Haaga-Helia
ammattikorkeakoulu Oy

Lääkintälaitteiden tietoturvan katselmointi laitteiden vastaanottovaiheessa

Tuija Kuparinen-Koho

Opinnäytetyö
Tietojenkäsittelyn koulutusohjelma
2017

Haaga-Helia
University of Applied Sciences

Tiivistelmä

27.5.2017

Tekijä
Tuija Kuparinen-Koho

Koulutusohjelma
Tietojenkäsittely

Opinnäytetyön otsikko
Lääkintälaitteiden tietoturvan katselmointi laitteiden vastaanottovaiheessa

Sivu- ja liitesivumäärä
45 + 5 (14)

Työssä tutkittiin lääkintälaitteiden tietoturvan toteuttamista lääkintälaitteen vastaanottotarkastuksessa. Työssä pyrittiin tuottamaan tietoa lääkintälaitteen käyttöönoton valmisteluun, jotta tietoturvan toteutumiseen vaikuttavat tekijät voidaan huomioida vastaanottovaiheessa. Tällä pyrittiin varmistamaan laitteen tietoturvallisen käytön edellytykset.

Työn toteutustapana oli aineistotutkimus ja työ perustui lähdemateriaalin analyyttiselle käytölle. Tavoitteena oli tuottaa käyttöönottosuunnittelua tukeva tarkistuslistamalli lähdemateriaalia tarkastelemalla.

Tässä tutkimuksessa ei toteutettu evaluointivaihetta eli ei arvioitu tarkistuslistan toimivuutta testitapauksella. Tutkimus palveli tutkijan omaa oppimista reflektion avulla, mutta sillä oli myös tarkoitus herättää keskustelua ja toimintaa lääkinnällisten laitteiden tietoturvan edistämiseksi sairaalaorganisaatiossa.

Kyberturvallisuus, tietoturva ja lääkinnälliset laitteet ovat kukin käsitteinä ja ilmiöinä sisällöllisesti laajat, joten tässä opinnäytetyössä keskityttiin tarkastelemaan lääkintälaitteiden tietoturvan huomioimista lääkintälaitteen vastaanottotarkastuksen yhteydessä. Laitteiden tietoturvallinen käyttäminen mahdollistaa potilasturvallisuuden ja potilaiden tietosuojan toteutumisen.

Tietoturvan huomiointi lääkintälaitteiden käyttöönotossa vaatii suunnitelmallista työpanosta ja eri sidosryhmien yhteistyötä. Tarkistuslista auttaa tietoturvavaateiden huomioinnissa ja tarvittavien jatkotoimenpiteiden suunnittelussa.

Työ sisältää luottamuksellisia osia eli esimerkkiorganisaation vastaanottoprosessikuvauksen sekä hankintavaiheen tietoturvalomakkeen. Näitä ei ole työn julkaistu työn julkisessa versiossa.

Opinnäytetyön tuloksena syntyi tarkistuslistaluonnos, jota voidaan käyttää mallina ja kehittää edelleen lääkintälaitteita käyttävissä ja niitä vastaanottavissa organisaatioissa. Tarkistuslistan käyttämistä ja sen kehittämistä edesauttaa sujuva moniammatillinen yhteistyö organisaation eri toimijoiden ja vastuutahojen välillä.

Asiasanat
Lääkintälaite, lääkintätekniikka, vastaanottotarkastus, tietoturva, kyberturvallisuus, riskienhallinta.

Sisällys

1 Johdanto

Viestintäviraston tammikuussa 2016 julkaistun Kyberturvallisuuskeskuksen Terveydenhuollon kyberuhkia –raportin mukaan terveydenhuollossa käytettyihin lääketieteellisiin laitteisiin liittyy merkittäviä kyberuhkia. Uhat voivat todentua lauenneiksi riskeiksi laitteisiin liittyvien ohjelmistorajapintojen ja verkkopalveluiden vuoksi.

Lääkintälaitteiden hallinnasta sairaanhoito- ja terveydenhuolto-organisaatioissa vastaa usein lääkintätekniikan yksikkö tai lääkintälaitehuolto – ei tietohallinto tai tietotekniikkayksikkö. Tietohallinto vastaa käyttöpalveluista, mutta laitteiden huolto- ja ylläpitovastuu kuuluu lääketieteellisen tekniikan tai sairaalatekniikan yksiköille. Tällöin kyberturvallisuudesta huolehtiminen ja tietoturvariskien arviointi saattaa jäädä riittämättömälle huomiolle, ellei asiantuntijuuksia voida hyödyntää poikkihallinnollisesti eri yksiköiden välillä.

Viestintäviraston 2015 Suomessa tehdyssä kartoituksessa löydettiin tuhansia kiinteistöautomaatioon[1] liittyviä suojaamattomia päätelaitteita, jolloin niitä on todennäköisesti myös terveydenhuollon organisaatioiden käytössä. Sairaaloissa käytetään erilaisia digitaalisia järjestelmiä, jotka voidaan käsittää automaatiojärjestelmiksi. Kyberturvallisuuskeskuksen raportin mukaan monet automaatiolaitteet ja -järjestelmät ovat voitu toteuttaa tietoturvattomasti.

Sosiaali- ja terveysalan lupa- ja valvontavirasto eli Valvira hoitaa Suomessa terveydenhuollon laitteista ja tarvikkeista säädetyn lain (629/2010) mukaisia laitteiden valmistajia, tuotteita, kliinisiä laitetutkimuksia, ammattimaisen käytön valvontaa ja markkinavalvontaa koskevia tehtäviä – samoin kuin terveydenhuollon tietojärjestelmien valvontaa ja niitä koskevan rekisterin ylläpitämistä. Valvirassa valmistellaan tällä hetkellä uuden lupa-, ohjaus- ja valvontaviraston tehtävien määritystä, sillä hyvinvointialan kasvaessa terveydenhuollossa tullaan hyödyntämään yhä enemmän ohjelmistoja, robotiikkaa sekä tietojärjestelmiin kytkeytyviä laitteita ja tarvikkeita. Näiden hallittavuuden edistäminen tulee olemaan keskeinen asia myös viranomaistyötehtävissä.

Lain mukaan markkinoille saatetun terveydenhuollon laitteen saa ottaa käyttöön, kun se asianmukaisesti toimitettuna, asennettuna, huollettuna ja käyttötarkoituksensa mukaan käytettynä täyttää laissa kuvatut vaatimukset. Turvallisen ammattimaisen käytön vaati-

[1] Kiinteistöautomaatio-käsite on korvattu rakennusautomaatiolla, yläterminä käytettävä automaatio kuuluu atk:n, tietotekniikan ja tietojenkäsittelyn ryhmään YSA:ssa. Lähde: https://finto.fi/ysa/fi/page/Y94818

muksia kuvataan 24 § laitetta käyttävän henkilön koulutuksena ja osaamisena, toimituksessa mukana olevina käyttöohjeina sekä käyttönä valmistajan ohjeiden mukaisesti ja käyttötarkoitukseen sopivana. Lisäksi laki määrää ammattimaisen käyttäjän varmistumaan siitä, että laite säädetään, ylläpidetään ja huolletaan valmistajan ohjeistuksen mukaisesti ja muutoin asianmukaisesti. Käyttöpaikan tulee soveltua laitteen turvalliseen käyttöön ja laitteeseen kytkettynä tai välittömässä läheisyydessä olevat toiset terveydenhuollon laitteet, rakennusosat ja rakenteet, varusteet, ohjelmistot tai muut järjestelmät ja esineet eivät saa vaarantaa laitteen suorituskykyä tai potilaan, käyttäjän tai muun henkilön terveyttä. Laitteen tulee asentaa, huoltaa ja korjata vain henkilö, jolla on tarvittava ammattitaito ja asiantuntemus.

Voimaan tultuaan laki herätti keskustelua, sillä sairaalaorganisaatioiden edustajat ilmaisivat huolensa kyvystään noudattaa lain vaatimuksia kaikilta osin. Osaltaan tähän vaikuttaa se, että lääkintälaitteiden tarkastusten taso käyttöorganisaatiossa vaihtelee edelleen ja laitteiden tietoturvan koetaan olevan vaikeasti arvioitavissa ammattimaisen käyttäjän näkökulmasta. Lisäksi laki tuo velvoitteita laitevalmistukseen, joka aiheuttaa epävarmuutta lain tulkintaan toiminnanharjoittajan vastuista oman laitevalmistuksen rajoihin ja laitekokoonpanoihin liittyen esimerkiksi endoskopiatorneihin, lisämonitoreihin ja itse tuotettujen sovelluksiin. (Laitinen 2014.)

Tämän opinnäytetyön tavoitteena on tuottaa kyberturvallisuutta tukeva työkalu lääkintälaitteen vastaanottamiseen tietoturvanäkökulmasta. Työkalu tuotetaan tarkistuslistana, jota käyttämällä toteutetaan ennakoivaa tietoturvaa. Ennakoinnilla pyritään varautumaan ja ehkäisemään mahdolliset häiriöt laitteen käyttöönottoa suunniteltaessa ja valmisteltaessa. Tarkistuslistan avulla voidaan kartoittaa huomioitavat asiat ja reagoida puutteisiin sekä varmistaa tarvittavien toimenpiteiden valmistelun aloitus. Tässä opinnäytetyössä ei tehdä tarkistuslistan laadullista arviointia. Käyttöön soveltuvuuden testaus eli tarkistuslistan validointi jätetään myös jatkotutkimusaiheeksi.

Työssä ei myöskään kehitetä vastaanottotarkastuksen työprosessia eikä lääkintätekniikan toimintaa. Kokonaisturvallisuutta edistävien toimintamallien ja työmenetelmien kehittäminen palvelu- tai henkilöstöhallinnollisesta näkökulmasta soveltuu jatkotutkimusaiheeksi. Vaikka työ sivuaa riskienhallintaa, tulee sitä tarkastella omana aihealueinaan jatkotutkimuksissa. Työllä on sidos myös lääkintälaitteiden vaatimustenmukaisuuden osoittamiseen, mutta tämä rajataan laajuuden vuoksi työn ulkopuolelle. Vaatimustenmukaisuuden selvittäminen edellyttää markkinamekanismien, sääntelyn ja ohjauksen tarkkaa läpikäyntiä lakeineen, suosituksineen, direktiiveineen ja standardeineen. Työn ulkopuolelle jää myös

lääkintälaitteen tuottaman kliinisen hyödyn ja vastaavasti sen käytön aiheuttaman kliinisen riskin arviointi.

Tutkimuskysymyksiä on kaksi. Ensimmäisenä selvitetään, millaisia tietoturvanäkökulmia lääkintälaitteita vastaanotettaessa ja käyttäessä tulee huomioida. Toiseksi selvitetään, mitä asiakokonaisuuksia tarkistuslista voi sisältää eli mitä sisältöjä listaan voidaan upottaa, jotta sen avulla saadaan tuotettua tietoturvaan liittyvää tietoa käyttöönoton suunnitteluun ja valmistelutoimenpiteisiin.

Tässä työssä lääkintälaitteella tarkoitetaan yksinään tai yhdistelmänä toimivaa laitetta ja sen ohjelmistoa, jota käytetään potilaan fysiologisen toiminnan tutkimiseen, seurantaan tai hoitoon. Lääkintätekniikalla tarkoitetaan toimialaa, joka omana palveluyksikkönään vastaa lääkinnällisten laitteiden teknisestä hallinnasta. Vastaanottotarkastuksella tarkoitetaan niitä katselmointitoimenpiteitä, joilla lääkintätekniseen yksikköön toimittajalta saapunut laite liitetään seurantaan ja todennetaan tekniseltä käyttövalmiudeltaan turvalliseksi (rekisteröinti, turvallisuusmittaukset). Tietoturvalla tarkoitetaan niitä tiedon laadun, eheyden ja koskemattomuuden takaavia teknisiä ja hallinnollisia toimenpiteitä, joilla henkilöiden (rekisteröidyn; potilaan) yksityisyyden suojaamiseen ja oikeuksien turvaamiseen pyritään. Kyberturvallisuudella tarkoitetaan tavoitetilaa, jossa sähköisessä muodossa olevan informaation (tiedon) käsittelyyn tarkoitettuun toimintaympäristöön voidaan luottaa ja sen toiminta turvataan. Riskienhallinta on prosessi, jossa riskit ja niiltä suojattavat kohteet tunnistetaan, käsitellään, määritellään riski- ja suojaustasot sekä luottamuksellisuus-, eheys- ja käytettävyysvaatimukset, seurataan sekä katselmoidaan, jotta toimintaan vaikuttavat riskitekijät saadaan arvioitua ja niiden hallintatoimet toteutettua.

2 Lääkintälaitteissa huomioitavat turvallisuuden osa-alueet

Lääkintälaitteiden ja -järjestelmien tietoturvaa koskevat vaatimukset tulee lähtökohtaisesti määritellä osana organisaation koko tietojärjestelmäympäristöä ja tietojärjestelmiä koskevaa kokonaisratkaisua. Tietoturvan on katettava kaikki lääkintälaitejärjestelmän käyttämät komponentit, ohjelmistot ja laiteyhdistelmät osana kokonaistoteutusta. (Pöyhönen & Kylmälä 2004.)

Euroopan unionin neuvoston 22.2.2017 kannanotossa 10728/16 lääkinnällisten laitteiden asetuksiin kuvataan liitteessä 1 yleisiä turvallisuus- ja suorituskykyvaatimuksia. Kohdassa 17 ja sen alakohdassa 17.1. esitetään vaatimuksia ohjelmoitavien elektronisten järjestelmien suunnitteluun. Laitteet, joihin sisältyy ohjelmoitavia elektronisia järjestelmiä (kuten ohjelmistot tai laitteiksi käsitettävät ohjelmistot) on suunniteltava siten, että varmistetaan toistettavuus, luotettavuus ja suorituskyky laitteiden suunnitellun käytön mukaisesti. Lisäksi alakohdassa 17.2. mainitaan, että ohjelmistot on suunniteltava ja valmistettava alan viimeisen kehityksen mukaisesti ottaen huomioon kehityskaareen ja riskinhallintaan liittyvät periaatteet sisältäen tietoturvallisuuden, todentamisen ja validoinnin. Alakohdan 17.4. mukaan valmistaja velvoitetaan esittämään laitteistoja, tietoteknisiä verkko-ominaisuuksia ja tietoteknisiä turvatoimenpiteitä (ml. luvattomalta käytöltä suojaaminen) koskevat vähimmäisvaatimukset, jotka ovat tarpeen ohjelmiston käyttämiseksi käyttötarkoitustaan vastaavalla tavalla.

Lääkintälaitteiden tietoturvallisen vastaanottotarkastuksen kannalta merkittävimmät turvallisuuden osa-alueet ovat laitteisto-, ohjelmisto-, tietoaineisto-, tietoliikenne- ja käyttöturvallisuus Vahti-ohjeiden tietoturvallisuuden osa-alueiden ryhmittelyn ja Valtionhallinnon tietoturvakäsitteistön (4/2004) sekä Valtionhallinnon tietoturvasanaston 8/2008 mukaisesti jaoteltuna. Myös henkilöstöturvallisuudella on oleellinen merkitys erityisesti lääkintälaitteen käyttövaiheessa, mutta myös vastaanottotarkastusvaiheessa. Henkilöstöturvallisuuden voidaan katsoa ohjaavan lääkintälaitteen vastaanottotarkastusta siten, että sen avulla vaikutetaan vastaanottotarkastuksen työsuoritukseen ja mahdollistetaan tekijöille riittävät edellytykset toimia.

Henkilöstöturvallisuuden tavoitteena on työntekijän tietoon kohdistuvan virheellisen vaikutuksen tai toiminnan estäminen. Riskit voivat liittyä esimerkiksi työntekijän asenteisiin (esim. välinpitämättömyys tietoturvaa kohtaan), liian suuriin käyttöoikeuksiin ja puutteelliseen hallintakykyyn (osaamiseen). Työntekijät saattavat olla haluttomia käymään läpi turvamenetelmiä tai käyttämään turvaratkaisuja. Laitteita, järjestelmiä ja verkkoja käyttävillä työntekijöillä voi olla erilainen asennoituminen tai näkemys tietoturvasta verrattuna niiden

fyysisistä palveluista vastaaviin henkilöihin ja työyksiköihin. (Vahtiohje.fi Henkilöstöturvallisuus; Valtiovarainministeriö 8/2008.)

Johto ja IT-palveluista vastaavat määrittelevät tietoturvastrategian, jonka pohjalta hyvät työmenetelmät muodostetaan. Asianmukaiset työmenetelmät ovat osa käytön turvallisuutta, joka sisältää järjestelmien ja ohjelmistojen osaamisen hallinnan ja käytön hallinnan. Päivittäisessä toiminnassa käyttöturvallisuus ilmenee henkilöstön käytön osaamisena, joka on syntynyt saadun koulutuksen ja kouluttautumisen myötä sekä oikeutettuna käyttönä. Henkilöstöturvallisuuden perustan muodostavat osaavat ja sitoutuneet työntekijät, joille tietoturvaan liittyvät vastuut ja tehtävät ovat kuvattu heidän toimenkuvissaan. (vahtiohje.fi Käyttöturvallisuus; Valtiovarainministeriö 8/2008.)

Vahti-ohjeistuksen ja tietoturvakäsitteistön mukaan **laitteistoturvallisuudella** tarkoitetaan laitteistojen suojausta, asennusta, ylläpitoa ja poistoa sekä niihin liittyvää hallinnointia, jossa määritellään laitteiden omistaja ja turvaluokka sekä laitteiden valvonta ja niiden kapasiteettien suunnittelu. Laitteistoturvallisuudella turvataan laitteiston elinkaarta, johon myös kuuluvat asennuksen, takuun ja ylläpidon lisäksi erilaiset tukipalvelut ja -sopimukset sekä laitteiston turvallinen poisto elinkaaren lopussa. (Vahtiohje.fi Laitteistoturvallisuus; Valtiovarainministeriö 8/2008.)

Tietoturvallisuuden toteuttamiseksi tarkastelu kohdistuu tietojenkäsittely- ja tietoliikennelaitteiden käytettävyyteen, toimivuuteen, kokoonpanojen määrittelyyn ja pääsynvalvontaan sekä varaosien ja tarvikkeiden saatavuuteen. (Vahtiohje.fi Laitteistoturvallisuus; Valtiovarainministeriö 8/2008.)

