Tietopalvelut
Sote-tieto ja -tiedonhallinta

9.12.2021

LUOKKAAN A KUULUVIEN SOSIAALI- JA TERVEYDENHUOLLON TIETOJÄRJESTELMIEN MUUTOSTEN ILMOITTAMINEN

Tässä liitteessä kuvataan, mitkä ovat sellaisia muutoksia aikaisemmin yhteistestatussa tai tietoturvallisuuden arvioinnin hyväksytysti läpäisseessä tietojärjestelmässä, joista tulee ilmoittaa Kelalle ja tietoturvallisuuden arviointilaitokselle. Liite kokoaa ja tarkentaa asiakastietolain ja määräyksen 4/2021 mukaisia menettelyjä tietojärjestelmien muutostilanteissa.

Tausta ja perusteet

Tietojärjestelmän valmistaja tai tietojärjestelmäpalvelun tuottaja vastaa asiakastietolain sekä määräysten 4/2021 ja 5/2021 mukaisesti sosiaali- ja terveydenhuollon tietojärjestelmän vaatimustenmukaisuudesta ja tähän liittyvistä asiakastietolain mukaisista yhteistestauksen, tietoturvallisuuden arvioinnin velvoitteista.

Asiakastietolaissa säädetään, että luokkaan A kuuluvien tietojärjestelmien merkittävistä muutoksista on ilmoitettava *tietoturvallisuuden arviointilaitokselle*. Todistus tietoturvallisuuden arvioinnista on uudistettava, jos tietojärjestelmään tehdään merkittäviä muutoksia tai järjestelmään kohdistuvia olennaisia vaatimuksia muutetaan.

Asiakas- ja potilastietojärjestelmien Kanta-palveluihin talletettavien tietojen yhteentoimivuus muiden asiakas- ja potilastietojärjestelmien kanssa on osoitettava Kelan kanssa suoritettavassa yhteistestauksessa. Yhteentoimivuusvaatimus koskee myös tilanteita, joissa järjestelmiin tehdään merkittäviä muutoksia. Tämän vuoksi asiakastietolaissa säädetään, että merkittävät tietojärjestelmien muutokset ilmoitetaan myös *Kelalle*.

Yhteistestauksen ja tietoturvallisuuden arvioinnin edellytyksenä on valmistajan selvitys siitä, kuinka tietojärjestelmän toiminnallisuutta koskevat vaatimukset on toteutettu ja testattu. Selvityksessä käytetään THL:n määräyksen 5/2021 liitteen 4 mukaista järjestelmälomaketta.

Tietojärjestelmiin tai määrittelyihin kohdistuvissa muutostilanteissa muutosten rajaamisella tiettyihin toimintoihin tai sisältöihin voidaan suoraviivaistaa uudelleentestaus- tai uudelleenarviointimenettelyjä. Esimerkiksi uuden asiakirjatyypin tai rakenteisen sisällön toteuttaminen järjestelmässä ei välttämättä edellytä kaikkien viestinvälitykseen liittyvien toiminnallisuuksien uutta testausta.

Tämä määräyksen liite perustuu aiempien säädösten nojalla annettuun THL:n ohjeeseen 2/2018, jonka tämä liite korvaa. Liitteen sisältö on valmisteltu viranomaisyhteistyössä (THL, Kela, Valvira, Viestintävirasto, STM, tietoturvallisuuden arviointilaitokset), pohjautuen näille tahoille tulleisiin kyselyihin sekä sertifiointiprosessista saatuihin kokemuksiin. Liitteessä käytetyt termit kuten valmistaja ja tietojärjestelmäpalvelun tuottaja vastaavat asiakastietolaissa ja määräyksessä 4/2021 noudatettuja termejä.

Muutosten ilmoittamisen menettely

Tietojärjestelmäpalvelun tuottajan tulee ilmoittaa luokkaan A1, A2 tai A3 kuuluvien järjestelmien merkittävistä muutoksista Kelalle ja tietoturvallisuuden arviointilaitokselle tämän liitteen mukaisesti. Ilmoituksen perusteella Kela tai tietoturvallisuuden arviointilaitos arvioivat, edellyttävätkö muutokset uutta yhteistestausta tai sellaista uutta tietoturvallisuuden arviointia, jonka johdosta tietojärjestelmälle tai osajärjestelmälle on kirjoitettava uusi todistus tietoturvallisuuden arvioinnista.

