Teknologia:

Tekniikan auditointi ja sertifiointi

Terveydenhuollon ATK-päivät 28-29.5.2013
Logomo, Turku

Ylitarkastaja Jari Knuuttila, Valvira

Valvira

Määritelmiä ja aiheeseen liittyvät lait

Auditointi, sertifiointi, sertifikaatti, tekniikka...

- Auditoinnilla selvitetään, miten organisaation laadunhallinta tai laadunvarmistus täyttävät tietyt kriteerit. Auditoinnin voi tehdä organisaatio itse (sisäinen auditointi) tai organisaation sidosryhmä, erityisesti asiakas tai ns. kolmas osapuoli.

- Sertifiointi tarkoittaa tuotteen/toiminnan ja laatujärjestelmän puolueetonta arviointia ennalta laaditun kriteeristön tai standardin avulla. Kolmannen osapuolen avulla todistetaan, että tietyt väitteet laadusta tai vaatimustenmukaisuudesta toteutuvat.

- Itsesertifiointi tarkoittaa valmistajan/toimijan itsensä suorittamaa vaatimustenmukaisuuden arviointia

- Todistus vaatimustenmukaisuudesta. Todistuksen/sertifikaatin voi antaa yrityksen johto, asiakas tai ulkopuolinen akkreditoitu (päteväksi todettu) sertifioija.

  Huom. Valmistajan antama vaatimustenmukaisuusvakuutus (Declaration of Conformity)

”Tekniikkaa” koskevat säädökset

(Tekniikka = Ohjelmistot sekä Asiakas- ja potilastietojärjestelmät)

Laitelaki

Laki (629/2010) terveydenhuollon laitteista ja tarvikkeista
(perustuen mm. direktiiviin 93/42/ETY)

Asiakastietolaki

Laki (159/2007) sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä

Sosiaali- ja terveysministeriön asetus (165/2012) terveydenhuollon valtakunnallisista tietojärjestelmäpalveluista

Luonnos (1.11.2012) asiakastietolain muuttamiseksi

Hallituksen esitys eduskunnalle laeiksi sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetun lain ja sähköisestä lääkemääräyksestä annetun lain muuttamiseksi

Säädösten keskeinen merkitys

Laitelaki

- perusta turvallisille, tehokkaille ja innovatiivisille terveydenhuollon laitteille
- vaatimukset: laitteille, niiden valmistajille, toiminnanharjoittajille, ja ammattimaisille käyttäjille
- menettelyt vaatimustenmukaisuuden arviointiin

Asiakastietolaki

- edistää sosiaali- ja terveydenhuollon asiakastietojen tietoturvallista sähköistä käsittelyä
- mahdollistaa yhtenäisen sähköisen potilastietojen käsittely- ja arkistointijärjestelmän terveydenhuollon palvelujen tuottamiseksi
- edistää potilaan tiedonsaantimahdollisuuksia

Ehdotettu asiakastietolain muutos:

- vaatimukset tietojärjestelmille: tietoturva, yhteentoimivuus ja toiminnallisuus
- vaatimukset käyttäjille
- menettelyt vaatimustenmukaisuuden arviointiin

Laki terveydenhuollon laitteista ja tarvikkeista (laitelaki) 629/2010

Käyttötarkoitus määrittelee onko ohjelmisto terveydenhuollon laite

- **Potilastietojärjestelmä**
  - Soveltuu päätöksenteon tukijärjestelmäksi potilaan diagnosoinnissa ja hoidossa

- **Potilastietojärjestelmä**
  - Soveltuu potilastietojen tallentamiseen ja arkistointiin

Hankinnan yhteydessä kannattaa tarkistaa miten valmistaja on kuvannut käyttötarkoituksen.