Ohjelmistoturvallisuuteen kuuluvat käyttöjärjestelmiin ja muihin ohjelmistoihin kohdistuvat toimet, esimerkiksi ohjelmistojen tunnistamis-, eristämis-, pääsynvalvonta- ja varmistusmenettelyt, tarkkailu- ja paljastustoimet, lokimenettelyt ja laadunvarmistus sekä ohjelmistojen ylläpitoon ja päivitykseen liittyvät toimet tietoturvallisuuden parantamiseksi. (Vahtiohje.fi Ohjelmistoturvallisuus; Valtiovarainministeriö 8/2008.)

Lääkintälaitteiden voidaan tulkita kuuluvan sulautettuihin tai automaatiojärjestelmiin. Ne sisältävät laite- ja sovellusohjelmiensa lisäksi usein myös rajapintoja keskitettyihin järjestelmiin. Mm. pääsynhallinnan toteuttamismahdollisuudet ovat riippuvaisia laitetyypistä ja laitteen käyttötarkoituksesta.

Tietoaineistoturvallisuuden mahdollistaminen edellyttää toimia asiakirjojen, tiedostojen ja muiden tietoaineistojen käytettävyyden, eheyden ja luottamuksellisuuden ylläpitämiseksi. Toimet voivat olla esimerkiksi tietoaineistojen luettelointia ja luokitusta sekä tietovälineiden ohjeistettua hallintaa, käsittelyä, säilytystä ja hävittämistä. (Vahtiohje.fi Tietoaineistoturvallisuus; Valtiovarainministeriö 8/2008.)

Laitetyypistä ja käyttötarkoituksesta riippuen lääkintälaitteissa voi olla ja niihin voi muodostua potilas- ja diagnostisia tietoja sisältäviä tietokantoja. Näiden tunnistaminen ja käsittely on merkityksellistä tietoaineiston turvallisuuden varmistamiseksi.

Tietoliikenneturvallisuus toteutetaan toimenpiteillä, jotka kohdistuvat laitteistojen ja siirtoyhteyksien ylläpitoon ja niiden kokoonpanojen hallintaan, verkonhallintaan, pääsynvalvontaan, tietoliikenteen käytön valvontaan ja tarkkailuun, ongelmatilanteiden raportointiin ja selvittämiseen, viestinnän varmistamiseen ja salaukseen sekä tietoliikenneohjelmien testaukseen ja hyväksymiseen. (Vahtiohje.fi Tietoliikenneturvallisuus; Valtiovarainministeriö 8/2008.)

Lääkintälaitteet voivat toimia erilaisissa käyttöympäristöissä, joiden turvallisuuden taso tulee huomioida. Laitteet muodostavat tietoliikenneyhteyksiä eri tekniikoilla sisä- tai julkiseen verkkoon ja käyttävät erilaisia medioita.

Käyttöturvallisuus tarkoittaa järjestelmien turvallisen käytön periaatteita, tapahtumien valvontaa ja jatkuvuuden turvaamista. Se sisältää tietotekniikan turvallisen käytön vaatimien toimintaolosuhteiden luomisen ja ylläpidon. Käyttäjiä ja laitteiden tilaa sekä käyttöä valvotaan järjestelmällisesti. Kehitys-testaus-tuotanto-elinkaari on dokumentoitu. Käytettävyysvaatimukset on luotu ja ne toimivat pohjana laitteen laatua ja sen käytön laatua tarkasteltaessa. Käyttöturvallisuuden taso perustuu käytettävien tietojen luokitukseen. (Vahtiohje.fi Käyttöturvallisuus; Valtiovarainministeriö 8/2008.)

3 Lääkintälaitteiden katselmointeja ja vastaanottotarkastuksia suorittavat tahot

Lääkelaitoksen voimassa olevassa julkaisusarjassa 1/2004 lääkintälaitejärjestelmien turvallisuudesta kuvataan vastaanottotarkastuksen tarkoitukseksi terveydenhuollon yksikössä käyttöön otettavien lääkintälaitteiden ja laitejärjestelmien vaatimustenmukaisuuden ja turvallisuuden valvonnan, tilausten ja toimitusten yhdenmukaisuuden todentamisen sekä vastuuhenkilöiden määrittelemisen laitteen ja järjestelmän myöhempää käyttöä varten. Vastaanottotarkastus tulee suorittaa siten, että sillä kyetään varmistamaan laitteiden ja järjestelmien oikea ja turvallinen käyttö.

Terveydenhuollon laitteista ja tarvikkeista määräävän lain 629/2010 24 § kohtien 4-7 mukaan lääkintälaitteen tulee asentaa, huoltaa ja korjata tarvittavan ammattitaidon ja asiantuntemuksen omaava henkilö. Laite tulee säätää, ylläpitää ja huoltaa valmistajan ohjeistusten mukaisesti. Myös laitteen sijoituspaikan soveltuvuudesta tulee varmistua käyttöturvallisuuden kannalta. Lisäksi tulee estää laitteen suorituskyvyn vaarantuminen sekä potilaan, käyttäjän tai muiden henkilöiden terveyden vaarantuminen laitteeseen kytkettynä tai sen välittömässä läheisyydessä olevien muiden laitteiden, rakennusosien ja rakenteiden, varusteiden, ohjelmistojen tai muiden järjestelmien ja esineiden vuoksi.

Tämä edellyttää lääkintälaitteiden hankintoja, katselmointeja ja vastaanottotarkastuksia suorittavilta organisaatiotahoilta oman henkilöstön ammattitaidosta ja pätevyydestä huolehtimista. Laitevalmistajien ohjeiden kirjaimellisen noudattamisen tulee olla kattavaa asennuksen ja ylläpidon aikana. Laitteet tulee liittää muihin järjestelmiin valmistajien ohjeistukset huomioiden. Laitteiden käyttöpaikkoihin tulee kohdistaa tarvittavia suojaustoimenpiteitä. (Vainiola 2016; Nihtinen 2016.)

Terveydenhuollon laitteista ja tarvikkeista määräävän lain 26 § edellyttää ammattimaisia käyttäjiä eli organisaatioita nimeämään vastuuhenkilön, joka vastaa siitä, että käyttäjän toiminnassa noudatetaan lakia ja sen nojalla annettuja säännöksiä ja määräyksiä. Laissa ei määritetä vastuuhenkilön koulutusta tai ammattiasemaa. Vastuuhenkilön tehtäviin kuluu lakia mukailtavien ohjeiden ja määräysten antaminen sekä organisaation velvoittaminen noudattamaan niitä. Lisäksi hänen tulee varmistaa tehtävävastuut sekä yhdenmukaiset menettelytavat organisaatiossa.

Sairaanhoitopiireissä lääkintälaitteiden teknisestä toimivuudesta vastaa lääkintätekniikan toimiala. Lääkintätekniikan yksiköt kuuluvat organisaatiohierarkisesti teknisiin tukipalveluihin, joita tuotetaan omien vastuuyksikköjen lisäksi liikelaitosmuotoisesti tai alihankintaso-

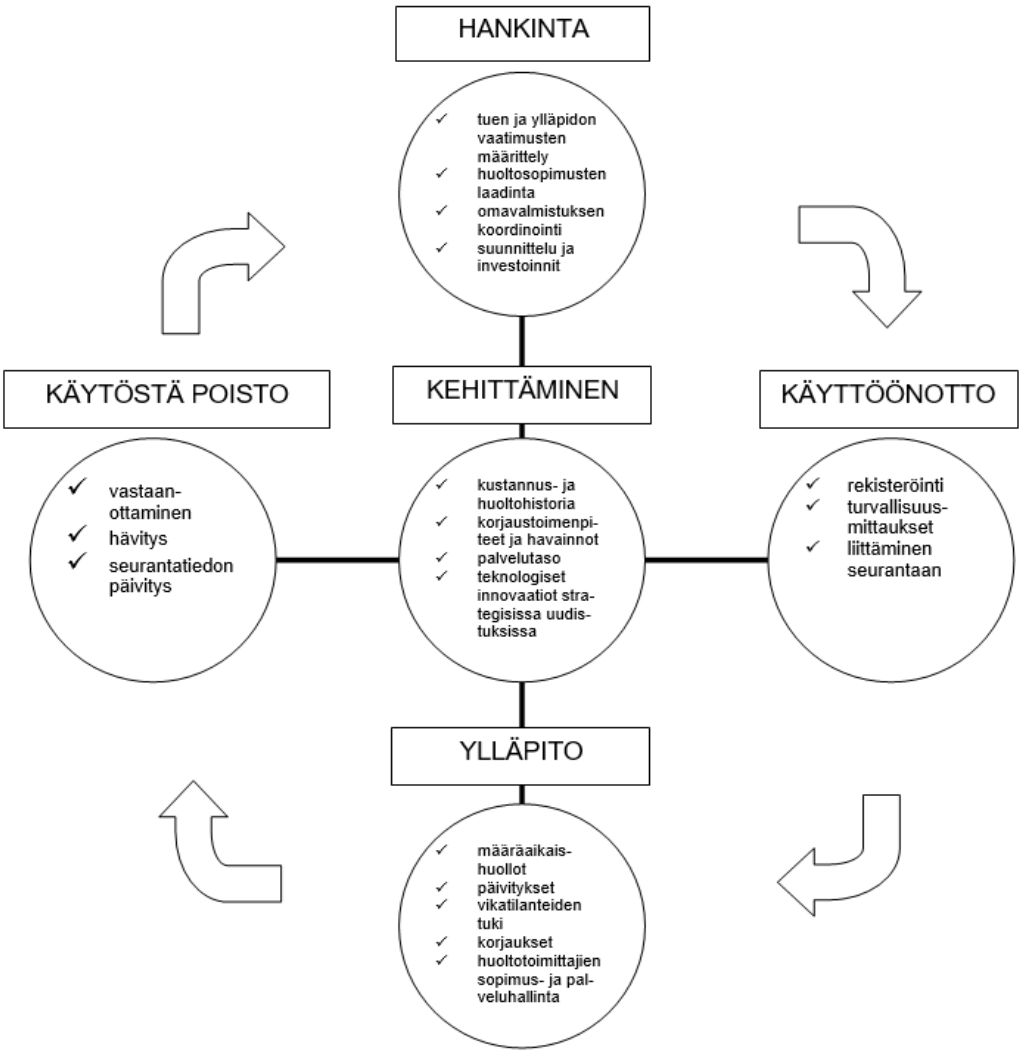
pimuksilla. Lääkintäteknisiä huolto-, korjaus- ja ylläpitopalveluita tuotetaan esimerkiksi anestesiaan ja mekaniikkaan, apuvälineisiin, ATK-laitteisiin, elektroniikkaan, laboratorioon, radiologiaan, sädehoitoon ja muihin sairaalalaitteisiin. Lisäpalveluita voidaan tuottaa mm. lääketieteelliseen kuvaukseen. (PPSHP Lääkintätekniikka; Kastek Oy palvelut; HUS Lääkintätekniikka.)

Asiakkaina ovat yksikön toimintasäännön tai yhtiöjärjestyksen mukaisesti sairaanhoitopiirin yksiköt, liikelaitokset ja yritykset sekä alueen kunnat tai kaupungit ja yksityiset toimijat.

Laboratorion ja kuvantamisen tukipalvelujen ammattihenkilöt, kuten esim. ylifyysikot voidaan nimetä tietyn lääkintälaiteen – mm. EKG-rekisteröintilaitteen – vastuukäyttäjiksi. Lääkintätekniikassa sairaalainsinöörin ja huoltomestarin työroolit ovat merkittäviä toimijoita lääkintälaitteiden hallinnassa. Lääkintälaitteista vastaavia tahoja ovat myös erilaiset laitteiden huoltopalveluja tarjoavat alihankkijat sekä ICT-palveluja tarjoavat toimittajat.

3.1.1 Lääkintätekniset asiantuntijapalvelut

Lääkintälaitteisiin kohdistuvien teknisten asiantuntijapalvelujen sisältöä voidaan tarkastella elinkaariajattelun mukaisesti (kuvio 1).



Kuvio 1. Lääkintälaitteiden hallinnan tehtäviä (mukaillen PPSHP, KASTEK, HUS)

Lääkintätekniikan asiantuntijapalveluita voidaan hyödyntää kehityshankkeiden suunnitteluvaiheessa, kun tarvitaan tietämystä uusista teknologioista sekä ajantasaista tietoa sovellettavista standardeista, säännöistä ja normeista. Hankintavalmisteluissa asiantuntemuskokemus on käytettävissä vaatimusten määrittelyyn. Kliinistä käyttöä valmisteltaessa suoritetaan tarvittavat turvallisuusmittaukset ja vastaanottotarkastus. Rekisteröinnillä lääkintälaite liitetään lakisääteisen seurannan piiriin. Laitteiden käyttövarmuus ja turvallisuus taataan määräaikaishuolloilla ja päivityksillä, joiden toteutuminen varmistetaan sopimusten ja palvelujen hallinnan avulla. Huollot, kalibroinnit ja korjaukset dokumentoidaan seurantajärjestelmään. Lääkintätekniikan tehtäviin kuuluu myös tukea laitteiden käyttäjiä häiriö- ja vikatilanteissa. Käytön loppumisen tai käytöstä luopumisen vaiheessa laitteet kootaan ja vastaanotetaan poistomenettelyä varten ja tilanne päivitetään seurantaan. (PPSHP Lääkintätekniikka; Kastek Oy palvelut; HUS Lääkintätekniikka.)

3.2 Seurantajärjestelmä

Terveydenhuollon laitteista ja tarvikkeista määräävän lain 629/2010 26 § mukaan seurantajärjestelmän käyttämisellä edistetään organisaation laiteturvallisuutta. Järjestelmä toimii myös ammattimaisen käytön vastuuhenkilön työkaluna lääkintäteknisen yksikön lisäksi. Lääkintätekniikan vastuulla on laiterekisterin ylläpito. Rekisteri on osa seurantajärjestelmää, johon talletetaan laiteen tuotetietojen lisäksi kustannus-, huolto-, vika-, korjaus-, kalibrointi-, päivitys- ja huomiotietoja. Esimerkiksi HUS:n laiterekisterissä on noin 20 000 laitetta ja niiden vuosittaisia huoltotapahtumia yli 22 000 kpl. Koko laitekannan tietueiden suuruus on noin 100 000 kpl. Huolto- ja korjauspyynnön tilaaminen voi olla automatisoitu seurantajärjestelmän rajapinnan tai sen osasovelluksen kautta, jolloin pyyntötiedot kirjautuvat osaksi laitteen huolto- ja korjaushistoriaa. (HUS Lääkintätekniikka; Sofor.fi.)

Seurantajärjestelmään kirjattujen tietojen edellytetään edellä mainitun lain mukaan noudattavan jäljitettävyyden periaatetta. Järjestelmään on kirjattava tietoja, jotka osoittavat lain 24 §:ssä säädettyjen velvoitteiden toteutumisen, mm. menetelmät, menettelytavat ja ohjeistukset, joilla turvataan laitteiden käyttöpaikan ja käyttöympäristön turvallisuus. Lisäksi on kirjattava laitteen käytön aikana ilmaantuneiden vaaratilanteiden tiedot. (Laki 629/2010; Knuuttila 5.11.2014.)

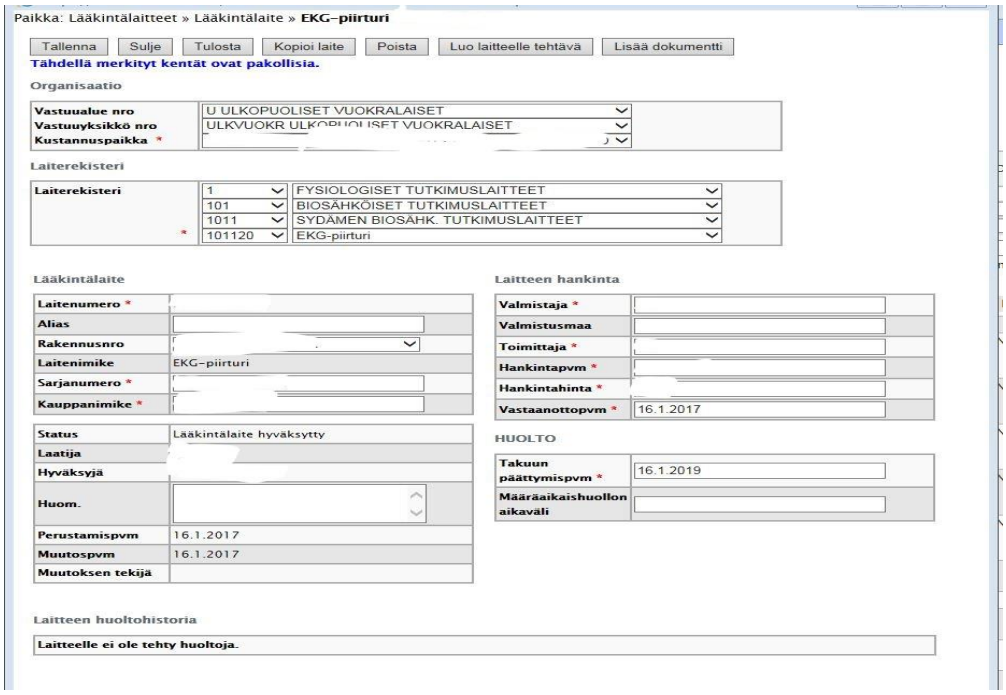
Seurantajärjestelmän tarkoituksena on varmistaa ja todentaa, että laitetta käytetään sen käyttötarkoituksen ja ohjeistuksen mukaisesti käyttöön soveltuvassa käyttöpaikassa ja -käyttöympäristössä, ja että laitteiden käyttäjillä on turvallisen käytön vaatima koulutus ja kokemus. Käytön turvallisuutta varmistetaan myös käyttöohjetietojen kirjaamisella. Seurantajärjestelmän avulla todennetaan, että valmistajan asettamat vaatimukset mm. laitteen ylläpidolle ja huollolle toteutuvat. Vaatimusten todentamiseksi kirjataan tiedot ylläpitoa ja huoltoa toteuttavien henkilöiden ammattitaidosta ja asiantuntemuksesta. (Laki 629/2010; Knuuttila 5.11.2014.)