Jos vaatimuksista vastaava tietojärjestelmäpalvelun tuottaja on joku muu kuin valmistaja, valmistajan ja tietojärjestelmäpalvelun tuottajan on keskenään sovittava siitä, kuka vastaa järjestelmämuutoksiin liittyvistä sertifiointimenettelyistä ja järjestelmään liittyvistä muutosilmoituksista.

Tietojärjestelmäpalvelun tuottajan vaihtuessa tulee huolehtia siitä, että järjestelmää ja sen päivityksiä koskevat vaatimukset täyttyvät edelleen, ja että niiden täyttyminen on dokumentoitu.

Muutosilmoituksen mukana on toimitettava THL:n määräysten 4/2021 ja 5/2021 mukaisesti täytetty järjestelmälomake (määräys 5/2021 liite 4). Lomake toimitetaan Kelalle, kun Kelalle tehdään muutosilmoitus yhteistestaustarpeen arviointia varten. Lomake toimitetaan myös tietoturvallisuuden arviointilaitokselle tehtävän muutosilmoituksen mukana, jotta se voi arvioida, onko järjestelmälle tarpeen suorittaa uusi tietoturvallisuuden arviointi. *Järjestelmälomakkeeseen on merkittävä määräyksen 5/2021 mukaisilla merkinnöillä uudet ja merkittäviä muutoksia sisältävät järjestelmään toteutetut tai järjestelmän kautta täytettävät toiminnot, tietosisällöt ja tietoturvavaatimukset. Uusien ja muuttuneiden järjestelmään toteutettujen olennaisten vaatimusten on erotuttava selkeästi aiemmin järjestelmässä todennetuista olennaisista vaatimuksista.*

Tämän liitteen mukaisten ilmoitusten yhteydessä on tarvittaessa päivitettävä tietojärjestelmää koskevat tiedot myös Valviran tietojärjestelmärekisteriin, mikäli aiemmin ilmoitetut tiedot muuttuvat tai täydentyvät. Myös tietojärjestelmän tuotantokäyttöön tarkoitetun version tuen päättymisestä on ilmoitettava Valviralle (AsTL 30 §).

Kela ja tietoturvallisuuden arviointilaitos voivat ohjeistaa tarkemmin muutosilmoituksissa käytettävistä lomakkeista ja yhteydenottokanavista sekä siitä, voiko jo muutosilmoituksen yhteydessä toimittaa myös muita sertifiointiprosessiin tarvittavia tietoja esimerkiksi tilanteissa, joissa on selvää, että uusi yhteistestaus tai tietoturvallisuuden arviointi tarvitaan.

Mikäli tämä liite ei sisällä vastausta siihen, tarvitaanko uuden yhteistestauksen tarpeen arviointia, asiaa voi tiedustella Kelan Kanta-palvelujen tai THL:n kautta. Tietoturvallisuuden uudelleenarvioinnin tarvetta voi tiedustella arviointilaitokselta tai THL:n kautta, jos liitteessä kuvatut säännöt eivät ole sovellettavissa.

Merkittävät muutokset

Luokkaan A2 tai A3 kuuluvaan tietojärjestelmään tehtävistä merkittävistä muutoksista tulee ilmoittaa Kelaan, joka arvioi tietojärjestelmän yhteistestauksen uusimistarpeen tai tarpeen suorittaa täydentävä yhteistestaus. Luokkaan A1 kuuluvan tietojärjestelmän merkittävistä muutoksista ei tehdä muutosilmoitusta Kelaan.

Jos tietojärjestelmä siirtyy luokasta A1 tai luokasta B luokkaan A2 tai A3, Kelan kanssa käynnistetään yhteistestaus vastaavasti kuin uuden järjestelmän hakeutuessa yhteistestaukseen.

Luokkaan A1, A2 tai A3 kuuluvaan tietojärjestelmään tehtävistä merkittävistä muutoksista tulee ilmoittaa tietoturvallisuuden arviointilaitokselle, joka arvioi, onko tietojärjestelmälle tarpeen suorittaa uusi tietoturvallisuuden arviointi.

Jos tietojärjestelmä siirtyy luokasta B luokkaan A1, A2 tai A3, tietoturvallisuuden arviointilaitoksen kanssa käynnistetään tietoturvallisuuden arviointi vastaavasti kuin uuden järjestelmän hakeutuessa tietoturvallisuuden arviointiin.