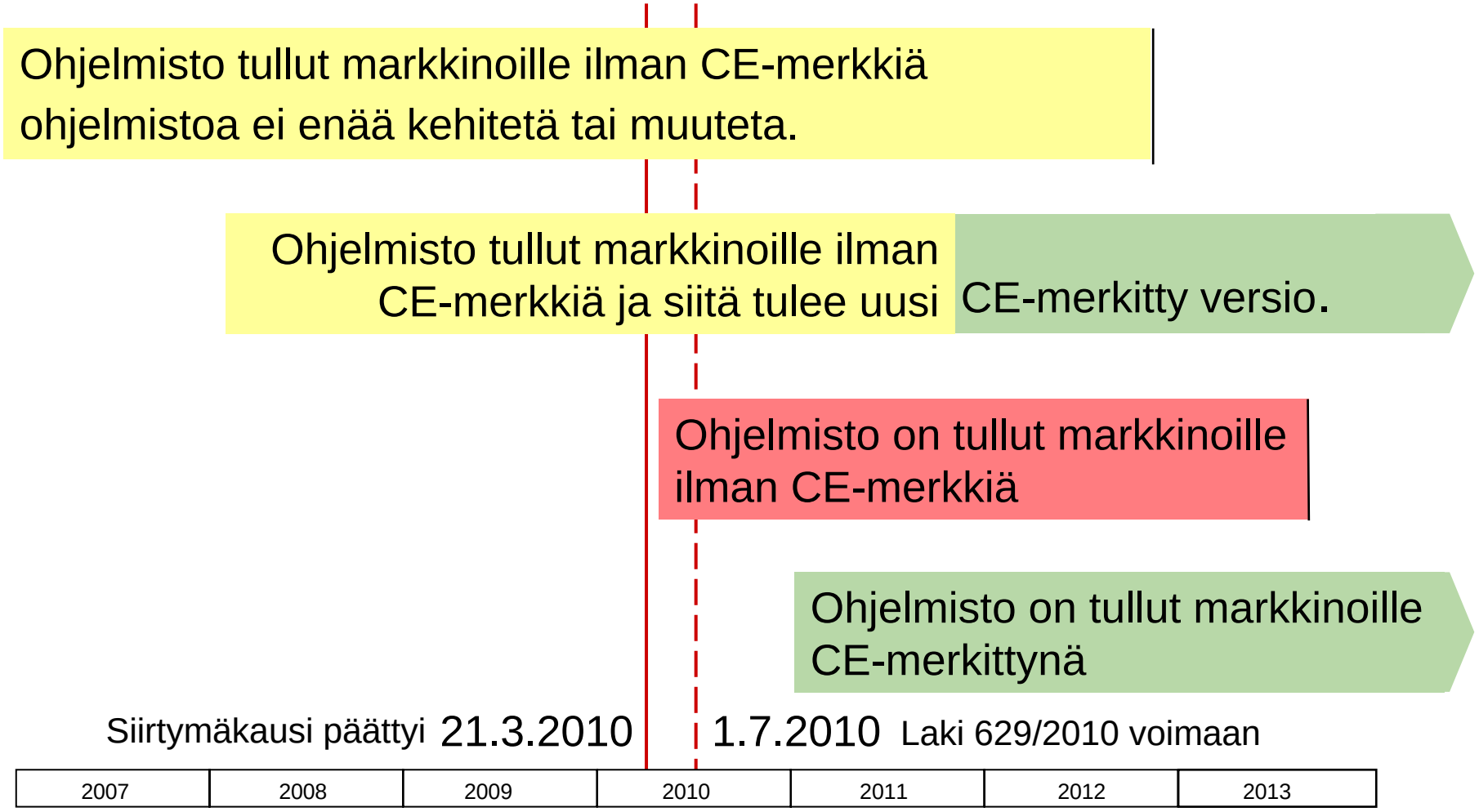
EU:n komission tulkintaohje MEDDEV 2.1/6 ohjelmistojen määrittelemiseksi ja luokittelemiseksi : http://www.valvira.fi/files/tiedostot/s/w/sw_luokitteluohje_2012-03-13.pdf

Laitelain vaatimuksia ohjelmiston valmistajalle

- Riskit tulee tunnistaa ja minimoida
- Käytettävyys on huomioitava suunnitelmallisesti
- Ohjelmistokehitys tehtävä dokumentoidun prosessin mukaisesti
- Soveltuvuus käyttötarkoituksen mukaiseen käyttöön osoitettava
- Asiakas/potilasympäristössä tapahtuvasta ohjelmistokehityksen aikaisesta koekäytöstä on ilmoitettava viranomaiselle
- Käyttö on ohjeistettava ja merkinnät laadittava
- Asiakaspalautetta on kerättävä potilasturvallisuuden vaarantavien tilanteiden tunnistamiseksi ja raportoimiseksi
- Ohjelmistossa piilevistä potilasturvallisuuden vaarantavista virheistä informoitava käyttäjiä ja virheet korjattava tarvittaessa myös käytössä oleviin tuotteisiin

Vaatimukset soveltuvat, kun ohjelmisto on luokiteltu terveydenhuollon laitteeksi.