Laissa ei ole määritelty seurantaan käytettävän järjestelmän muotoa. Järjestelmä voi olla manuaalinen tai sähköinen tai se voi olla yksi järjestelmä tai koostua erilaisista tietokokonaisuuksista tai järjestelmistä. Seurantajärjestelmä voi esim. olla osa lääkintätekniikan toiminnanohjausjärjestelmää. Tavoitteena on saada näkymä laitteiden elinkaaresta ja samalla tukea palvelutoiminnan suunnittelua ja ohjausta. Seurantajärjestelmän hyödyt ilmenevät mm. vastaanotettaessa uusia laitteita ja valmisteltaessa niitä käyttöön tai siirrettäessä olemassa olevia laitteita toisiin käyttöympäristöihin. Seurantajärjestelmään tallennetusta laitteen käyttöohjeistuksesta voidaan tarkistaa, onko valmistaja määritellyt erityisiä

tilavaatimuksia, jotta laitetta olisi turvallista käyttää. Erilaisissa käyttöympäristöissä (mm. sairaalan teho-osasto, leikkaussali, koti) voi olla eri tyyppisiä turvallisuusriskejä ja nämä täytyy käydä läpi ennen käytön aloittamista. Turvallisuusriskit voivat aiheutua esim. langattomasta tiedonsiirtotavasta tai sähkömagneettisten kenttien vaikutuksesta laitteisiin. (Vainiola 2016.)

Haasteita seurantajärjestelmän kehittämiselle aiheuttaa laitteiden suuri määrä sekä laitetyyppien laaja kirjo. Myös käyttäjäkunta on keskenään erilaista vaihtelevien käyttöympäristöjen myötä. Osa laitteista voi edellyttää huolto- tai käyttökoulutuksen tai ammattitutkinnon olemassa olon dokumentointia seurantatietoihin. Lisäksi käyttöön hankitaan täysin uuden tyyppisiä ja uusia teknologioita sisältäviä laitteita, joiden turvalliselle hallinnalle ja käytölle on tarpeen luoda menettelytavat. Lakia noudattaen on seurantajärjestelmään tarvetta tallentaa käytännössä enemmän tietoja kuin sähkökäyttöisten laitteiden laiterekisteri on perinteisesti sisältänyt. (Vainiola & Nihtinen 2016; Laitinen & Knuuttila 2014.)

Seurantajärjestelmässä oleva laiterekisteri sisältää laitekortin, johon kirjataan laitteen perustietojen lisäksi hankintaan, hallintaan, sijaintiin ja ylläpitoon liittyviä tietoja. Kuvassa 1 on esitetty erään lääkintälaitteen laitekortti.



Kuva 1. Laitekortti

4 Lääkintälaitteiden tietoturvallinen käyttö

Tekniikan tieteenalaan Suomalaisen asiasanasto- ja ontologiapalvelu Finto:n ja Tilastokeskuksen 2010 mukaan kuuluvassa lääketieteen tekniikassa hyödynnetään laajalti tietotekniikkaa. Sovellutusesimerkkeinä ovat mm. hengitys-, kuvantamis- ja mittauslaitteet.

Lain 629/2010 5 § kohdan 1 mukaan terveydenhuollon laitteella ja tarvikkeella tarkoitetaan instrumenttia, laitteistoa, välinettä, ohjelmistoa, materiaalia tai muuta yksinään tai yhdistelmänä käytettävää laitetta tai tarviketta sekä sen asianmukaiseen toimintaan tarvittavaa ohjelmistoa, jonka sen valmistaja on tarkoittanut käytettäväksi ihmisen
a) sairauden diagnosointiin, ehkäisyyn, tarkkailuun, hoitoon tai lievitykseen,
b) vamman tai vajavuuden diagnosointiin, tarkkailuun, hoitoon, lievitykseen tai kompensointiin,
c) anatomian tai fysiologisen toiminnon tutkimiseen, korvaamiseen tai muunteluun; tai
d) hedelmöitymisen säätelyyn.

Euroopan komission ohjeasiakirja MEDDEV 2.1/6 tammikuulta 2012 määrittelee lääkinnälliset laitteet seuraavasti (ote):
”Aktiivinen lääkinnällinen laite on laite, jonka toiminta perustuu sähköiseen energialähteeseen tai muuhun energialähteeseen kuin suoraan ihmiskehon aikaansaamaan voimaan tai painovoimaan ja jotka toimivat tätä energiaa muuntamalla. Lääkinnällisiä laitteita, jotka on tarkoitettu aktiivisen lääkinnällisen laitteen ja potilaan välisen energian, aineiden ja muiden tekijöiden siirtämiseen siten, etteivät ne huomattavasti muutu, ei pidetä aktiivisina lääkinnällisinä laitteina. Itsenäistä ohjelmistoa pidetään aktiivisena lääkinnällisenä laitteena. Diagnosointiin tarkoitettua laitetta käytetään yksin tai yhdessä muiden lääkinnällisten laitteiden kanssa hankkimaan tietoja fysiologisten tilojen, terveydentilan, sairauksien tai synnynnäisten epämuodostumien havaitsemiseksi, diagnosoimiseksi, valvomiseksi tai hoitamiseksi.” EU-alueen markkinoilla on yli 500 000 erityyppistä lääkinnällistä ja in vitro diagnostista (IVD) -laitetta (Euroopan komissio 2017).

Lääkintälaitteet luokitellaan laitetta käytettäessä ihmiselle aiheutuvan riskin ja potilaan haavoittuvuuden pohjalta. Luokassa I on matalin riski, luokissa IIa ja IIb keskisuuri ja luokassa III korkein riski. Luokittelusäännöt perustuvat mm. kehon kosketuksen ja elimistöön ulottuvuuden tai kajoavuuden asteeseen sekä käytön paikalliseen tai systeemivaikutukseen. Laitteiden luokittelu on haasteellista, sillä osa laitteista on rajatapauksia esim. kahden eri luokan välillä. Esimerkiksi sykemittari voidaan luokitella kuuluvaksi joko lääkinnälliseksi laitteeksi (MD) tai muuksi laitteeksi – käyttötarkoituksensa mukaisesti. Vastaavasti

potilastietojärjestelmä voidaan tulkita terveydenhuollon laitteeksi tai arkistointiohjelmistona käytettäessä muuhun tuoteluokkaan kuuluvaksi. (93/42/EEC Annex IX; Salminen 2013.)

Edellä kuvatun luokittelun soveltaminen ei saa vaarantaa laitteen turvallista käyttöä tai sen suorituskykyä, kun kyseessä on käyttötarkoituksen mukainen järjestelmäkokonaisuus. Tämä tarkoittaa sitä, että mikäli laite on tarkoitettu käytettäväksi yhdistelmänä muiden laitteiden tai varusteiden kanssa, on yhdistelmäkokonaisuuden (ml. liitosjärjestelmien) oltava turvallinen, eikä se saa vähentää laitteen määriteltyä suorituskykyä. Laitteen käyttöä koskevat rajoitukset on ilmoitettava merkinnöissä tai käyttöohjeessa. (93/42/EEC Annex 1.)

Lääkintälaitteiden tyyppikirjo mm. infuusiopumpuista diagnostiikkalaitteisiin on laaja ja käyttötarkoitukset moninaisia. Tietoturvan taso on usein korotettu potilaan tietosuojavaatimusten ja potilasturvallisuuden vuoksi. Lääkintälaite muodostaa aina systeemin ts. järjestelmän kytkeytyessään toisiin laitteisiin, tietokoneeseen tai tietoverkkoon. Lääkintälaitteet voivat muodostaa herätteitä ja hälytyksiä antavia verkkoautomaatiojärjestelmiä. Laitteiden toimintaa voidaan automaattisesti ja reaaliaikaisesti muuttaa potilasvasteiden ja komentojen mukaan. Tietojärjestelmä tai ohjelmisto on aina lääkinnällinen laite (MD), jos sitä käytetään lääkinnälliseen käyttötarkoitukseen.

Laitteiden tietoturvallista käyttöä voidaan edistää hyödyntämällä Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmän ohjeistuksia (Vahti), kansallista turvallisuusauditointikriteeristöä (Katakri) sekä EU:n lääkintälaitteita ja ohjelmistoja koskevia turvallisuusdirektiivejä. Merkittävimmät standardit kuuluvat ISO/IEC 27000-sarjaan, joissa kuvataan tietoturvallisuuden hallintaa ja turvallisuustekniikoita. Näiden lisäksi standardi SFS-EN ISO 14971 Terveydenhuollon laitteista ja tarvikkeista kuvaa riskinhallinnan soveltamista laitteiden ja tarvikkeiden elinkaaren aikana.

4.1 Lääkintälaite-esimerkki

Tässä opinnäytetyössä tutkimusaihetta tarkastellaan tyypillisen terveydenhuollossa käytettävän lääkintälaitteen kautta. Esimerkkilaitteena toimii sydänsähkökäyrän rekisteröintilaite eli EKG-laite. Euroopan komission MEDDEV-ohjeasiakirjan mukaan tietokoneavusteiset tulkintajärjestelmät (Computer Aided Detection, CAD) on tarkoitettu antamaan terveydentilaan liittyviä tietoja, ja siten ne luokitellaan lääkinnällisiksi laitteiksi. Tällainen järjestelmä voi esimerkiksi lukea automaattisesti röntgenkuvia tai tulkita EKG-käyriä. MEDDEV 2.4/1 -ohjeasiakirjan liitteessä IX kuvataan direktiivin 93/42/ETY luokittelusäännöt, joiden mukaan EKG-rekisteröintilaite kuuluu luokkaan IIa sovellettavan säännön 10 perus-

teella. Samaisen säännön perusteella se voidaan sydänvalvontalaitteena (kardioskooppi) erityisesti mm. operatiivisen ja tehohoidon aikana tai pitkäaikaisseurantaan (jatkuva käyttö, esim. holter) käytettynä luokitella kuuluvaksi luokkaan IIb.

THL:n raportissa nro 12/2015 Tieto- ja viestintäteknologian käyttö terveydenhuollossa vuonna 2014 kuvataan sydämen sähköisen toiminnan rekisteröintiä yhdeksi lääketieteelliseksi perustutkimukseksi, jonka sähköinen tallentaminen oli käytössä vuonna 2014 86 % sairaanhoitopiireistä – lisääntyen edellisvuosista. EKG-tutkimusten signaalimuotoisen tuloksen sähköinen käsittelyyn ja arkistointiin käytetään kansainvälisesti 39 erilaista standardia, minkä lisäksi laitevalmistajat käyttävät myös omia suljettuja tai avoimia formaatteja. Tämä eri tallennusmuotojen ja laitteiden välinen yhteensopimattomuus on osaltaan myötävaikuttanut siihen, että ns. sähköisen EKG:n eli keskitetyn tallennusjärjestelmän käyttöönottaminen on ollut hidasta Suomessa verrattuna muuhun terveydenhuollon tieto- ja viestintäteknologisiin järjestelmiin.

EKG-rekisteröintilaitteessa käsitellään signaalidataa, joka siirretään laitteen muodostamalla verkkoyhteydellä joko langattomasti tai kiinteästi keskitettyyn EKG-hallintajärjestelmään. Siirrettävä data sisältää tutkittavan potilaan henkilötietojen lisäksi raakatietoa ja tulkintaa hänen sydämensä sähköisestä toiminnasta. Tietoturvaa täytyy ylläpitää rekisteröintiprosessin kaikissa vaiheissa signaalitiedon keräämisestä tulkintaan, tietokantataltiointiin ja välitettyyn tallenteeseen asti.

4.2 Lääkintälaitteiden tietoturvariskit

Lääkintälaitteet täyttävät niille asetetut direktiivit (MDD, CE), mutta niiden sekä välttämättömien lisäkomponenttien käyttö kokonaisratkaisuna muuttaa tietoturvan tilannetta. Kokonaisratkaisun kyberturvallisuuden ylläpito voi muodostua haasteelliseksi, kun kokonaisuuden tietoturvallisuustaso muodostuu sen osien tietoturvallisuudesta ja järjestelmäympäristöt ovat monimutkaisia. Puutteet voivat olla lähtöisin epätäydellisestä tietoturvastrategiasta, -politiikasta, laitehallinnasta, henkilöstön tietoturvaosaamisesta, käytön hallinnasta, laitedokumentaatiosta, koulutuksesta ja käytön tuesta. Laitteen tietoturvan toteutuminen riippuu laitteen sisältämien ominaisuuksien ja toiminnallisuuksien lisäksi myös sen käyttöympäristöstä, käyttäjistä, käyttökohteista ja -tarkoituksesta sekä muista ulkopuolisista tekijöistä. Vaarana on, että erikseen tai ns. irrallisina hankitut laitteet ja niiden ohjelmistot eivät ole yhteensopivia jo käytössä olevien järjestelmien kanssa, laitteet muuttavat hoitoprosessia tai työtapaa aiempaa turvattomammaksi. Voi myös ilmetä laitteiden hankinta- ja käyttöönottovaikeuksia, kun odotetaan asennuksia ja laitteen saamista käyttövalmiuteen

eri toimijatahojen epäselvien vastuiden ja toimintaprosessiepäselvyyksien vuoksi. (Pöyhönen 2008.)

Valviran mukaan lääkintälaitteiden vaaratilanneilmoitusten määrä lisääntyy vuosittain noin 19 %. Ilmoitusten määrä kasvaa eniten sähkökäyttöisten ja mekaanisten lääkintälaitteiden ryhmässä, jossa ilmoituksia oli 41 kpl vuonna 2015 (kokonaisuus 3515 kpl). Tämä lääkintälaiteryhmä on laaja ja sisältää uuden tyyppisiä terveysteknologialaitteita. Yleisesti ottaen käyttäjät ilmoittavat paljon mm. potilasmonitoreista, potilastietojärjestelmistä ja infuusio- sekä hengityslaitteista verrattuna vähän ilmoituksia aiheuttaviin teknisiin apuvälineisiin tai kertakäyttölaitteisiin. (Nissinen 2016.)

Valviran taustaselvityslausunnossa 13.1.2017 Sosiaali- ja terveysministeriölle todetaan, että koneet minimoivat inhimillisen virheen todennäköisyyden, mutta tekevät sosiaali- ja terveydenhuollon toiminnasta toisella tavalla haavoittuvaa. Kyberuhat ovat uusia ja niiden torjunta vaatii uudenlaista osaamista. Lausunnossa kuvataan terveydenhuollon olevan kriittistä toimintaa, joka liittyy ihmisten perimmäisten perusoikeuksien eli hengen ja terveyden turvaamiseen. Tietojärjestelmien, ohjelmistojen ja lääkinnällisten laitteiden toimimattomuus ja niihin kohdistuvat hyökkäykset saattavat vaarantaa näiden keskeisten perusoikeuksien toteutumisen. Valvira mainitsee lausunnossaan esimerkiksi tahdistimen kytkemisen tietojärjestelmiin, jolla mahdollistetaan sydämen toiminnan aiempaa parempi seuraaminen. Kytkeminen voi lisätä alttiutta kyberhyökkäykselle, jolla elintärkeän terveydenhuollon laitteen toiminta saatetaan estää. Valvira toteaa, että uhat ja niiden kontrolloiminen ovat myös kustannusriski, kun palvelun tai työkalun käyttäminen edellyttää käytännössä erikseen ostettavia turvapalveluita.

Lausunnossa mainitaan myös, että robotiikan täysimittainen hyödyntäminen tuo uudenlaista valvottavaa ja muuttaa valvontatyön luonnetta. Valitun teknologian oikean kohdennuksen, toteutuksen ja turvallisen käytön arviointi ja valvonta tulevat lisääntymään. Laitteiden osalta niiden tekniset ominaisuudet kasvavat ja monimutkaistuvat ja liityntäpintoja ohjelmistoihin tulee lisää. Valviran arvion mukaan liittymäpinnat erilaisiin tietojärjestelmiin tulevat vaatimaan syvällistä ja monipuolista osaamista valvonnassa työskenteleviltä. Omavalvonnan sekä potilas-/asiakasturvallisuuden ja laadun hallinnan vaatimuksissa esimerkiksi laitteiden huollon ja ohjelmistojen päivittämisen merkitys saattaa kasvaa. Lisäksi valvonnan työtehtävien painopiste tulee muuttumaan, kun perinteisen ammattihenkilöiden valvonnan rinnalle tulee enenevässä määrin laitteiden käytön valvontaa ja laitteiden tuottaman tiedon tulkinnan valvontaa.

Terveydenhuollon tietoturvallisuuteen vaikuttavia ajankohtaisia päätrendejä ovat langaton sairaala ja lääkintälaitteiden verkottuminen sekä omahoitoa tukevien laitteiden ja sovellusten kytkeytyminen potilastietojärjestelmiin ja hoitoprosesseihin (Lähteenmäki & Ahonen 2016). Lääkintälaitteiden taustalla olevan ICT-ympäristön tulee edustaa korkeaa käytettävyyttä, millä varmistetaan potilastiedon saatavuus, eheys ja luottamuksellisuus sekä digitalisaatiosta aiheutuva riskien hallinta ja kriittisten järjestelmien katkottomuus (Pekkarinen 2016).

Verkkolaitteina käytettäviä lääkintälaitteita ei vastaanottotarkasteta tietoliikenteen ja tietoturvan näkökulmista. Tarkastus perustuu sähkötekniseen näkökulmaan. Hankinnan määrittelyt eli laitteille asetetut vaatimukset ovat usein kyberturvallisuuden näkökulmasta suppeat. Laitehankintoja ei välttämättä myöskään suunnitella kokonaisarkkitehtuurinäkökulmasta, vaan ne käsitetään usein erillisiksi ja yksittäisiksi hankintaeriksi kliinisen käytön näkökulmasta, jolloin kattavaa laitteistoarkkitehtuuria ei pääse muodostumaan.

Tietohallinnon, lääkintälaitetekniikan ja kliinisten käyttäjien edustajat yrittävät tunnistaa, mistä osioista kukin hankittava ja vastaanotettava tuoteratkaisu koostuu ja millaisia kyberturvaan liittyviä tekijöitä kussakin tuoteratkaisussa tulee huomioida sitä käyttöönotettaessa. Ns. mekaaniset vaaratekijät ja sähköön sekä säteilyyn liittyvät tekijät ovat helpommin tunnistettavissa ja ratkaisukeinot toteutettavissa verrattuna tietoturvaan, sillä niistä löytyy runsaasti selkeää ohjeistusta ja lähdemateriaalia pitkältä ajalta.