Esimerkiksi alla kuvatut muutokset ovat sellaisia, jotka edellyttävät ilmoitusta Kelan Kanta-palveluihin yhteistestaustarpeen arviointia varten sekä ilmoitusta tietoturvallisuuden arviointilaitokselle, jotta arviointilaitos voi päättää tarvitaanko järjestelmälle uusi tietoturvallisuuden arviointi.

1. Järjestelmään toteutetaan toiminnallisuuksia kansallisten määrittelyjen perusteella, ja näissä määrittelyissä tai niihin liittyvässä julkaisusuunnitelmassa mainitaan, että määrittelyn käyttöönotto edellyttää uudelleentestausta tai uutta tietoturvallisuuden arviointia.

2. Järjestelmän käyttäjäkunta tai liittymismalli muuttuu olennaisesti uuden version yhteydessä, esimerkiksi ammattilaiskäyttäjien lisäksi järjestelmän käyttäjiksi tulee sote-palvelujen asiakkaita tai potilaita, tai järjestelmän käyttäjäksi tulee yksityisten palveluntuottajien lisäksi julkisia palveluntuottajia tai päinvastoin.

3. Järjestelmä liittyy Kanta-palveluun, johon se ei ole aiemmin liittynyt, esimerkiksi reseptikeskuksen lisäksi potilastiedon arkistoon, potilastiedon arkiston lisäksi sosiaalihuollon asiakastiedon arkistoon tai Omakannan omatietovarantoon, tai sosiaalihuollon asiakastiedon arkiston lisäksi potilastiedon arkistoon.

4. Järjestelmän käyttöliittymä tai toiminnallisuus uusitaan merkittävin osin tai niihin tehdään merkittäviä muutoksia. Tällaisista muutoksista on ilmoitettava, jos muutokset voivat vaikuttaa myös Kanta-palveluihin lähetettävien tai sieltä haettavien tietojen tai asiakirjojen oikeellisuuteen, Kanta-rajapintojen tai sanomarakenteiden toimivuuteen, tai tietoturvavaatimusten toteuttamistapaan.

5. Järjestelmä liitetään suoraan Kanta-palveluihin, kun se on aiemmin ollut liittyneenä Kanta-palveluihin asiakastietojen välityspalvelun tai Kanta-palveluista tietoja välittävän järjestelmän kautta.

6. Valvontaviranomainen, kuten Valvira, edellyttää järjestelmän tai sen uuden version uudelleentestaustarpeen arviointia tai arviointia siitä, tarvitaanko järjestelmälle uusi tietoturvallisuuden arviointi.

7. Tietojärjestelmän valmistaja tai tietojärjestelmäpalvelun tuottaja tekee tietoturvallisuuden arviointivaatimuksiin liittyvissä dokumentaatiojärjestelyissä tai järjestelmän kehitystyön organisoinnissa merkittäviä muutoksia (esimerkiksi merkittävä liiketoimintamuutos kuten yritysfuusio tai yrityskauppa, järjestelmän tuottaneen kehittäjätiimin vaihtuminen).

8. Järjestelmään X kohdistuvia olennaisia vaatimuksia on yhteistestattu tai todennettu tietoturvallisuuden arvioinnissa hyväksytysti järjestelmän tai tuotteen Y kautta, ja järjestelmä Y muuttuu siten, että muutos voi vaikuttaa olennaisten vaatimusten toteutumiseen järjestelmässä X.

9. Järjestelmästä löydetään merkittäviä potilas- tai asiakasturvallisuuteen liittyviä puutteita tai virheitä. Merkittävien virheiden osalta on erityisesti huolehdittava myös ilmoituksista valvontaviranomaisille (Valvira) sekä järjestelmien käyttäjille.

Merkittäviä muutoksia, jotka edellyttävät ilmoitusta Kelan Kanta-palveluihin yhteistestaustarpeen arviointia varten, mutta eivät edellytä ilmoitusta tietoturvallisuuden arviointilaitokselle ovat esimerkiksi seuraavan tyyppiset muutokset:

10. Järjestelmään tehdään muutoksia, jotka vaikuttavat Kanta-rajapintaan, järjestelmän käyttämiin Kanta-palvelupyyntöihin tai näissä käytettyihin sanoma- tai dokumenttirakenteisiin.

