvitaan ennen kuin järjestelmän Kanta-yhteydet voidaan ottaa tuotantokäyttöön.

Kysymys: Järjestelmäämme on suoritettu tietoturvallisuuden auditointi ja yhteistestaus ennen 1.1.2015. Koska tarvitaan uudelleenauditointi ja uusien määräysten mukainen vaatimustenmukaisuustodistus?
Vastaus: Nykyisten määräysten mukaisesti vanha auditointi on voimassa auditointiraportissa todetun voimassaolon mukaisesti. Kelan päätöksellä ennen 1.1.2015 hyväksytty järjestelmä on voitu liittää Kanta-

palveluihin enintään kahden vuoden ajaksi. Voimassa olevat vanhan hyväksyntäprosessin mukaiset hyväksynnät vanhenevat siis viimeistään 1.1.2017. Mikäli järjestelmään tai palveluun on tehty vain itseauditointi, tulee huolehtia ulkoisesta tietoturva-auditoinnista siirtymäaikojen puitteissa. Muutokset järjestelmissä tai olennaisissa vaatimuksissa voivat aiheuttaa tarpeita suorittaa sertifiointia, yhteistestausta ja tietoturvallisuuden auditointia ennen aiemman hyväksynnän päättymispäivämäärää, ja uusissa sertifioinneissa hankitaan uusien säädösten mukainen vaatimustenmukaisuustodistus. Esimerkiksi sähköisen lääkemääräyksen toiminnallisuuksia toteuttavien potilastieto- ja apteekkijärjestelmien osalta määräaikoja, menettelyjä ja tarvittavia yhteistestauksia on tarkennettu mm. ohjeessa 6/2015:
https://www.thl.fi/fi/web/tiedonhallinta-sosiaali-ja-terveysalalla/tiedon-ja-vaatimusten-yhdenmukaistaminen/maaraykset-ja-ohjeet

Kysymys: Voiko Kanta-palveluihin liittyä 1.1.2015 jälkeen sellaisen välittäjäpalvelun kautta, joka on ennen tätä suorittanut tietoturvan itseauditoinnin?
Vastaus: Kyllä voi, mutta käytössä olevassa Kanta-välityspalvelussa on huolehdittava uusien määräyksien mukaisen sertifioinnin toteuttamisesta määräysten voimaantulosäädösten mukaisesti, kuten edellisessä kysymyksessä on kuvattu.

Kysymys: Pitääkö tietojärjestelmällä olla vaatimustenmukaisuustodistus, ennen kuin sen valmistaja hakee arkiston asiakirjoihin tarvittavaa järjestelmäallekirjoitusvarmennetta palveluna yksityisen terveydenhuollon toimijoille tarjottavaan järjestelmään?
Vastaus: Kyllä pitää. Asiaa käsitellään mm. ohjeessa 4/2015:
http://www.thl.fi/attachments/oper/ohje_4_2015_jarjestelmavarmenteet_yksityisessa_terveydenhuollossa.pdf
Mikäli palveluun kuuluu myös Kanta-liityntäpiste, siinä hyödynnettävä palvelinvarmenne on mahdollista hakea erikseen välittäjäroolissa. Varmenteiden hakemisesta lisätietoja löytyy VRK:n varmennepalvelujen sivuilta:

9 Ohjaus ja neuvonta

Sertifioinnin ja omavalvonnan määräykset sekä lisätietoja verkossa:

http://www.thl.fi/fi/web/tiedonhallinta-sosiaali-ja-terveysalalla/tiedon-ja-vaatimusten-yhdenmukaistaminen

http://www.kanta.fi/web/ammattilaisille/sertifiointi