Seuraavissa kappaleissa mainitut riskit perustuvat Viestintäviraston Kyberturvallisuuskeskuksen tammikuussa 2016 julkaistuun Terveydenhuoltoalan kyberuhkia -raporttiin sekä ENISA:n (The European Union Agency for Network and Information Security) marraskuussa 2016 julkaisemaan raporttiin aiheesta Smart Hospitals Security and Resilience for Smart Health Service and Infrastructures. Lisäksi kappaleissa on hyödynnetty Pöyhösen ja Kylmälän kirjoittamaa ja Lääkelaitoksen (Fimea) 2014 julkaisemaa raporttia terveydenhuollon laadunhallinnasta ja lääkintälaitejärjestelmien turvallisuudesta.

Haitta- ja vaaratilanteita voivat aiheuttaa laitteissa ilmenevät tekniset viat, jotka aiheuttavat häiriöitä tietoliikenneyhteyksiin tai -verkkoon. Tämä saa aikaan sen, että järjestelmäkokonaisuuden laatu erityisesti mm. potilaan tilaa monitoroivien laitteiden osalta jää puutteelliseksi. Tämän lisäksi tietoverkkoon liitettyyn laitteiseen voi kohdistua tai tahallisesti kohdistaa sähkömagneettista häirintää, joka keskeyttää meneillään olevan prosessin, toiminnan ja tietojen välittymisen. Tällä on suora vaikutus potilasturvallisuuden toteutumiseen.

Laitteilla voi olla suojaamaton yhteys langattomaan verkkoon, jolloin järjestelmään on mahdollista päästä ei-toivotun käyttäjän toimesta. Käyttäjä voi ottaa laitteen ja verkon omaan hallintaansa ja siten päästä käsiksi suoraan laitteen sisältämään tietoon tai aiheuttaa haittaa verkossa esim. salakuuntelemalla, DoS-hyökkäyksellä tai MitM-tunkeutumisella. Tätä avattua tunkeutumisreittiä voidaan hyödyntää myös muiden haavoittuvien laitteiden etsinnässä tai tietoliikenteen ohjaamisessa.

Laitteiden sisältämää potilastietoa (esim. diagnostiset tiedot, tulosdata) ei saateta käsitellä tietoturvallisesti laitteen käytön yhteydessä, jolloin tietoa ei salata tai sitä välitetään edelleen turvattomien kanavien kautta. Laitteeseen voidaan tallentaa suuria määriä tunnistettavissa olevaa potilastietoa pitkältä ajalta, jota ei poisteta muistista. Mikäli pääsynhallinta on puutteellinen tai sitä ei voida hyödyntää, saattaa se tiedot alttiiksi luvattomalle käytölle. Yksinkertaisimmillaan laite – erityisesti pienikokoinen tai kannettava – voidaan varastaa, jolloin kaikki sen sisältämät potilastiedot katoavat.

Käyttäjän- ja pääsynhallinnan ollessa puutteellinen voivat kaikki käyttäjät (myös ei-toivotut) muuttaa paikallisesti laitteiden asetuksia tai päästä istuttamaan haittaohjelmia laitteeseen. Pääsyoikeuksia tai käyttövaltuuksia voidaan lähtökohtaisesti käytännön syistä käsitellä tai hallita riittämättömästi, jolloin myös verkon tietoturvallisuus voi vaarantua laitejärjestelmäympäristöissä. Laitteet eivät voi varmistaa vastaanottamiensa komentojen aitoutta ja sallivat sisältämiensä tietojen käsittelyn ilman käyttäjän tunnistusta. Turvattomuutta voi aiheutua mm. pakotetun (kovakoodaus) tehdas- tai oletussalasanojen käytön vuoksi tai yleiskäyttöisten sekä julkisesti saatavilla olevien salasanojen käytännön vuoksi. Laitteet voidaan väärillä asetuksilla saada lähettämään epäluotettavaa ja virheellistä dataa, jolloin tiedon luotettavuus ja eheys vaarantuu.

Laitteiden ohjelmistoille ei mahdollisesti voida suorittaa virheiden korjauksia tai toiminnallisuuksien parannuksia tai ne eivät ole ylipäätään päivitettävissä uusiin versioihin. Tällöin haavoittuvuuksien hallinta jää puutteelliseksi. Oletusasetukset ja -ohjelmat voivat sisältää haavoittuvuuksille altistavia ominaisuuksia. Laitejärjestelmiin voi olla mahdollista suorittaa esim. SQL-injektio. Laitteiden tuottama tieto voi kulkea verkossa paljaana siitä syystä, että laitteet tukevat suojaamatonta FTP-protokollaa tai muita turvattomia tai vanhentuneita protokollia. Laitteet voivat saastua tai lakata toimimasta haittaohjelmien tai pahantahtoisten tunkeutujien vuoksi. Päätelaitetason virustorjuntaa ei voida välttämättä toteuttaa ollenkaan.

Eri osista ja komponenteista koostuvia laitejärjestelmiä ei voida kattavasti testata etukäteen, vaan kokonaisjärjestelmän todellinen toimivuus voidaan joutua todentamaan vasta

tuotantokäytössä. Verkkojen ja verkkolaitteiden konfigurointi voi olla riittämätöntä tai laadullisesti huonoa, jolloin se tekee koko toimintaympäristön turvattomaksi. Lisäksi kokonaisuuden eri osat vanhentuvat eri tahtiin, laitteiden käyttöikä (ikäkierto) voi olla pitkä tai laite voi olla valmiiksi tuotettu vanhentuneella teknologialla.

4.3 Vastaanottotarkastuksen kehittäminen riskienhallintakeinona

Organisaation tietoturvastrategian ja -politiikan tulisi ohjata myös lääkintälaitteiden tietoturvan hallintaa ohjaamalla organisaation eri toimintayksiköiden ja palvelualojen, kuten lääkintätekniikan ja ammattimaiseksi vastuukäyttäjäksi määritettyjen tahojen toimintaa. Tavoitteena on suojata potilas- ja käyttäjätietoja lääkintälaitteissa, muissa laitejärjestelmän päätelaitteissa ja verkossa. Laitteiden identiteettiä tulisi vahvistaa myös siten, että niiden turvallisuuden ja yksityisyyden vaatimustasojen tulisi olla määritettävissä ja tarkoituksenmukaisesti säädettävissä. Tiedon luottamuksellisuus, eheys ja saatavuus tulee turvata laitteen elinkaaren ja sen käyttöprosessin aikana.

Lääkintätekniikan työprosesseilla ja vastuukäyttäjän rooliin kuuluvilla tehtävillä on oleellinen merkitys lääkintälaitteiden tietoturvan toteutumiseen. Teknisen asiantuntija- ja huoltohenkilöstön riittävällä tietoturvatietämyksellä ja -osaamisella varmistetaan tietoturvan toteuttamiselle otolliset edellytykset. Ammattimaisen vastuukäyttäjän rooliin kuuluu edistää lääkintälaitteen turvallista käyttöä käytettävyys säilyttäen. (Vainiola 2016.)

Tietoturvauhkien konkretisoituessa riskien toteumiksi riskien ja haavoittuvuuksien hallinnan kyvykkyys muodostuu siitä, että laitteiden seurantajärjestelmää hyödynnetään tehokkaasti ylläpitämällä laitteista ajantasaista tietoa. Laitteiden kriittisyys, turvallisuustaso ja riippuvuudet voidaan arvioida ja määrittää. Laitteiden ja järjestelmien hallintaan voidaan nimetä riittävä määrä käytettävissä olevia osaavia ja vaatimusten mukaiset kyvykkyydet omaavia henkilöitä. (Vainiola 2016.)

Riskienhallintaan sisältyy myös haitta- ja vaaratilanteista raportoiminen sekä ilmoitusten käsittelymenettely. Ilmoituksista saatavan seurantatiedon perusteella on mahdollisuus luoda uusia entistä turvallisempia käytäntöjä ja työmenetelmiä yhdessä käyttäjien kanssa. Valmistajien ja tuotetoimittajien tietoturvatiedotteiden ja Viestintäviraston haavoittuvuus- ja tietoturvaloukkausten ilmoitusten seuranta kannattaa vastuuttaa ja seurantaa toteuttaa jatkuvana. (Vainiola 2016.)

Riskienhallinnassa voidaan käyttää erilaisia tarkistuslistoja, jotka auttavat riskien tunnistamisessa ja seurannassa. Tarkistuslistat tarkoitetaan yleensä arkiseen ja toistuvaan käyt-

töön ja tavoitteena on muodostaa pysyvä toimintatapa tietoturvariskien toteutumisen välttämiseksi. Suomen Automaatioseuran Turvallisuusjaos suositteli 2010 tietoturvan mittausprosessien kehittämistä, jotta tietoturvan arviointi saataisiin jatkuvaksi, prosessimuotoiseksi ja muuttuviin tilanteisiin reagoivaksi. Irralliset tai yksittäiset satunnaiset tietoturvatarkastukset eivät riitä tietoturvan arviointiin.

4.3.1 Vastaanottoprosessi

Lääkintälaitteen vastaanottoprosessissa lain 629/2010 mukaiset päätehtävät ovat toimitussisällön tarkistus, CE- ja potilasliitynnän merkintöjen tarkastukset sekä käyttöohjeen tarkistus. Vuotovirtamittauksen lisäksi suoritetaan säteilylaitteen vastaanottomittaus. Nämä tehtävät toteuttaa lääkintätekniikka tai ostopalvelusopimuksella toimiva tekninen alihankkijayritys ennen laitteen luovuttamista käyttäjälle. Lisäksi tarkistetaan takuuaika ja sovitaan takuukatselmus sekä huoltosopimus.

Esimerkki erään lääkintätekniikan toimijan vastaanottoprosessista on kuvattu liitteessä 1. Prosessikuvaus on luottamuksellista tietoa, joten tämän opinnäytetyön julkisesta versiosta se on jätetty pois.

4.3.2 Tietoturvalomakkeet

Eräs sairaanhoitopiiri käyttää lääkintälaitteiden ja ohjelmistojen hankintavaiheessa määrämuotoista tietoturvalomaketta (luottamuksellinen liite), joka kuvaa tietoturvaan liittyviä huomioitavia kohteita. Tarjoaja eli toimittaja, joka vastaa tarjouspyyntöön täyttää lomakkeen, jonka perusteella arvioidaan laitteen tai ohjelmiston tietoturvataso ja tarvittavat käyttöönottovalmistelut.

Lomakkeessa kysytään laitteen perustietojen lisäksi tietoja verkkoyhteyden tarpeesta ja muista tarvittavista tietoteknisistä laitteista. Tarjoajan täytyy lomakkeessa selvittää, sisältääkö lääkintälaite tietokoneen käyttöjärjestelmineen ja ohjelmistoineen vai tarvitaanko laitteeseen liittää joko hankkivan organisaation tai laitetoimittajan työasema. Lisäksi kysytään tietoja laitteen tarvitsemista palvelimista ja ylläpidosta.

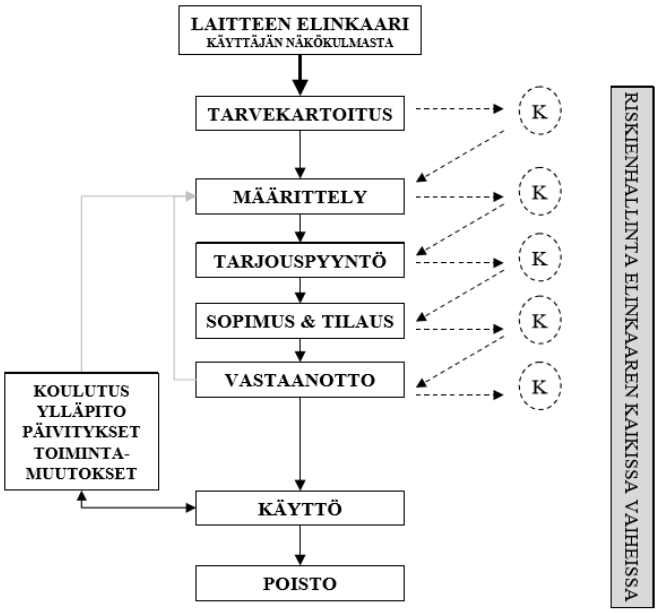
Opitietosuojaa.fi -sivustolla on kirjautuneelle käyttäjälle saatavissa tarkistuslistan muodossa olevia työkaluja henkilötietojen käsittelyn ja tietoturvallisuuden tarkastamiseksi. Tarkistuslistoja voidaan käyttää pohjatyökaluna sovellettuna oman toiminnan tarpeisiin esimerkiksi ostopalvelusopimuksia tehdessä ja suunniteltaessa ICT-hankintoja. Ne on laadittu eri projekteissa työskentelevien sekä sopimustekstejä laativien työntekijöiden avuksi helpottamaan henkilötietojen oikeaoppisen käsittelyn huomioimista sekä toimivat apuna varmis-

tettaessa, että hankittavissa tai käytettävissä tietojärjestelmissä on huomioitu tietoturvan ja tietosuojan peruslähtökohdat. Nämä tarkistuslistamallit ovat luottamuksellisia liitteitä.

5 Tarkistuslistan luominen

Tämän opinnäytetyön tavoitteena on tuottaa työkalu lääkintälaitteen vastaanottotarkastukseen tietoturvanäkökulmasta. Työkalu tuotetaan tarkistuslistana. Tarkistuslistan käyttäminen ajoittuu laitteen vastaanottovaiheeseen.

Laitteiden elinkaarimallin mukaan ennen laitteen vastaanottoa on ihannetilassa jo määritetty mm. vaadittava tietoturvataso. Tämä ei kuitenkaan aina toteudu, jolloin katselmuksia voidaan hyödyntää tukemaan elinkaaren eri vaiheita. Kuviossa 2 on esitetty laitteidenelinkaaren vaiheet.



Kuvio 2. Laitejärjestelmän elinkaari (Pöyhönen & Kylmälä 2004)

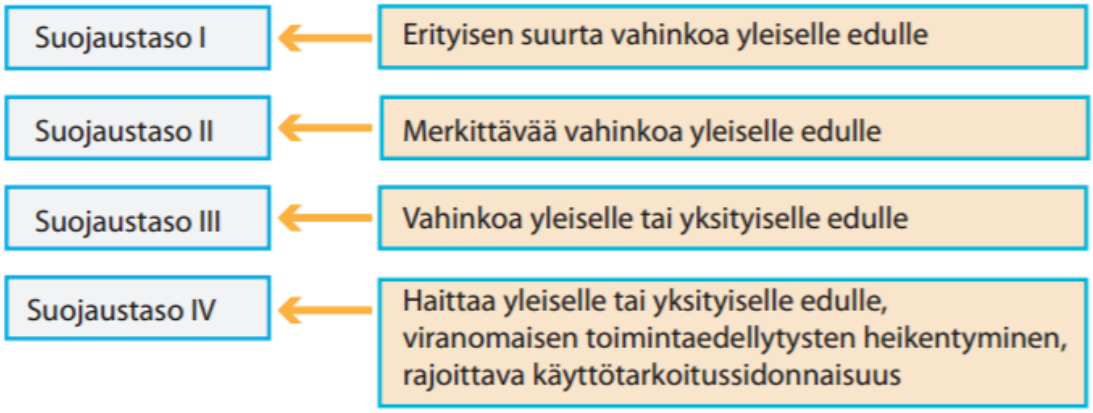
Eri vaiheiden jälkeen suoritettavien katselmusten avulla varmistetaan, että kaikki kyseisen vaiheen tehtävät on suoritettu hyväksytysti ja vaiheille asetetut tavoitteet on saavutettu. Katselmointikäytännön harjoittaminen edellyttää kuitenkin kullekin vaiheelle asetettujen tavoitteiden huolellista kirjausta ja katselmoinnin toimintaohjeiden laatimista. Katselmointien tukena ja käytännön toteutustapana voidaan käyttää erilaisia tarkastuslistoja kuvion 3 mukaisesti, joissa esitetään riittävä määrä erilaisia kysymyksiä laitteen elinkaarivaiheiden mukaisille sisällöllisille osa-alueille. Vaikka tämän menettelytavan ei katsota riskienhallinnan muodollisia menetelmiä, riittää se kuitenkin löytämään mahdolliset ongelmakohdat. (Pöyhönen & Kylmälä 2004.)

Kuvio 3. Laitteen elinkaarivaiheissa huomioitavia katselmoinnin kohteena olevia tekijöitä (Pöyhönen & Kylmälä 2004)

Ohjelmiston ja kokonaisuuden toimivuuden testaaminen sekä tietoturvallisen käyttövalmiuden todentaminen vastaanottotarkastuksen yhteydessä on haasteellista. Vastaanottotarkastusta voitaisiin tehostaa luomalla tarkistus- tai arviointitilaisuus, jossa laitteen kohdekäyttäjien kanssa katselmoitaisiin laitteen toiminnot, toimivuus ja tavanomainen käyttöprosessi. Vaikka vastaanottotarkastuksella ei ole tarkoitus korjata esim. hankintavaiheen määrittelyissä tapahtuneita puutteita tai laiminlyöntejä, on tarve kuitenkin viimeistään laitetta vastaanotettaessa käydä läpi tietoturvan toteutumista. Riittävän tarkkoja tietoturvamäärityksiä ei useimmiten ole sisällytetty tarjouspyyntöön, tilaukseen tai toimitussopimukseen eikä laitteen toimivuutta voitu testata kokonaisjärjestelmän osana koko toiminta- ja tietoketjun avulla. (Pöyhönen & Kylmälä 2004.)

Valtioneuvoston asetuksen 1.7.2010/681 tietoturvallisuudesta valtionhallinnossa 9 § 1 momentin mukaan arkaluonteisten henkilötietojen suojaustason voidaan katsoa olevan vähintään luokkaa IV tai III, sillä tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa joko haittaa tai suoranaista vahinkoa salassapitosäännöksessä tarkoitetulle yleiselle tai yksityiselle edulle. Henkilötietolain 11 § mukaisesti näitä (potilas)tietoja ovat mm. henkilön terveydentila, sairaus tai vammaisuus taikka häneen kohdistetut hoitotoimenpiteet tai niihin verrattavat toimet sekä henkilön sosiaalihuollon tarve tai hänen saamansa sosiaalihuollon palvelut, tukitoimet ja muut sosiaalihuollon etuudet. Kuviossa 4 on esitetty tiedon suojaustasot ja turvallisuusluokitukset Puolustusministeriön julkaiseman viranomai-

sille tarkoitetun Tietoturvallisuuden auditointityökalun eli Katakrin mukaan. Ensimmäinen Katakri julkaistiin 2009 ja tässä hyödynnetty versio on vuodelta 2015.