Merkittäviä muutoksia, jotka edellyttävät ilmoitusta tietoturvallisuuden arviointilaitokselle, mutta eivät edellytä ilmoitusta Kelan Kanta-palveluihin yhteistestaustarpeen arviointia varten ovat esimerkiksi seuraavan tyyppiset muutokset:

11. Tietojärjestelmän käyttötarkoituksen laajuus kasvaa merkittävästi esimerkiksi yksittäisestä palveluntuottajasta laajaksi alueeksi, tai tietojärjestelmän riskitaso nousee perustasolta korkean riskin tasolle järjestelmään tehtyjen muutosten tai muiden riskitasoon vaikuttavien seikkojen muuttumisen johdosta. Riskitason määrittely tehdään määräyksen 4/2021 mukaisesti.

12. Tietojärjestelmäpalvelun tuottajan vastuulla olevaan järjestelmän käyttö- tai suoritusympäristöön tehdään sellaisia merkittäviä muutoksia, jotka vaikuttavat käyttöympäristön tietoturvallisuuden olennaisten vaatimusten toteuttamiseen. Muutos voi olla esimerkiksi sellainen, jossa järjestelmä tai sen merkittävä osakomponentti siirtyy sote-palveluntuottajan tai tietojärjestelmäpalvelun tuottajan ympäristöstä ulkoiselle alusta- tai ohjelmistopalvelun tuottajalle. Ilmoitustarve ei koske hyväksytyn ja tietoturvallisuuden arvioinnin hyväksytysti läpäisseen järjestelmän asennusta uuteen asiakasympäristöön, jossa vaatimukset täytetään vastaavalla tasolla ja vastaavilla menettelyillä kuin aiemmissa käyttöympäristöissä. Uusittavissa tietoturvallisuuden arvioinneissa on kuitenkin syytä käydä läpi, onko järjestelmää asennettu sellaisiin uusiin käyttöympäristöihin, joiden riskit poikkeavat aiemmista.

13. Järjestelmästä löydetään merkittäviä tietoturvallisuuteen liittyviä puutteita tai virheitä, joiden korjaaminen on varmistettava tietoturvallisuuden arvioinnilla. Merkittävien virheiden osalta on erityisesti huolehdittava myös ilmoituksista valvontaviranomaisille (erityisesti Valvira) sekä järjestelmien käyttäjille.

Järjestelmää ei tarvitse ilmoittaa uuden tietoturvallisuuden arvioinnin tarpeen tai uuden yhteistestaustaustarpeen arviointiin seuraavissa tilanteissa. Näissäkin tilanteissa on kuitenkin huolehdittava siitä, että Valviran tietojärjestelmärekisterissä sekä Kelan Kanta-palveluissa ja tietoturvallisuuden arviointilaitoksella on ajantasaiset tiedot tuotannossa käytettävien järjestelmien tuotenimistä ja niiden valmistajista:

14. Aiemmin hyväksytysti testattuun tai tietoturvallisuuden arvioinnin hyväksytysti suorittaneeseen järjestelmään toteutetaan uusi sisältö tai toiminnallisuus, joka ei vaikuta Kanta-rajapintoihin tai tietoturvavaatimusten toteutumiseen, esimerkiksi sairaalajärjestelmään toteutetaan uusi osaston vuodepaikkojen statusnäkymä tai sosiaalihuollon asiakastietojärjestelmään toteutetaan uusi toiminnallisuus muistutteiden esittämiseen käyttäjille.

15. Järjestelmän myyntinimi tai tuotenimi muuttuu, mutta järjestelmään ei tehdä Kanta-rajapintoihin, tietoturvavaatimuksiin, tai merkittäviä toiminnallisuuteen liittyviä muutoksia. Todistus tietoturvallisuuden arvioinnista on sallittua päivittää järjestelmän uudelle tuotenimelle siten, että järjestelmän kaikkien tuotannossa olevien versioiden nimet käyvät ilmi todistuksessa ja todistuksen voimassaoloaika säilyy ennallaan.

16. Yrityksen nimi tai y-tunnus muuttuu, mutta muutoksella ei ole vaikutuksia yrityksen toteuttamiin tuotteisiin tai tietojärjestelmiin.

17. Valmistajan tai tietojärjestelmäpalvelun tuottajan yhteyshenkilö tai yhteystiedot tietoturvallisuuden arvioinnissa tai yhteistestauksessa muuttuvat.