Laitelain vaatimusten voimaantulo



Toimijoiden velvollisuuksia (L629/2010)

Valmistaja

- määrittelee ohjelmiston käyttötarkoituksen
- osoittaa vaatimustenmukaisuuden (**itsesertifiointi tai NB-sertifiointi**)
- laatii vaatimustenmukaisuusvakuutuksen
- ”kiinnittää” ohjelmistoon ja käyttöohjeisiin CE-merkin
- rekisteröi ohjelmiston Valviran laiterekisteriin
- seuraa käytön turvallisuutta ja ohjelmiston soveltuvuutta käyttötarkoituksen mukaiseen käyttöön

Ammattimainen käyttäjä

- noudattaa valmistajan käyttöohjeita
- ilmoittaa vaaratilanteista
- noudattaa valmistajan turvallisuustiedotteiden ohjeita
- noudattaa myös muita vaatimuksia (24 §)

Valvira

- tekee tarkastuksia valmistajien (ja muiden toimijoiden) tiloissa varmistaakseen, että velvoitteet on asianmukaisesti täytetty (**auditointi**)
- käsittelee ja arvioi käyttäjien ja valmistajien vaaratilanneilmoitukset
- voi kieltää käytön, rajoittaa käyttöä tai asettaa ehtoja käytölle

Ammattimaisen käyttäjän velvollisuuksia

On varmistuttava (24 §) siitä, että:

– henkilöllä, joka käyttää terveydenhuollon laitetta, on sen turvallisen käytön vaatima koulutus ja kokemus;

– laitetta käytetään valmistajan ilmoittaman käyttötarkoituksen ja -ohjeistuksen mukaisesti;

– laitteeseen kytkettynä tai välittömässä läheisyydessä olevat toiset terveydenhuollon laitteet, rakennusosat ja rakenteet, varusteet, ohjelmistot tai muut järjestelmät ja esineet eivät vaaranna laitteen suorituskykyä tai potilaan, käyttäjän tai muun henkilön terveyttä;

Seurantajärjestelmään (26 §) on kirjattava tiedot, jotka osoittavat, että ammattimainen käyttäjä on huolehtinut 24 §:ssä säädetyistä velvoitteista.

Auditointi ja sertifiointi lain 629/2010 näkökulmasta

AUDITOINTI

- Ilmoitetun laitoksen suorittama auditointi valmistajan tiloissa*
- Viranomaisen suorittama tarkastus toimijan tiloissa
- Toimijoiden sisäiset auditoinnit lakisääteisten vaatimusten täyttymisen arvioimiseksi

SERTIFOINTI*

- Ilmoitetun laitoksen (Notified Body) suorittama laatujärjestelmän ja tuotteen vaatimustenmukaisuuden arviointi

*) muut kuin luokan I laitteet

ITSESERTIFIOINTI

- Valmistajan suorittama arviointi oman tuotteen vaatimustenmukaisuudesta
- (käyttäjäorganisaation arvio laitteiden käyttäjien pätevyydestä)

TODISTUS

- Ilmoitetun laitoksen todistus laatujärjestelmän arvioinnista
- Valmistajan antama vaatimustenmukaisuusvakuutus
- Todistus käyttäjän laitekoulutuksesta tai pätevyydestä käyttää laitetta

Ehdotus asiakastietolain muuttamisesta (1.11.2012)

Vaatimustenmukaisuuden arviointi

Asiakastietolain (ehdotetun muutoksen mukaisesti) nojalla tullaan antamaan asiakas- ja potilastietojärjestelmille olennaiset vaatimukset vastaavasti kuin laitelaissa.

Vaatimuksilla varmistetaan asiakas- ja potilastietojen asianmukainen käsittelyn tietosuoja ja tietoturvallisuus. Vaatimukset voivat koskea myös yhteentoimivuutta ja toiminnallisuutta.

Kanta-järjestelmään liittyviltä tietojärjestelmiltä tullaan edellyttämään kolmannen osapuolen sertifiointia tietosuojan ja tietoturvan osalta. Muilta osin valmistaja vastaa vaatimustenmukaisuuden osoittamisesta (itsesertifiointi).