Kuvio 4. Tietoturvallisuusasetuksen suojaustasot (Puolustusministeriö, Katakri 2015)

Katakrin teknistä tietoturvallisuutta koskevassa osa-alueessa (I) kuvataan tekniselle tietojenkäsittely-ympäristölle asetetut turvallisuusvaatimukset jaoteltuna tiedon suojaustasojen II-IV mukaisesti (Katakri 2015). Valtioneuvoston asetuksen 1.7.2010/681 tietoturvallisuudesta valtionhallinnossa 16 § ja 19 § mukaan suojaustasoon III kuuluvan asiakirjan saa siirtää sellaisessa viranomaisen tietoverkossa, jonka käyttö on rajoitettu edellyttäen, että viranomainen on varmistanut tietoverkon ja tietojenkäsittelyn kokonaisuudessaan täyttävän tavanomaisesti sovellettavan korotetun tietoturvallisuuden tason vaatimukset. Tämä pätee myös suojaustasoon IV kuuluvien valtakunnalliseen henkilörekisteriin talletettujen arkaluonteisten henkilötietojen tai biometristen tunnistetietojen siirtämistä tietoverkossa. Suojaustasoon III kuuluva sähköinen asiakirja voidaan laatia, tallettaa ja sitä muokata viranomaisen tietoverkkoon liitetyllä laitteella, mikäli verkon käyttö on rajoitettu ja asiakirja talletetaan salattuna tai muutoin suojattuna siten, että tietoverkko ja tietojenkäsittely koko-

naisuudessaan täyttävät tavanomaisesti sovellettavan korotetun tietoturvallisuustason vaatimukset.

5.1 Tavoite ja rajaus

Tarkistuslistan käytöllä toteutetaan ennakoivaa tietoturvaa, jolla pyritään mahdollisimman kattavasti varautumaan ja ehkäisemään mahdolliset häiriöt laitetta otettaessa käyttöön ja sen käyttöaikana. Tarkistuslistan avulla voidaan kartoittaa huomioitavat asiat ja reagoida puutteisiin sekä varmistaa tarvittavien toimenpiteiden valmistelun aloitus. Tarkistuslistaa käyttämällä sovelletaan suojattavien kohteiden tunnistamisen periaatetta.

Tarkistuslista toimii yleisenä mallipohjana erittelemättömän lääkinnällisen laitteen vastaanottamiseen. Tarkistuslistalla ei tuoteta suoraan laitekohtaisia tietoturvavaatimuksia eikä arvioida lääkintälaitteen teknisen tietoturvan laatua, mutta sitä voidaan hyödyntää näiden vaatimusten ja laadun suunnittelussa.

Mallipohja on luonnos. Tässä opinnäytetyössä ei tehdä tarkistuslistan laadullista arviointia. Käyttöön soveltuvuuden testaus eli tarkistuslistan validointi jätetään jatkotutkimusaiheeksi, kuten myös listan versionhallinnan toteutustapa.

Työssä ei myöskään kehitetä vastaanottotarkastuksen työprosessia eikä lääkintätekniikan toimintaa. Kokonaisturvallisuutta edistävien toimintamallien ja työmenetelmien kehittäminen palvelu- tai henkilöstöhallinnollisesta näkökulmasta soveltuu jatkotutkimusaiheeksi. Työ liittyy riskienhallintaan riskien tunnistamisen ja analyysin valmistelun osalta, mutta lääkintälaitteiden riskienhallinnan suunnittelu ja ohjaaminen on laaja alue, josta on suotavaa tehdä erillinen tutkimus. Tästä perustietoa on saatavissa mm. ISO 14971 sekä IEC 60601 -standardeista sekä NIST:n (SP 800-30, Risk Management Guide for Information-Technology Systems) ja NCSC:n (A framework and set of good practice guides for securing Industrial Control Systems) viitekehyksistä. Lisäksi lääkintälaitteiden tietoturvallinen ohjelmistokehitys kuuluu toisen tutkimusaiheen piiriin, johon lähtötietoa voi hakea esim. VTT:n julkaisusta 2320 Turvallisuuskriittisten ohjelmistojen suunnittelusta ja lääkintälaitteiden ohjelmistojen suunnittelun kehityskohteista (Pöyhönen 2005).

National Institute of Standards and Technology´n (NIST) kyberturvallisuuden viitekehyksessä (Framework for Improving Critical Infrastructure Cybersecurity 2014) ensimmäisessä vaiheessa tunnistetaan käytettävissä olevat varannot ja vahvuudet. Näihin luetaan kuuluvaksi tiedot, henkilöt, laitteet, järjestelmät ja resurssit sekä puitteet, joiden avulla organisaatio toteuttaa omaa toimintaansa. Tunnistamalla lääkintälaitteet varannoiksi otetaan

ensiaskel kohti riskienhallintaa ja voidaan edetä kohti niiden haavoittuvuuksien ja uhkien tunnistamista sekä hallintakeinojen luomista.

NIST:n riskienhallintaoppaan (SP 800-30) mukaan turvallisuusvaatimusten tarkistuslistan kehittäminen omassa organisaatiossa tai valmiin pohjalistan hyödyntäminen edistää hallintakeinojen eli kontrollien järjestelmällistä ja tehokasta suunnittelua, määrittelyä sekä analysointia. Tarkistuslista auttaa toteutumien ja puutteiden havainnoinnissa ja muodostaa organisaatiossa eri tahoilla laajasti hyödynnettävän tietovarannon kerätyn tiedon kautta.

Tarkistuslista palvelee tietojen keräämisessä osana riskienhallinnan ensivaiheen toteutusta. Sen voidaan katsoa olevan ennen varsinaista riskienhallintaa tapahtuva valmisteleva lähtösuorite tai ensitaso, jonka pohjalta voidaan aloittaa riskien tunnistaminen ja edetä niihin varautumiseen. Tämä alkaa toimintaympäristön ja käyttökontekstin ymmärtämisellä käyttöönottosuunnittelun perustana.

5.2 Toteutus

Lääkintälaitteen toiminnallisten ominaisuuksien määrittämisessä sekä uhkien ja riskien tunnistamisessa haetaan vastausta siihen, onko laitteessa, laitejärjestelmässä tai käyttöprosessissa mahdollisesti vahinkoa tai vaaraa aiheuttavia tekijöitä ihmisille tai laitteen ympäristölle. Lähtökohtaisesti pyritään selvittämään, mikä on kyseinen tekijä, joka voi aiheuttaa vahinkoa tai vaaraa ja mitkä voivat olla tätä aikaan saavat syyt. Laitteen ominaisuuksien lisäksi toiminta- ja käyttöprosessin ominaisuudet, käytön tuki sekä käyttäjät ja käyttökohteet (potilaat) muodostavat huomioitavia ja tietoturvan toteutumiseen vaikuttavia tekijöitä. (Pöyhönen & Kylmälä 2004.)

Tarkistuslista on luotu hyödyntäen Valtionvarainministeriön Vahti-ohjeistuksia ja Puolustusministeriön Katakri-kriteeristöä. Vahti-ohjeista on käytetty erityisesti Päätelaitteiden tietoturvaohjetta (5/2013), Teknisen ympäristön tietoturvataso-ohjetta (3/2012) ja Sisäverkko-ohjetta. Katakrista on käytetty seuraavia osia: I 502.0, I 504.0, I 505.0, I 506.0, I 507.0, I 514.0, I 602.0, I 603.0, I 604.0, I 701.0, I 702.0, I 707.0, I 708.0. Lisäksi hyödynnettiin ISO/IEC 27000 -sarjan 27001:ssä ja 27002:ssa mainittuja laitteen vastaanottotarkastusvaiheeseen soveltuvia tietoturvallisuuden hallintakeinoja.

Pöyhönen ja Kylmälä totesivat jo 2004, että vaikka käyttäjän mahdollisuudet vaikuttaa monimutkaisten järjestelmien turvallisuuteen ja luotettavuuteen voivat tuntua rajallisilta, saadaan systemaattisten menettelytapojen soveltamisella hankinnassa, hoitoprosesseis-

sa, huollossa ja riskienhallinnassa sekä hankintojen tarkalla määrittelyllä varmistettua lääkintälaitteiden turvallista ja oikeaa käyttöä sekä hallintaa.
Lääkintälaitejärjestelmien turvallisuusoppaassa 2004 on esitetty toimintamalli vastaanotto-tarkastukseen sekä kooste hankinnan suunnittelun aikana varmistettavista asioista. Näistä jälkimmäistä on hyödynnetty tarkistuslistan luonnissa sen sisältämien tietoturvanäkökohtien vuoksi.

Valtiovarainministeriön Tietojärjestelmäkehityksen tietoturvallisuussuositus 3/2000 sisältää tietojärjestelmän elinkaaren eri vaiheiden tietoturvallisuustarkistuslistoja (liite 3). Suositus ohjeistaa tekemään ja tarkentamaan kaikissa vaiheissa tietoturvallisuusuhkien riskianalyysin ja suunnittelemaan niiden hallinnan. Tarkistuslistat ovat yleisiä ja kuvaavat tietoturvan toteuttamiseen liittyviä tehtäviä järjestelmän esitutkimuksen, määrittelyn, suunnittelun, toteutuksen, käyttöönoton, ylläpidon, tuotantoaikaisen käytön, version vaihdon ja käytöstä poiston aikana sekä myös testauksen ja laadunvarmistuksen näkökulmista. Listat sisältävät ylätason kysymyksiä ja niitä voi hyödyntää organisaation tietoturvapolitiikan rakentamisessa.

Finnish Cyber Security Certificate (FINCSC) on Jyväskylän ammattikorkeakoulun IT-instituutin alaisuudessa toimivan kyberturvallisuuden tutkimus-, kehitys- ja koulutuskeskuksen Jyväskylä Security Technology´n (JYVSECTEC) ylläpitämä yrityksille ja yhteisöille tarkoitettu sertifiointijärjestelmä. FINCSC koostuu arviointikohdista, joille tietoa tuotetaan eri kysymysalueiden kautta. Kysymyksillä mitataan sertifiointia hakevan organisaation vallitsevaa kyberturvallisuustasoa, ohjataan parhaiden tietoturvakäytäntöjen valintaa sekä varmistutaan organisaation kyvystä huolehtia tietoturvasta. Nämä ns. itsearvioinnin kysymykset rakentuvat seuraavista osa-alueista: hallinnollinen turvallisuus, henkilöstöturvallisuus, fyysinen turvallisuus, riskien- ja jatkuvuudenhallinta, arvioitavan ICT-ympäristön pääsynhallinta, toimintatavat ja järjestelmien hallinta, haittaohjelmat ja tietomurrot sekä tietojärjestelmien ja Internetin välinen suojaus. Hallinnollisen turvallisuuden kysymysalueella arvioidaan mm. keinoja johtaa ja ohjata kyberturvallisuuden kokonaisuutta sekä määritellä vastuita. Vastuiden ja valtuuksien riittämätön tai puuttuvat määrittely voivat aiheuttaa virhetoimintoja esim. henkilöstön rooleissa. Henkilöstöturvallisuuden kysymykset kohdistuvat mm. henkilöstön työtehtäviin soveltuvuuteen, ammatilliseen osaamiseen sekä tietoturvallisten työmenetelmien hallintaan. Osaamaton henkilöstö aiheuttaa vakavia riskejä toiminnan laadulle. Fyysisen turvallisuuden osa-alueella käydään mm. läpi keinoja suojata toimitiloja sekä kiinteää ja irtainta omaisuutta esim. omaisuuden anastamiselta ja luvattomalta käytöltä. Lisäksi arvioidaan omaisuuden sijoittelua ja säilytystä. Fyysisen turvallisuuden laiminlyönti heikentää myös hallinnollisten ja teknisten tietoturvakontrollien antamaa suojaa. (www.fincsc.fi.)

Tarkistusmallin luonnissa on hyödynnetty edellä kuvattujen lähteiden lisäksi myös opinnäytetyössä esimerkkeinä käytettyjä tietoturvalomakkeita. Nämä lomakkeet ovat suunniteltu käytettäviksi hankintavaiheessa ja sopimussuhteita solmittaessa, mutta jatkuvuuden ja yhteentoimivuuden näkökulmasta niiden sisältö on luontevaa huomioida soveltuvin osin.

5.3 Tuotos

Tarkistuslistamalli on jaoteltu tietoliikenne-, laitteisto-, ohjelmisto-, tietoaineisto- ja käyttöturvallisuuden osioihin, joihin on tuotettu tietoturvallisuuden tarpeiden hahmottamisessa auttavat kysymykset fyysisten, loogisten ja hallinnollisten kontrollien eli hallintakeinojen näkökulmasta.

Tarkistuslista on taulukkomuotoinen kysymyssarja, joka sisältää 101 kysymystä alikysymyksineen. Kysymysten jaottelu on tarkoituksenmukaista, jotta voidaan muodostaa käsitys siitä, mihin tietoturvallisuuden aihealueeseen (kontrolliin) kysymykset liittyvät. Tällä pyrittiin oikeuttamaan kysymysten esittämistä. Kysymykset ilmentävät tietoturvaan liittyviä havaintoja. Liitteenä olevassa listassa ne ovat satunnaisessa järjestyksessä.

Tarkistuslistaliite jakaantuu kysymysluettelona useammalle A4-sivulle. Lista on tuotettu myös excel-muotoon, jossa sisältöä on laajennettu. Taulukossa 1 on esitetty exceliin sisällytetyt kysymyskohtaiset määreet.

Taulukko 1. Tarkistuslistan kysymysten määreet

Kontrolli	Fyysinen
	Looginen
	Hallinnollinen
Vähimmäiskriteeri	Taustatieto
Merkitys tietoturvalle	Vähäinen
	Suuri
Vaikutus (häiriöiden eli tietoturvan toteutumattomuuden vaikutus potilasturvallisuudelle; haitan, vamman tai vaaran aste)	Vähäinen
	Merkittävä
	Kriittinen
Todennäköisyys haitalle tai vaaralle	Epätodennäköinen
	Vähäinen
	Todennäköinen
Laiteluokka	I
	IIa
	IIb
	III
Tiedon suojaustaso	I
	II
	III
	IV

Tämän rakenteen tavoitteena on valmistella riskilähtöistä tietoturvan arviointia, jotta tietoturvallisuuden hallintaa voidaan edesauttaa ja kysymysten vastauksia eli tuloksia voidaan soveltaa riskienhallinnassa. Pohjamalliin ei voida suoraan määrittää valmiiksi kysymyskohtaisen toteutumattomuuden – esim. tietojen salaamattomuuden – vaikutusta, sillä se riippuu täysin tarkasteltavasta lääkintälaitteesta tai laitejärjestelmäkokonaisuudesta sekä mitä suurimmassa määrin käyttökontekstista. Pohjamalli muodostaa kuitenkin perustan, jolle voidaan luoda organisaatiolle itselleen soveltuva luokittelujärjestelmä. Tarkempi laitekohtainen luokittelu voidaan suorittaa laitteen käyttöönottovaiheessa.

Laiteluokka ja tiedon suojaustaso kuuluvat perustietoihin. Osa kysymyksistä on taustatietoa, joka on syytä jatkossa erottaa omakseen kontrolleista. Taustatieto voi samalla toimia ns. vähimmäisvaatimuksena, jolla esim. vakiolaitekokoonpano määritetään tai asennusohjeiden toimitus varmistetaan. Osa kontrolleista on päällekkäisiä, sillä ne voidaan toteuttaa yhtä valittua useampana kysymyksen asettelusta ja siihen saadusta vastauksesta riippuen.

Pohjamallia voidaan myös jalostaa määrittelemällä potilasturvallisuusvaikutukselle ja vaaran tai haitan todennäköisyydelle raja-arvot esim. siten, että kriittistä vaikutusta ja todennäköisyyttä saa olla tietty sallittu määrä. Tietoturvallisuusmerkitystä voidaan tarkastella lähemmin ja tehdä laite- tai järjestelmätyyppikohtaista kysymysten vastausten sisällönanalyysiä niiltä osin, joilla on suuri merkitys tietoturvaan. Näin saadaan pohjustettua eri tyyppisten riskien vertailukelpoisuutta.

Kysymyksiin vastaaminen voi olla haasteellista niiden lukuisuuden ja erityisosaamisen vuoksi. Tarkistuslista onkin tarkoitettu läpikäytäväksi yhteistyössä eri vastuutahojen eli lääkintätekniikan, vastuukäyttäjien, tietohallinnon ja toimittajan kanssa. Vastaajien tiedot on merkittävä ylös jäljitettävyyden vuoksi. Tavoitteena on käynnistää tuloksekas keskustelu eri toimijoiden kesken, jotta organisaatio pystyy ennen pitkää muodostamaan kerätyn tiedon perusteella oman tietovarantonsa tietoturvan- ja riskienhallinnan perustaksi.

6 Pohdinta

Tutkimuksen tavoitteena oli tuottaa työkalu tietoturvan huomiointiin lääkintälaitteen vastaanottotarkastusvaiheeseen osana kyberturvallisuutta. Työkalu pyrittiin tuottamaan tarkistuslistan muodossa. Tavoite toteutui, sillä tarkistuslistaluonnos saatettiin tuotettua. Luonnos toimii pohjamallina, jota täytyy kehittää edelleen jatkotutkimusvaiheessa ja arvioida sen soveltuvuus.

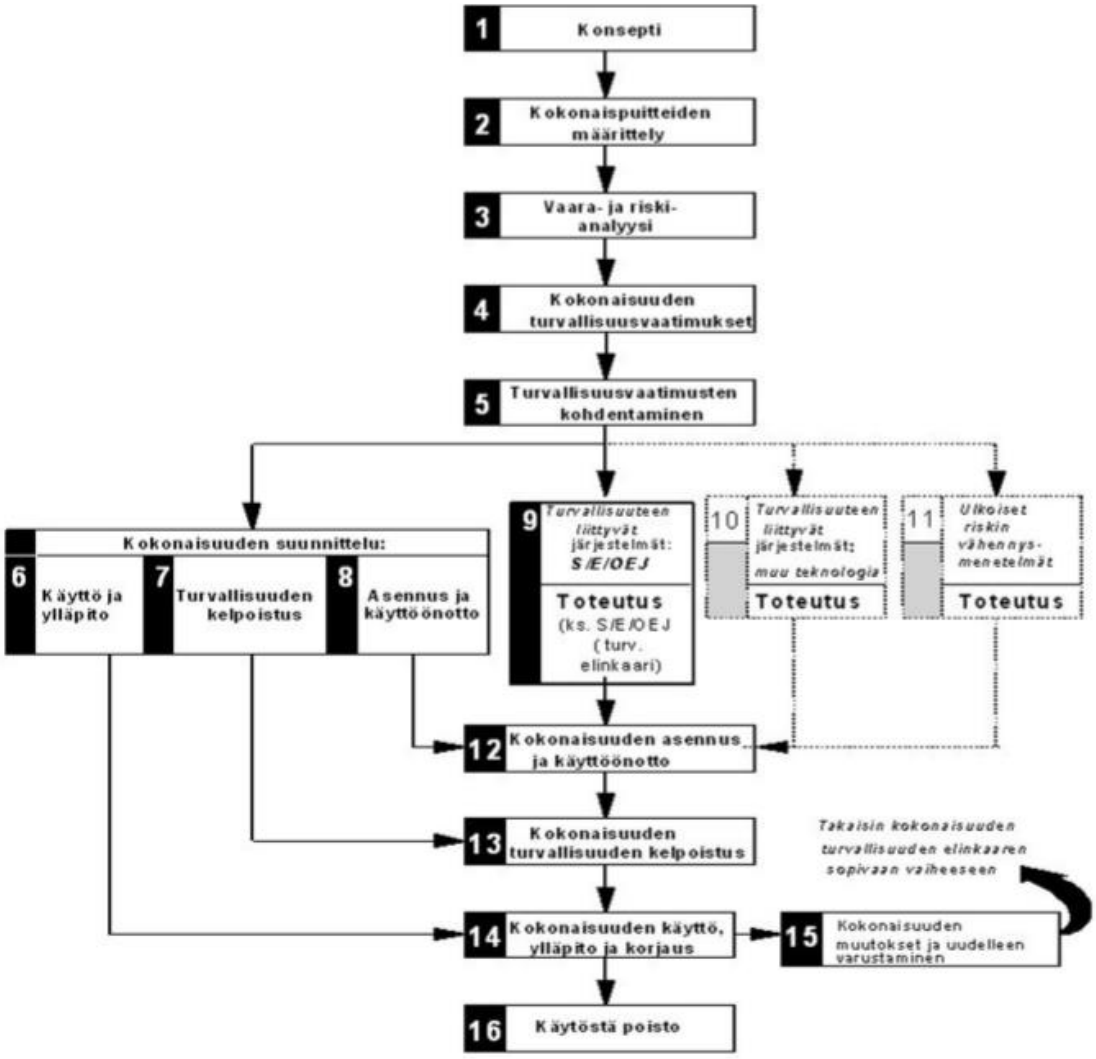
Tutkimuskysymyksinä oli selvittää, millaisia tietoturvanäkökulmia lääkintälaitteita vastaanotettaessa ja käyttäessä tulee huomioida sekä mitä asiakokonaisuuksia tarkistuslista voi sisältää eli mitä sisältöjä listaan voidaan upottaa, jotta sen avulla saadaan tuotettua tietoturvaan liittyvää tietoa käyttöönoton suunnitteluun ja valmistelutoimenpiteisiin. Ensimmäiseen kysymykseen saatiin vastaus runsasta lähde- sekä taustamateriaalia tarkastelemalla. Tarkistuslista rakentuu tietoturvallisuuden osa-alueista ja niiden hallintakeinojen jaottelusta. Vahti- ja Katakri-materiaalit antoivat rungon ja kysymyssisällöt tarkistuslistan mallipohjaan. Kysymyksiä on paljon, mikä kuvaa tietoturvan moninaisuutta ja monipuolisuutta. Kysymysten suuri määrä ei saisi kuitenkaan lannistaa tietoturvan katselmoijaa. Oletuksena on, että mikäli kysymyksiin saadaan paljon myöntäviä ja tarkentavia vastauksia, kuvastaa se lääkintälaitteen kompleksisuutta.

Yksinkertainen järjestelmärajapintoja sisältämätön verkkoon kytkemätön laite saa vastaavasti kielteisiä vastauksia kysymyksiin. Oma käsitykseni on, että laitteiden tietoturvan vaateita ja kokonaisuutta on vaikea hahmottaa ilman järjestelmällistä läpikäyntiä. Epäilen myös, että lääkintälaitteiden hankinta- ja vastaanottovaiheessa esimerkiksi tietoliikenteeseen liittyviin turvallisuusvaateisiin vastaamisen haasteellisuus saattaa yllättää tarkastajat ja käyttäjät. Kysymyksiä jouduttaneen jatkossa selventämään ja muotoilemaan entistä paremmin tarkoitustaan vastaaviksi. Lisäksi olisi suotavaa luonnostella kysymysten oheen myös selvennöstä yksittäisen kysymyksen tarkoitusperästä sekä alustavaa vastausten perusteella aiheutuvaa tehtävälistausta tai vastuumatriisia (esim. RACI). Taustatavoitteena on myös, että tarkistuslistaa hyödynnettäisiin moniammatillisesti, jolloin kysymysten edellytetään olevan ymmärrettäviä ammattiroolista riippumatta.

Tarkistuslista vaatii kehitystyötä erityisesti osana toimintaprosesseja. Organisaation on valittava, haluaako se käyttää systemaattista tietojen keräystä ja tehostaa siten tarkistusten, tarkastusten ja katselmointien toimintoja vai halutaanko tiukemman prosessin sijaan soveltaa niukempia käytäntöjä ja menettelytapoja. Mikäli tämän tyyppiseen tietojen keräämiseen ryhdytään, on syytä luoda prosessi myös tulosten soveltamiselle.

Tarkistuslistan mallipohjan hyödyntämiseen vaikuttaa suuresti se, miten vastuut sovitaan ja rajataan eri toimijatahojen kesken terveydenhuollon organisaatiossa. Vastuiden sopimista määrittää toimijoiden ja vastuuhenkilöiden palvelu- ja tehtäväkuvaukset sekä osaamistaso ja kyvykkyydet. Yhteistyötä on tiivistettävä tietoturvan kokonaishallinnan toteuttamiseksi. Tarkistuslistaa kannattaa kehittää siten, että kukin vastuutoimija ja merkittävä sidosryhmä pystyy saamaan listasta hyötyä omien tietoturvaa edistävien toimiensa toteuttamiseksi. Vastuiden määrittelyn lisäksi avainasemassa tulevat olemaan tarkistuslistamallipohjan kysymysten laukaisemien lisätoimien hallinta. Laitetoimittajat sisällyttävät toimituksiinsa laitteiden tietoturva-, turvallisuus- tai käyttöohjeet, mutta esim. samaa laitetta käytettäessä erilaisissa käyttöympäristöissä hieman erilaisiin käyttötapauksiin on syytä katselmoida laitteen tietoturvallinen käyttövalmius.

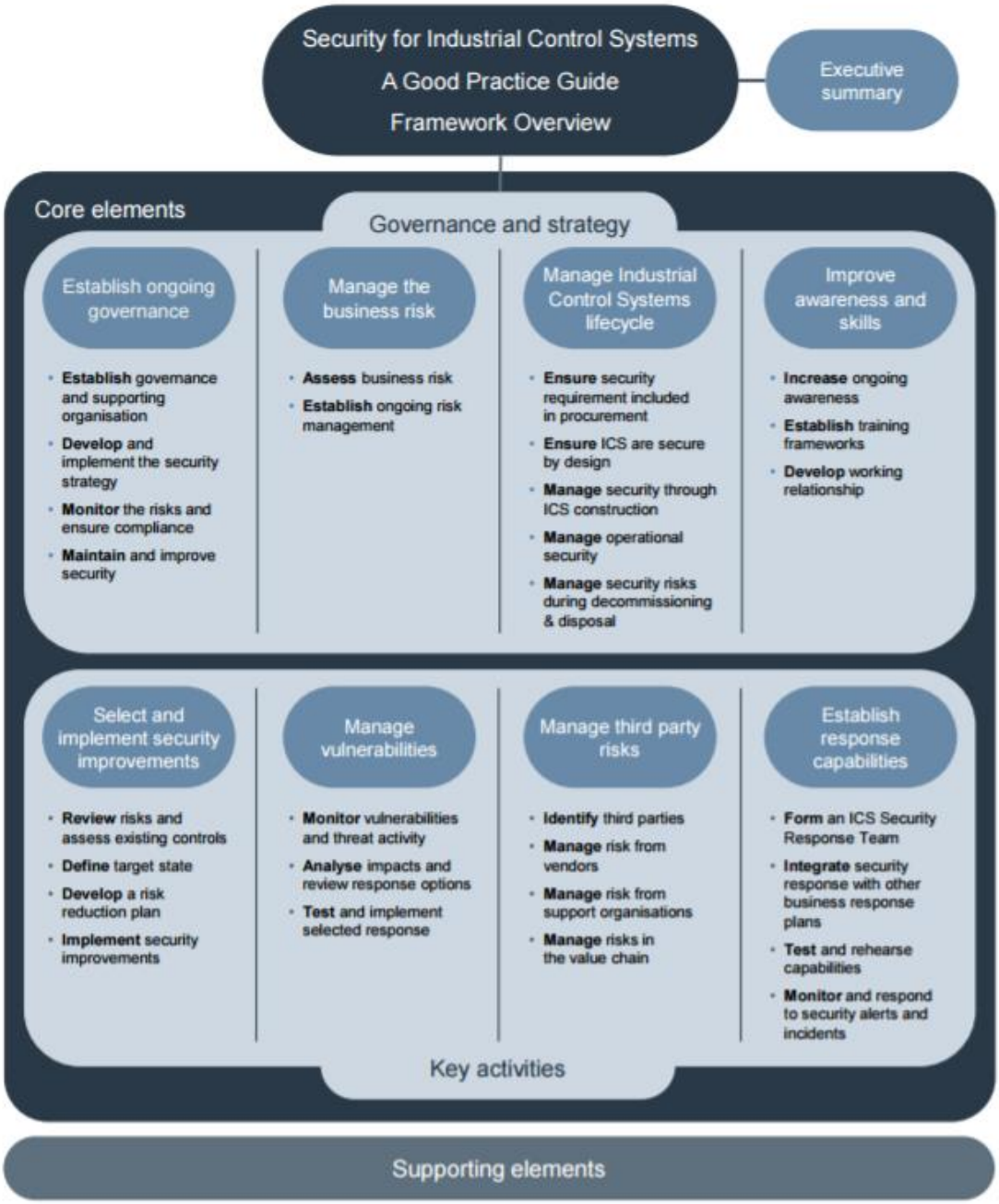
Tarkistuslistaa voidaan jatkossa kehittää teollisuusautomaation toiminnallisen turvallisuuden mallin avulla. Kuviossa 5 esitettyä Suomen Automaatioseuran Turvallisuusjaoksen mukaan IEC 61508 –standardisarjaan pohjautuvaa elinkaarimallia käytetään laajalti teknisten järjestelmien turvallisuuden varmistamiseen ja se soveltuu myös laitteiden tietoturvan hallinnan suunnitteluun strategia- ja periaatevaiheesta vaatimusten määrittelyyn, hankintaan, vastaanottoon, käyttöönottoon ja käytöstä poistoon.



Kuvio 5. Teollisuusautomaation elinkaarimallin vaiheet IEC 61508-1 mukaan

Teollisuusautomaatiossa tietoturvan arviointi ja sertifiointi pohjautuu Common Criteria for Information Technology Security Evaluation (CC) menetelmään, jonka ISO-standardi on 15408. Tätä menetelmää voitaisiin hyödyntää myös lääkintälaitteiden tietoturvavaatimusten määrittämiseen ja arviointiin sekä laitteiden hankinta- että vastaanottovaiheessa.

Toinen mahdollinen sovellettavissa oleva malli on CESG:n ja CPSI:n julkaisema SICS-viitekehys (PA Consulting Group 2015), joka on tarkoitettu kriittisten toimialojen teollisuuden hallintajärjestelmien turvaamiseen. Viitekehyksen pääelementit on esitetty kuviossa 6.



Kuvio 2. SICS viitekehys (PA Consulting Group 2015)

6.1 Jatkotutkimusaiheet

Jatkotutkimusaiheita on runsaasti. Tarkistuslistan laadullisen arvioinnin ja kehittämisen lisäksi voidaan laatia suunnitelma kokonaisturvallisuuden kehittämiselle tietoturvanäkökulmasta. Pyrkimyksenä voi olla selvittää, voidaanko vastaanottotarkastusta laajentaa kyberturvaa tukevaksi toimintamalliksi ja saadaanko lääkintätekniikan tekemällä vastaanottotarkastuksella ja laajennetulla toimintamallilla riittävät tulokset kokonaisratkaisun kyberturvallisuudesta.

Aiheeksi voidaan valita myös tietyn tyyppisten lääkintälaitteiden (esim. EKG:n pitkäaikaisrekisteröintien, potilasvalvontajärjestelmien EKG:n, mobiili- tai kannettavien EKG:ien tai ambulanssi-EKG:n) kyberturvallisuuden katselmointi, tyyppikohtainen tietoturva- ja riskitason määritys tai tietyn lääkintälaitteen tietoliikenteen monitorointi langattomassa verkkoympäristössä sekä penetraatiotestaus. Vaihtoehtoisesti voidaan keskittyä lääkintälaitteista raportoitujen kyberturvallisuuspoikkeamien tiedon kokoamiseen eri lähteistä ja kerätyn tiedon analysointiin esim. siitä näkökulmasta, miten lääkintälaitteiden tietoturvallinen käyttö eroaa organisaatioiden kliinisten tietojärjestelmien tietoturvallisesta käytöstä.

Aihe on myös tuore käytännön toimijoille ja haastaa asenteiden ja vastuukäsitysten muuttumiseen. Tästä syystä jatkotutkimusaiheeksi soveltuisi erinomaisesti kyselytutkimus, jossa selvitetään vastaanottotarkastuksen ja laiteseurannan tilannetta ja tasoa tietoturvan näkökulmasta eri sairaanhoitopiireissä ja terveydenhuollon organisaatioissa. Tällä saataisiin samalla selville tarpeet toimenpiteille, joilla halutaan edistää tietoturvan toteutumista.

6.2 Yhteistoiminta ja menettelytavat tietoturvallisuuden varmistamiseksi

Vastuiden sopiminen ja samalla yhteistyön tiivistäminen on oleellista, jotta laeissa, asetuksissa ja direktiiveissä asetetut velvoitteet voidaan toteuttaa ja tietoturvasta huolehtia kattavasti. Kliinisen hoitotyön puolella on jo toiminnassa monia erilaisia moniammatillisia tiimejä, joten miksipä moniammatillisuutta ei voisi toteuttaa työskentelymallina tai -periaatteena tässäkin. Mm. Valvira järjesti 2013 koulutustilaisuuksia (esim. alueellinen koulutus 12.2.2013 KYS:ssä) potilasturvallisuuden moniammatillisesta yhteistyöstä, jonka aiheena oli laiteturvallisuus sekä laki terveydenhuollon laitteista ja tarvikkeista. Lääkintätekniikan palveluntarjoaja toimii potilasturvallisuuden toteutusketjussa yhtenä merkittävänä tahona.

Keskustelua yhteistyön tiivistämisestä voitaisiin aloittaa tarkastelemalla VTT:n kehittämää DISC-mallia (Design for Integrated Safety Culture), joka on esitetty kuviossa 7. Malli kuvaa turvallisuuden näkökulmasta hyvin toimivan organisaation ja hyvän turvallisuuskulttuurin tai turvallisuuspotentiaalin omaavan organisaation kriteereitä sekä funktioita. Oleellista on, miten mallia osataan hyödyntää turvallisuuden johtamisessa ja tavoitteellisessa ohjauksessa. Tavoitteena on mallin avulla huomioida laajasti potilasturvallisuuden kannalta tärkeät organisaation toiminnot ja kiinnittämään huomiota siihen, millaisia piirteitä turvallisuuden johtamisella on hyvä pyrkiä luomaan organisaatioon. (Pietikäinen et all. 2012.)

Kuvio 7 DISC-malli (Reiman et all. 2012)

Vastuiden rajojen määrittämisen tarpeellisuus korostuu myös lääkintälaitteiden muodostaessa automaatiojärjestelmiä. Lääkintätekniikkapalveluja tarjoavassa toimiyksikössä voi olla erikseen oma sähkö- ja automaatioyksikkö, jolloin vastuiden määrittelyn tarve ja yhteistyön sujumisen edesauttaminen korostuvat.

Pauliina Hankivaara toteaa lääkintälaitteiden laiteasiantuntijuutta ja laitevastaavan tehtävää käsittelevässä tutkimuksessaan (Hoitotyön laiteasiantuntija 2016), että myös sairaanhoitajilta tullaan vaatimaan entistä laajempaa teknologiaosaamista pelkän laitteiden käyttöosaamisen lisäksi laitteiden määrän suurenemisen, kehittyneiden teknologioiden sekä laitteiden ja tietojärjestelmien enenevän integroitumisen vuoksi. Uudelle laiteasiantuntijan työroolille on tarvetta hoitotyön laadun, potilasturvallisuuden, työturvallisuuden ja viranomaisvaatimusten toteutumiseksi. Laiteasiantuntija edustaa toiminnallista asiantuntijuutta, joka toimii moniammatillisessa yhteistyössä lääkintätekniikan kanssa laitteiden käyttöönottovaiheessa ja edistää toiminnallaan laitteiden turvallista käyttöä.