Lisäksi Kanta-järjestelmään liitettäville asiakas- ja potilastietojärjestelmille tulee tehdä KELAn yhteistestaus yhteentoimivuuden varmistamiseksi.

Vaatimukset palvelun antajalle

1) henkilöillä, jotka käyttävät tietojärjestelmiä, on niiden käytön vaatima koulutus ja kokemus;

2) tietojärjestelmien yhteydessä on saatavilla niiden asianmukaisen käytön kannalta tarpeelliset käyttöohjeet;

3) tietojärjestelmiä käytetään valmistajan antaman ohjeistuksen mukaisesti;

4) tietojärjestelmiä ylläpidetään ja päivitetään valmistajan ohjeistuksen mukaisesti;

5) käyttöympäristö soveltuu tietojärjestelmien asianmukaiseen sekä tietoturvan ja tietosuojan varmistavaan käyttöön;

6) tietojärjestelmiin liitetyt muut tietojärjestelmät tai muut järjestelmät eivät vaaranna tietojärjestelmien suorituskykyä eivätkä niiden tietoturva- tai tietosuojaominaisuuksia; sekä

7) tietojärjestelmiä asentaa, ylläpitää ja päivittää vain henkilö, jolla on siihen tarvittava ammattitaito ja asiantuntemus.

Omavalvonta tukee turvallista käyttöä

Vaatimustenmukainen ja asiakasvaatimukset täyttävä tietojärjestelmä on lähtökohta tehokkaalle ja turvalliselle asiakas- ja potilastietojen käsittelylle.

Sosiaalihuollon ja terveydenhuollon palvelujen antajan on laadittava

- tietoturvaan ja tietosuojaan sekä
- tietojärjestelmien käyttöön

liittyvä omavalvontasuunnitelma.

Siinä on selvittävä miten palvelun antajalle asetettujen vaatimusten (ks. edellä) täyttyminen varmistetaan.

Kanta-palvelujen käyttäjäksi liittyneen, on selvitettävä myös, miten tietoturvallisen käytön edellyttämät vaatimukset on varmistettu.

Vaaratilanteista ja poikkeamista ilmoittaminen

Jos sosiaali- tai terveydenhuollon palvelujen antaja havaitsee, että tietojärjestelmän olennaisten vaatimusten toteutumisessa on merkittäviä poikkeamia, on palvelujen antajan ilmoitettava siitä tietojärjestelmän valmistajalle.

Jos poikkeama voi aiheuttaa merkittävän riskin potilasturvallisuudelle, tietoturvalle tai tietosuojalle, on siitä ilmoitettava myös Sosiaali- ja terveysalan lupa- ja valvontavirastolle.

Auditointi ja sertifiointi asiakastietolain (muutosehdotuksen) näkökulmasta

AUDITOINTI / ARVIOINTI

- Tietoturvallisuuden arviointilaitoksen suorittama auditointi valmistajan tiloissa
- Toimijoiden auditoinnit asetettujen vaatimusten (STM auditointivaatimukset?) täyttymisen arvioimiseksi
- KELAn yhteistestaus yhteentoimivuuden varmistamiseksi
- Viranomaisen suorittama tarkastus toimijan tiloissa

SERTIFOINTI

- Tietoturvallisuuden arviointilaitoksen suorittama vaatimustenmukaisuuden sertifiointi

ITSESERTIFIOINTI

- Valmistajan suorittama arviointi tietojärjestelmän vaatimustenmukaisuudesta
- (käyttäjäorganisaation suorittama käyttäjien pätevyyden arviointi)

TODISTUS

- Tietoturvallisuuden arviointilaitoksen todistus vaatimustenmukaisuudesta
- Valmistajan antama vaatimustenmukaisuusvakuutus
- Organisaation vakuutus vaatimusten täyttymisestä

Lisätietoja

Laki terveydenhuollon laitteista ja tarvikkeista
http://www.finlex.fi/fi/laki/alkup/2010/20100629

Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä
http://www.finlex.fi/fi/laki/ajantasa/2007/20070159

Luonnos hallituksen esitykseksi asiakastietolaiksi ym.
http://www.stm.fi/vireilla/lausuntopyynnot

Asiakastietolain olennaiset vaatimukset
(tullaan määrittelemään myöhemmin, lähtökohtana nykyiset auditointivaatimukset)
http://www.kanta.fi/fi/web/ammattilaisille/57

etunimi.sukunimi@valvira.fi
p. 0295 209 111