Terveydenhuollossa on ajankohtainen tarve tietoturvamenetelmien ja kriteerien valmisteluun ja niiden soveltamiseen, jotta tietoturvatoimien hallinta ja organisointi voitaisiin toteuttaa tarpeita vastaavalla yhteistyöllä. Toimien suunnittelun ja toteutuksen järjestelmällisyys on avainasemassa, jotta ns. Security-Build-in ja Defence-in-Depth -periaatteet ovat toteuttavissa. Turvallisuusajattelun tulosten tulisi näkyä käytännön toteutuksina laite- ja järjes-

telmätuotteissa, toimintaprosesseissa sekä eri vastuutahojen yhteistyössä. Kwon ja Johnson totesivat 2012 tutkimuksessaan Security Practices and Regulatory Compliance in the Healthcare Industry Second, että terveydenhuollon organisaatiot (sairaalat) priorisoivat mielellään teknisiä keinoja, kuten esimerkiksi palomuureja, turvasähköposteja, verkkoliikenteen tarkkailua, tunkeutumisen havaitsemisjärjestelmiä sen sijaan, että ne hyödyntäisivät turvallisuuden hallinnan prosesseja ja toimintamalleja. Sama havainto tehtiin myös auditoinnissa, jossa auditoinnin prosessin kehittämisen sijaan pääpaino oli usein IT-sovellutusten käyttämisessä. Tämä välineellisen suuntauksen soisi edistyvän kohti tietoturvallisuuden kokonaiskehittämistä.

EU:n 2018 voimaan tuleva yleinen tietosuoja-asetus velvoittaa rekisterinpitäjiä ja organisaatioita varmistamaan tietosuojakäytäntöjensä lainmukaisuuden sekä tietoturvansa riittävyyden ja valmistelemaan varautumisensa ongelmatilanteisiin. Asetuksella pyritään suojaamaan aiempaa paremmin henkilötietoja, joita tuotetaan ja käsitellään lääkintälaitejärjestelmissä. Jotta esim. henkilön yksityisyyden suojaamiseksi sekä tietojen salaamiseksi, pseudo- tai anonymisoimiseksi voidaan asettaa tarvittavat vaatimukset, täytyy laitteiden liittämisen osaksi toimintaympäristöä ja kokonaisratkaisua tapahtua järjestelmällisesti tietoturva huomioiden. Terveydenhuollon tietoturvan tavoitteena on potilasturvallisuuden toteutuminen. Lääkintälaitteen vastaanottotarkastus ja tietoturvallisuuden katselmointi palvelee tätä lopputavoitetta.

Sosiaali- ja terveysalan lupa- ja valvontavirasto eli Valvira uutisoi 26.5.2017 lääkinnällisten laitteiden EU-asetusten voimaantulosta. Uusien asetusten tavoitteena on yhtenäistää lääkinnällisten laitteiden valvontaa ja siten parantaa potilasturvallisuutta sekä parantaa lääkinnällisten laitteiden laatua, turvallisuutta ja luotettavuutta. Siirtymäaikaa on kolme vuotta, mutta 26.11.2017 mennessä on nimettävä kansalliset toimivaltaiset viranomaiset, jotka valmistautuvat hoitamaan asetusten toteuttamiseen perustuvat valvontatehtävät. Lisäksi samaan päivämäärään mennessä on nimettävä myös maamme edustajat uuteen perustettavaan EU:n lääkinnällisten laitteiden koordinaatioryhmään, jolla tulee olemaan merkittävä rooli terveysteknologian kehittymisen seurannassa ja arvioimisessa. Koordinaatioryhmän tehtävinä on laitteita koskevien standardien, yhteisten linjausten ja tiettyjen laitteiden kliinisiä tutkimuksia koskevien tieteellisten ohjeiden ja tuotekohtaisten ohjeiden kehittäminen. (Euroopan komissio 2017)

Uusien EU-asetusten myötä lääkinnällisen laitteen määritelmä muuttuu, luokittelusääntöihin tulee muutoksia mm. ohjelmistoja koskien, yksilöllinen laitetunniste tulee pakolliseksi asteittain, IVD-laitteisiin tullaan soveltamaan uutta kansainvälisten ohjeiden mukaista riskiluokitusjärjestelmää sekä kaupallisille toimijoille ja valmistajille asetetaan uusia vaatimuk-

sia erityisesti markkinoille saatettujen laitteiden toimintakykytietojen keräämiseen liittyen. Laitteiden kattavan jäljitettävyyden varmistamiseksi tullaan luomaan seurantajärjestelmä. Vuoteen 2020 mennessä EUDAMED-tietokannalla saadaan tilannekuva kaikista lääkinnällisistä laitetuotteista ja jokainen uusi laite voidaan tunnistaa jatkossa yksilöllisesti. (Euroopan komissio 2017)

Uusilla lääkinnällisten laitteiden EU-asetuksilla määrätään myös valmistajien palveluksessa olevan nimetyn laitevastuuhenkilöstä. Vastuuhenkilöitä tulee olla vähintään yksi pätevyys- ja kelpoisuusvaatimukset täyttävä henkilö, jolla on erityisasiantuntemusta lääkinnällisistä laitteista. Erityisasiantuntemus on osoitettava joko viiden vuoden ammattikokemuksena lääkinnällisten laitteiden sääntelyasioista tai laadunhallintajärjestelmistä tai esim. korkea-asteen tutkintotodistuksella lääketieteen, farmasian, tekniikan tai muun asiaankuuluvan tieteen alalla lisättynä vähintään kahden vuoden ammattikokemuksella lääkinnällisten laitteiden sääntelyasioista tai laadunhallintajärjestelmistä. (Euroopan komissio 2017)

Lääkinnälliset laitteet tuottavat ja niillä tuotetaan terveyden- ja sairaanhoitoon ja lääketieteeseen liittyviä palveluita. Tietoverkkoon kytkettyinä laitejärjestelminä niiden voidaan laajasti ajatella kuuluvan IT-palveluiden piiriin, jolloin esimerkiksi niitä voidaan tarkastella esimerkiksi ITIL-prosessikehyksen näkökulmasta. IT-palvelut jaotellaan palveluiden elinkaarien eli palvelustrategian, -suunnittelun, -transition, -tuotannon sekä jatkuvan palvelun parantamisen prosesseihin. Tietoverkkoa hyödyntävät lääkinnälliset laitteet ja laitejärjestelmät tulisi liittää tietoturvan hallinnan, häiriön hallinnan, ongelmanhallinnan, muutoksenhallinnan sekä jatkuvuudenhallinnan prosesseihin mukaan. (ITIL v3 2013)

Pöyhösen ja Kylmälän (2004) mukaan lääkintälaitejärjestelmiin liittyvät hankinnat voivat olla hankkeina erittäin laajoja. Hankkeista voidaan tällöin muodostaa projekteja, jotka jaetaan eri osavaiheisiin. Projekteihin osallistetaan eri henkilöstöryhmiä työroolien,- vastuiden ja -tehtävien pohjalta. Hankintojen laajetessa voitaisiin niissä laadun, tuloksellisuuden ja tarkoituksenmukaisuuden varmistamiseksi hyödyntää standardeihin perustuvia ohjausmalleja, kuten esimerkiksi Scope Management -konsepteja.

Jyväskylän seudun kehittämisyhtiö Jykes Oy on järjestänyt 2016 työpajoja eri puolilla Suomea lääkintälaitteiden kyberturvallisuudesta. Työpajoihin on osallistunut laitevalmistajia sekä palvelujen tuottajia ja niiden tavoitteena on ollut muodostaa tilannekuva lääkintälaitteiden kyberturvallisuuden nykytilasta ja kehitystarpeista sekä hakea suuntaviivoja mahdollisille lääkintälaitteiden kyberturvallisuuden tutkimus- ja kehityshankkeille. Eniten tarvetta on noussut lääkintälaitteen hankinnan ja käyttöönoton kehittämiselle, lääkintälai-

tevalmistajan kyberoppaalle sekä yhteistyöverkostoille ja tiedonvaihdolle kyberuhkiin varautumisessa.

JYKES:n käynnistämän hankkeen soisi etenevän ja sitä on syytä seurata, sillä sen lopputuloksiksi tavoitellaan yhteistä käsitteistöä, yleisiä lääkintälaitteiden kyberturvallisuusvaatimuksia, tapaa lääkintälaitteiden tietoturvatasojen luokitteluun, toimintamallia lääkintälaitteiden riskianalyysin tekemiseksi kyberturvallisuus huomioiden, mallia riskianalyysin hyödyntämiseksi kyberturvallisuusvaatimusten sovittamisessa kuhunkin hankintaan sopivaksi, ohjetta hankintaprosessiin, ohjetta verkottuneen lääkintälaitteen käyttöönottoon ja ylläpitoon sekä Proof-of-Concept´ia lääkintälaitteen käyttöönottotestauksesta.

Tämän opinnäytetyön viimeistelyvaiheessa NIST julkaisi yhdessä NCCoE:n (The National Cybersecurity Center of Excellence) kanssa ohjeraportin (SP 1800-8A) langattomien infuusiopumppujen turvaamisesta terveydenhuollon organisaatioille. Julkaisussa on raportoitu infuusiopumppujärjestelmien riskianalyysi, johon kerättiin pohjatiedot kyselypohjaisella riskiarvioinnilla. Julkaisussa ohjeistetaan terveydenhuollon organisaatioita hyödyntämään standardeihin ja parhaisiin käytäntöihin perustuvia menetelmiä infuusiojärjestelmien turvaamiseksi. Riskien arvioinnin ja analysoinnin työkaluna hyödynnettiin Clearwater´n IRM|Analysis™ hallintakeinoihin (kontrollit) pohjautuvaa ja terveydenhuollon toimialaan soveltuvaa sovellusta SaaS-palveluna.

Erilaisia riskianalyysityökaluja on tarjolla runsaasti. Edellä mainittu työkalu vaikuttaa olevan alustavan tutustumisen perusteella hyvin kattava. Työkalujen käyttö edellyttää kuitenkin joka tapauksessa sisällön luomista tarvekohtaisesti kunkin organisaation taholta. Tietoturvan edistämisessä pääsee eteenpäin myös yksinkertaisimmilla sovelluksilla, joilla voidaan kuvata esimerkiksi katselmoinnin tehtäviä alitehtävineen, osoittaa niiden suorittamiseen tarvittavat resurssit (toimeksianto kohdehenkilöille) ja seurata tehtävien suorittamisen etenemistä ja niiden valmistumista tilannekuvanomaisesti. Lääkintälaitteiden tietoturvan katselmointi voidaan näin liittää osaksi esim. kokonaisturvallisuuden hallintaa.

Tutkija Moe siteerasi Bruce Schneier´ia vaikuttavassa puheenvuorossaan Suomen Sairaalatekniikan yhdistyksen järjestelmässä sairaanhoitopiirien kyberturvallisuusseminaarissa 14.4.2016 tyhjentävästi: ”We need to be able to verify the software that controls our lives”. Pienetkin askeleet ovat tärkeitä tämän edistämiseksi - esimerkiksi tarkistuslistan muodossa. Tarkistuslista käynnistänee keskustelun yhteistoiminnasta ja kokonaishallinnasta, jonka avulla tietoturvallisuutta toteutetaan aktiivisesti.

Lopuksi totean, että opinnäytetyön tekeminen edesauttoi omaa oppimistani sekä ammatillista ja tietämyksen kasvua. Opinnäyteprosessi sujui melko kitkatta, sillä aihe on henkilökohtaisesti kiinnostava ja tietoa oli kerätty pitkän aikaa. Työhön liittyvän sisältötiedon hallinta on hyvä toteuttaa jatkossa paremmin, jotta mm. lähteiden dokumentointi olisi tämänkertaista sujuvampaa. Työn lähdemateriaalien saatavuus ja ajantasaisuus sekä aiheen rajaus ja kohdentaminen oli haastavaa. Lähdemateriaalia on runsaasti, mutta aiheesta ei ole julkisesti vielä riittävästi saatavilla yksityiskohtaista, luotettavaa ja kohdennettua lähdetietoa. Aiheeseen liittyvää uutta tietoa tuli julkisuuteen kuitenkin aina viime hetkiin saakka, mikä toi haastetta työn rajaukselle, mutta myös avasi lisää mahdollisuuksia jatkotutkimuskohteiksi. Tämän työn tarkistuslistan viimeistely olisi vaatinut vielä aikaa. Mielestäni opinnäytetyö tässä muodossaan toimiikin parhaiten keskustelunavauksena tietoturvan huomiointiin osana kokonaisturvallisuutta sekä valmisteluna riskienhallintaan.

Lähteet

ENISA 2016. Smart Hospitals. Luettavissa: https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals. Luettu: 1.2.2017.

European Comission DG Health and Consumer Directorate B, Unit B2 “Cosmetics and medical devices” 2010. Medical Devices Guidance document. Classification of medical devices. Luettavissa: http://ec.europa.eu/consumers/sectors/medical-devices/files/meddev/2_4_1_rev_9_classification_en.pdf. Luettu 20.5.2017.

Euroopan komissio 5.4.2017. Lehdistötiedote. Lääkinnällisiä laitteita koskevat uudet EU-säännöt potilasturvallisuuden parantamiseksi ja terveydenhuollon nykyaikaistamiseksi. Luettavissa: http://europa.eu/rapid/press-release_IP-17-847_fi.htm . Luettu 20.5.2017.

Euroopan unionin neuvosto 22.2.2017. Kanta Euroopan parlamentin ja neuvoston asetuksen antamiseksi lääkinnällisistä laitteista, direktiivin 2001/83/EY, asetuksen (EY) N:o 178/2002 ja asetuksen (EY) N:o 1223/2009 muuttamisesta sekä neuvoston direktiivien 90/385/ETY ja 93/42/ETY kumoamisesta. (OR. en) 0728/16. Luettavissa: http://data.consilium.europa.eu/doc/document/ST-10728-2016-INIT/fi/pdf. Luettu 20.5.2017.

Euroopan yhteisöjen virallinen lehti 12.7.1993. 13/Nide 24. N:o L 169 /1. s. 85-125. Luettavissa: http://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:31993L0042&from=EN. Luettu 19.5.2017.

Euroopan parlamentti 5.4.2017. Lehdistötiedote. Luettavissa: http://www.europarl.europa.eu/news/fi/news-room/20170329IPR69055/l%C3%A4%C3%A4kinn%C3%A4lliset-laitteet-enemm%C3%A4n-turvallisuutta-ja-j%C3%A4ljitett%C3%A4vyytt%C3%A4. Luettu: 1.5.2017.

FDA 28.12.2016. Postmarket Management of Cybersecurity in Medical Devices. Luettavissa: http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022.pdf. Luettu: 1.5.2017.

Finlex 2010. Laki terveydenhuollon laitteista ja tarvikkeista. Luettavissa: http://www.finlex.fi/fi/laki/ajantasa/2010/20100629. Luettu: 1.5.2016.

Finlex 1.7.2010/681. Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa. Luettavissa: http://www.finlex.fi/fi/laki/ajantasa/2010/20100681#L2P4. Luettu 20.5.2017.

Finnish Cyber Security Certificate FINCSC. Sertifiointijärjestelmä. Sertifiointivaatimukset. Luettavissa: https://www.fincsc.fi/sertifiointivaatimukset/. Luettu 26.5.2017.

FINTO. Suomalainen asiasanasto- ja ontologiapalvelu. Lääketieteen tekniikka. Luettavissa: https://finto.fi/okm-tieteenala/fi/page/ta217. Luettu: 1.5.2017.

Hankivaara, P. 2016. Hoitotyön laiteasiantuntija. Opinnäytetyö joulukuu 2016. Tampereen ammattikorkeakoulu, ylempi ammattikorkeakoulututkinto, Hyvinvointiteknologian koulutus. Luettavissa: https://publications.theseus.fi/bitstream/handle/10024/121135/Hankivaara_Pauliina.pdf?sequence=1. Luettu: 11.5.2017.

HUS. Lääkintätekniikka. Luettavissa: http://www.hus.fi/hus-tietoa/sairaanhoitoalueet/hyks/hus-kuvantaminen/Vastuualueet/laakintatekniikka/Sivut/default.aspx. Luettu: 1.6.2017.

KASTEK Oy. Palvelut. Luettavissa: http://www.kastek.fi/palvelut.html. Luettu: 1.6.2016.

Knuuttila, J. 4.11.2014. Lain 629/2010 soveltaminen. Valvira. Lääkintätekniikan alan koulutustilaisuus. Luettavissa: http://ssty.fi/laakintatekniikanjaos/download/Luentomateriaalit04112014/Jari%20Knuuttila%202014-11-04-lain629-2010-soveltaminen.pdf. Luettu: 1.5.2017.

Knuuttila, J. 5.9.2012. Terveydenhuollon laitteiden valvonta. Valvira. Terveydenhuollon tietotekniikka -seminaari. SFS. Luettavissa: https://www.sfs.fi/files/1390/Knuuttila_05092012.pdf. Luettu: 1.5.2017.

Kwon J. et all. 2012. Security practices and regulatory compliance in the healthcare industry. Association for Information Systems. Luettavissa: http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1483&context=amcis2012. Luettu: 1.5.2017.

Kylmälä, K. 6.6.2008. Riskienhallintaprosessi. ISO 14971 riskienhallinta. Lääkintälaitteiksi luokiteltavinten tuotteiden ja IT-järjestelmien kehittäminen asiantuntijapartnereiden avulla

sekä IEC 60601-1:n uudet tuulet. FIHTA ry:n seminaari. Luettavissa: http://docplayer.fi/28550313-Riskienhallintaprosessi-iso-riskienhallinta.html. Luettu 19.5.2017.

Laitinen, T. 27.10.2014. Ammattimaisen käyttäjän kokemuksia lain vaatimusten täytäntöönpanosta. KYS Kuvantamiskeskus. Luettavissa: https://www.valvira.fi/documents/14444/37132/Valvira_281014_KYS_TLa.pdf. Luettu: 1.5.2017.

Liimatainen, T. 2014. Lääkintätekniikan ohjaaminen prosessijohtamisella ja prosessien kehittäminen. Lappeenrannan teknillinen yliopisto, Teknistaloudellinen tiedekunta, Tietotekniikan koulutusohjelma, Pro Gradu. Luettavissa: https://www.doria.fi/xmlui/bitstream/handle/10024/98431/diplomity%C3%B6_Liimatainen_0382844_valmis_16-6-2014.pdf?sequence=2. Luettu: 1.5.2017.

Linnavuori, K. 2015. Uusi lääkinnällisten laitteiden EU-asetus. Valvira. Luettavissa: https://www.fimea.fi/documents/160140/765540/28338_Linnavuori_ATMP_2015-02-04_2_.pdf. Luettu 25.5.2017.

Lähteenmäki, J. & Ahonen, P. 14.4.2016. Sosiaali- ja terveydenhuollon sähköisten palvelujen trendit. Mitä kyberuhkia on nähtävissä ja miten niihin tulisi varautua? Sairaanhoitopiirien kyberturvallisuusseminaari 14.4.2016. Luettavissa: http://ssty.fi/download/valmiusseminaari/Valmiusseminaari-La%25CC%2588hteenma%25CC%2588ki_Ahonen.pdf. Luettu: 14.4.2016.

Lääketieteellisen fysiikan ja tekniikan yhdistys LTTY. Luettavissa: http://www.lfty.fi/lfty.php. Luettu: 1.5.2016.

Moe, M. 14.4.2016. Hacking Medical Devices. SINTEF. Suomen Sairaalatekniikan yhdistyksen valmiusseminaari. Luettavissa: http://ssty.fi/download/valmiusseminaari/Marie-Moe-2016-04-14-NCSC-FI-til-publisering.pdf. Luettu: 14.4.2016.

National Institute of Standards and Technology NIST 2002. SP 800-30, Risk Management Guide for InformationTechnology Systems. Luettavissa: https://www.nist.gov/publications/risk-management-guide-information-technology-systems. Luettu 25.5.2017.

National Institute of Standards and Technology NIST 12.2.2014. Framework for Improving

Critical Infrastructure Cybersecurity. Version 1.0. Luettavissa: https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf. Luettu 25.5.2017.

National Institute of Standards and Technology NIST 2017. SP 1800-8A. May 2017. Securing Wireless Infusion Pumps In Healthcare Delivery Organizations. Luettavissa: https://nccoe.nist.gov/publication/draft/1800-8/VolB/index.html#cybersecurity-controls. Luettu 26.5.2017.

Nihtinen, P. 26.5.2016. Tilastotietoa terveydenhuollon laitteista ja vaaratilanteista. Ammattimainen käyttäjä laiteturvallisuuden varmistajana. Luettavissa: https://www.valvira.fi/documents/14444/1776602/Tilasto_2016_05_PN.pdf/469c9d08-7654-4075-9dd3-8ce83f349196. Luettu: 1.5.2017.

NIST 26.5.2016. Cyber-Physical Systems Public Working Group. Draft Framework for Cyber-Physical Systems. Release 1.0. Luettavissa: https://insidecybersecurity.com/sites/insidecybersecurity.com/files/documents/may2016/cs05262016_CPS_PWG_Draft_Framework.pdf. Luettu: 1.5.2017.

Opitietosuojaa.fi. Työkalupakki. Luettavissa: https://opitietosuojaa.fi/index.php/fi/tyokalulaatikko/johdanto. Luettu: 10.5.2017.

Pekkarinen, T. 12.10.2016. Kyberturvallisuus sairaaloiden eri toimialoilla. Sairaanhoitopiirien kyberturvallisuusseminaari 19.10.2016. Luettavissa: http://ssty.fi/download/valmiusseminaari19102016/Pekkarinen_kybertuvallisuus_sairaalan_eri_toimialoilla.pdf. Luettu: 19.10.2016.

Pietikäinen, E. et all. 2012. Adaptiivinen potilasturvallisuuden johtaminen. VTT. Luettavissa: http://www.vtt.fi/inf/pdf/technology/2012/T58.pdf. Luettu: 1.5.2017.

PPSHP 2017. Lääkintätekniikka. Luettavissa: https://www.ppshp.fi/laakintatekniikka. Luettu: 1.5.2017.

Puolustusministeriö 2015. Katakri 2015. tietoturvallisuuden auditointityökalu viranomaisille. Luettavissa: https://www.defmin.fi/files/3165/Katakri_2015_Tietoturvallisuuden_auditointityokalu_viranomaisille.pdf. Luettu 10.3.2017.

Pyörre, N. 2011. ISA-100 Spesifikaation tietoturvaominaisuudet. Tampereen teknillinen yliopisto, Automaatiotekniikan koulutusohjelma, Automaation tietotekniikka. Kandidaatintyö, elokuu 2011. Luettavissa: https://wiki.ase.tut.fi/courseWiki/images/5/51/Py%C3%B6rre-201108.pdf. Luettu: 1.5.2017.

Pöyhönen, I. 2005. Lääkintälaitteiden ohjelmistot. Yrityskohtainen malli turvallisuuskriittisten ohjelmistojen suunnitteluun. VTT tiedotteita 2320. Luettavissa: http://www.vtt.fi/inf/pdf/tiedotteet/2005/T2320.pdf. Luettu 18.5.2017.

Pöyhönen, I. 14.11.2008. Terveydenhuollon tietojärjestelmien elinkaarimalli. VTT, Terveydenhuollon tuotetekniikka. Luettavissa: http://docplayer.fi/3032467-Terveydenhuollon-tietojarjestelmat-elinkaarimalli-ja-toimenpiteita-parantaa-jarjestelmien-luotettavuutta-kayttajan-nakokulmasta.html. Luettu: 1.6.2016.

Pöyhönen, I. et all. 2002. Vaatimukset ohjelmistoa sisältäville lääkintälaitteille. VTT. Tiedotteita 2150. Luettavissa: http://www.vtt.fi/inf/pdf/tiedotteet/2002/T2150.pdf. Luettu: 1.6.2016.

Pöyhönen, I. & Kylmälä, K. 2004. Lääkintälaitejärjestelmien turvallisuus. Fimea/Lääkelaitos. 1/2004. Verkkojulkaisu. Luettavissa: http://www.fimea.fi/documents/160140/753095/19706_julkaisut_laitteet_ja_tarvikkeet_Julkaisu_01_2004_04-07-06_2_.pdf.pdf. Luettu: 1.6.2016.

Qualmed 14.3.2017. Hankekonsepti. Versio 0.12. JYKES. Luettu: 27.4.2017.

Salminen, L. 19.3.2013. EU ja CE-merkki. Medfiles. Luettavissa: https://www2.uef.fi/documents/976466/1745345/06-19Salminen+EU+CE/945a3d50-9925-4aac-977a-8546cdb44450. Luettu: 1.6.2016.

Schwartz, S. 27.12.2016. Managing Medical Device Cybersecurity in the Postmarket: At the Crossroads of Cyber-safety and Advancing Technology. FDA. Luettavissa: http://blogs.fda.gov/fdavoice/index.php/2016/12/managing-medical-device-cybersecurity-in-the-postmarket-at-the-crossroads-of-cyber-safety-and-advancing-technology/. Luettu: 1.2.2017.

Seppälä, J. 16.10.2013. Automaation elinkaari ja tietoturva. Tampereen yliopisto. Automaation tietoturvallisuuden teemapäivä. Luettavissa:

http://www.automaatioseura.fi/site/assets/files/1431/seppala_jari_automaation_elinkaari_tty_sas_asaf_16_10_2013.pdf. Luettu: 1.5.2017.

Sofor Oy 2017. Referenssit. Luettavissa: https://www.sofor.fi/web/-Irtaimistorekisteri-HUS. Luettu: 1.5.2017.

Standardisoinnin oppilaitosportaali SFSedu.fi 2017. ISO/IEC 27000-sarja. Luettavissa: http://www.sfsedu.fi/haku?searchterms=ISO+27000&x=0&y=0. Luettu: 1.5.2017.

Suomen Automaatioseura ry 2017. Turvallisuusjaos. Toiminta ja tavoitteet. Luettavissa: http://www.automaatioseura.fi/sas/jaostot/turvallisuus/. Luettu: 1.5.2017.

Suomen Automaatioseura ry 2017. Turvallisuusjaosto 2005. Verkottumisen riskit ja niiden hallinta. Verkkopainos 2010. Luettavissa: https://www.viestintavirasto.fi/attachments/tietoturva/TeollisuusautomaationTietoturva.pdf. Luettu: 1.5.2017.

Suomen Sairaalatekniikan yhdistys ry. 2017a. Lääkintätekniikan jaos. Luettavissa: http://ssty.fi/laakintatekniikanjaos/. Luettu 1.5.2016.

Suomen Sairaalatekniikan yhdistys ry. 2017b. Kyberseminaari. Luettavissa: http://ssty.fi/blog/event/sairaanhoitopiirien-kyberseminaari/. Luettu: 1.5.2016

Suomen Standardoimisliitto ry 2017. Standardit. Luettavissa: http://www.sfs.fi. Luettu: 1.5.2016.

Tilastokeskus 2017. Tieteenalaluokitus 2010. Luettavissa: http://www.stat.fi/meta/luokitukset/tieteenala/001-2010/index.html. Luettu :1.5.2017

Vainiola, T. 26.5.2016. Seurantajärjestelmä ja ammattimaisen käyttäjän vastuuhenkilö. Keskustelutilaisuus, Valvira. Luettavissa: https://www.valvira.fi/documents/14444/1776602/Seurantaj%C3%A4rjestelm%C3%A4_260516+TV.pdf/f509e9fc-87f3-483b-bf79-b88db523691b. Luettu: 1.5.2017

Valtiovarainministeriö 3/2000. Valtionhallinnon tietoturvallisuuden johtoryhmä Tietojärjestelmäkehityksen tietoturvallisuussuositus. Luettavissa: https://www.vahtiohje.fi/c/document_library/get_file?uuid=7342e259-12de-4142-b172-5455f9589090&groupId=10229. Luettu 25.5.2017.

Valtiovarainministeriö 2008. Valtionhallinnon tietoturvasanasto 8/2008. Luettavissa: https://www.vahtiohje.fi/c/document_library/get_file?uuid=7e2220f1-cc93-4ba6-8c70-a67869c526cc&groupId=10229. Luettu: 1.6.2016

Valtiovarainministeriö 2013. Sovelluskehityksen tietoturvaohje. Luettavissa: http://www.finlex.fi/data/normit/41655-VAHTI_1_Sovelluskehityksen_tietoturvaohje_NETTI.pdf. Luettu: 1.5.2016

Valtiovarainministeriö 2017. Valtionhallinnon tieto- ja kyberturvallisuuden ohjausryhmän (VAHTI) ohjesivusto. Luettavissa: https://www.vahtiohje.fi/web/guest/home. Luettu: 1.5.2016.

Valvira 2017. Euroopan komission ohjeasiakirja lääkinnällisistä laitteista. Luettavissa: http://www.valvira.fi/documents/14444/37132/sw_luokitteluohje_2012-03-13.pdf. Luettu: 1.5.2016

Valvira 13.1.2017. Lausunto hyvinvointialan robotiikan tilanteesta ja mahdollisuuksista. Dnro 6760/00.02.00.03/2016. Luettavissa: https://www.valvira.fi/documents/14444/92813/Lausunto_robotiikan_hyodyntaminen.pdf/f0745d7f-a9ee-4777-a73e-3099a0347bb8. Luettu: 1.5.2017

Valvira 2017. Lääkinnällisten laitteiden vaaratilanteiden ilmoittamista koskevat ohjeet. Euroopan komissio, Yritys- ja teollisuustoiminnan pääosasto, osasto F. Tulkintaohje. MEDDEV 2.12-Huhtikuu 2007. Luettavissa: http://www.valvira.fi/documents/14444/37132/Meddev_suomeksi.pdf. Luettu: 1.5.2017

Viestintävirasto 2017. Kyberturvallisuus. Luettavissa: https://www.viestintavirasto.fi/kyberturvallisuus.html. Luettu: 1.5.2016

Viestintävirasto 2017. Kyberturvallisuuskeskus. Terveydenhuoltoalan kyberuhkia. Verkkojulkaisu. Luettavissa: https://www.viestintavirasto.fi/attachments/tietoturva/Terveydenhuoltoalan_kyberuhkia.pdf. Luettu: 1.5.2017.

Liitteet

Liite 1 Esimerkki vastaanottoprosessista, Kastek Oy. Luottamuksellinen.

Liite 2 Tarjottavan lääkintälaitteen tietotekniset tiedot. Ilmoitus, tarjouspyynnön liite. HUS. Luottamuksellinen.

Liite 3 Henkilötietojen käsittelyn tarkastuslista. Opitietosuojaa.fi. Luottamuksellinen.

Liite 4 Tietoturvallisuuden tarkastuslista. Opitietosuojaa.fi. Luottamuksellinen

Liite 5 Tarkistuslistamalli lääkintälaitteen vastaanottovaiheeseen

Liite 5 Tarkistuslista

Perustiedot	Mihin lääkintälaiteluokkaan laite kuuluu?	
	Minkä suojaustason tietoja laitteella käsitellään?	
	Mikä asetetaan laitekohtaiseksi tietoturvatasoksi?	
	Milloin laite on turvamerkitty ja mikä sen turvaluokka on?	
	Milloin laite on liitetty laiterekisteriin?	
Turvallisuuden osa-alue	**Tarkistuskysymys**	**Hallintakeino**
Laitteistoturvallisuus	Miten laitteen varkaus on estettävissä?	Fyysinen
	Sisältääkö laite laiteliitäntöjä (fyysiset portit), joiden käyttö tulee mahdollistaa tai estää?	Fyysinen
	Millaisia fyysisiä lisäkomponentteja laitekokoonpano sisältää (esim. antureita, moduuleita, omia työasemia tms.)?	Fyysinen
	Käytetäänkö laitetta siten, että sitä siirretään sijainnista toiseen (onko laite mobiilikäyttöinen)?	Fyysinen
	Liitetäänkö laite etähallintaan?	Looginen
	Onko etähuollon tekevä taho todennettavissa tietoturvapolitiikan vaatimukset täyttävällä todennusratkaisulla?	Looginen
	Sisältikö laitetoimitus asennusohjeet?	Hallinnollinen
	Voidaanko varalaitteiden ja varaosien optimaalinen määrä laskea vikaantumisvälien odotusarvoista ja käytettävyystavoitteista?	Hallinnollinen
	Mikäli laite kuuluu johonkin laitteistokokonaisuuteen (ns. emolaitteen lisäksi muita lisälaitteita ja järjestelmiä), onko kokonaisuutta dokumentoitu systemaattisesti (tunnistaminen, jäljitettävyys, ymmärrettävyys)?	Hallinnollinen
	Onko laitetoimittajan kanssa sovittu laitteen toimitukseen, ylläpitoon ja hallintaan liittyvät toimintaprosessit, tiedotus ja tietojenvaihto?	Hallinnollinen
	Onko olemassa suunnitelma laitevahinkotapahtuman lieventämiseksi?	Hallinnollinen
	Onko laitteen huoltosopimussisällössä huomioitu laitteelle mahdollisesti tehdyn riskianalyysin tulokset (esim. huoltoväli, palveluaika yms.)?	Hallinnollinen
	Onko tiedossa ja voidaanko dokumentoida, missä tapauksessa valmistajan ohjeista tai suosituksista on jouduttu pakottavista syistä poikkeamaan (esim. esiasetukset, säädöt, käyttö, huolto, liitännät)?	Hallinnollinen
	Joudutaanko laite/ohjelmisto asentamaan muunlaiseen kuin valmistajan suosittelemaan järjestelmäympäristöön?	Looginen
	Onko laitteen etäyhteyskäytännöt sovittu toimittajan kanssa?	Hallinnollinen
Tietoliikenneturvallisuus	Edellyttääkö laitteen toiminta tietoverkon (verkkolaitteet, yhteydet) konfigurointia?	Fyysinen

	Käytetäänkö laitteessa omaa WLAN-moduulia?	Fyysinen
	Käyttääkö laite langatonta tiedonsiirtotekniikkaa (radio, sähkö, mikro, IR, matkapuhelin, GPS)?	Fyysinen
	Käyttääkö laite langatonta sisäverkkoyhteyttä?	Fyysinen
	Käyttääkö laite kiinteää sisäverkkoyhteyttä (Ethernet, DSL, kaapelimodeemi, puhelinverkko)?	Fyysinen
	Voidaanko lääkintälaitejärjestelmään kuuluvilta työasemilta avata yhteys julkiseen verkkoon?	Looginen
	Onko etäyhteydet laitteeseen sallittava (esim. keskitetty laitehallinta, toimittajayhteydet)?	Fyysinen
	Mitä tiedonsiirtoprotokollia, varmenteita ja sertifikaatteja laite tukee ja vastaavatko ne organisaation asettamia tietoturvavaatimuksia?	Looginen
	Onko tarvetta seurata laitteen tieliikennettä ja liittää se IDPS-/SIEM-järjestelmään?	Looginen
	Aiheuttaako laite tarvetta verkon koventamistoimenpiteille?	Looginen
	Tuleeko laitteen tietoliikennettä salata ja millä menetelmillä ja teknologioilla se suoritetaan? Esim. https, WPA2, VPN? Käytetäänkö salaamatonta yhteyttä (esim. FTP)?	Looginen
	Onko estetty avoin pääsy laitteeseen sen ulkopuolelta?	Looginen
	Ottaako laite vikaantumistapauksessa itse etäyhteyden etähuoltoon? Tukeeko laite automaattista vikailmoitusta? Onko tarpeen sallia etähuoltoyhteyden avaaminen vain erikseen auktorisoidun käyttäjän (esim. järjestelmävastaava) toimesta?	Looginen
	Miten laitteen langattomaan verkkoon pääsyä hallitaan; miten AAA-prosessi (todentaminen, valtuutus, tilastointi) toteutetaan? Hyödynnetäänkö SSID:tä?	Looginen
	Onko laitteen vaatimat koventamistoimenpiteet tietoverkolle ja verkkolaitteistolle dokumentoitu?	Hallinnollinen
	Onko laitteen käytön mukainen verkkoarkkitehtuuri kuvattu (sis. topologia, verkon pääsynhallinta)?	Hallinnollinen
	Onko laitteen vaatimista tietoliikenneyhteyksistä ja verkkolaitteista on ajan tasalla oleva dokumentaatio?	Hallinnollinen
	Onko laitteen verkolle aiheuttama kuormitus ja kaistatarve arvioitu?	Hallinnollinen
	Onko laite liitetty sen käyttötarkoituksen, ulkoisten liityntätarpeiden ja suojaustason mukaisesti sille kuuluvaan verkkosegmenttiin (aliverkkoon)?	Hallinnollinen
	Onko ratkaistu, kuinka laitteen huollossa ja korjaustoimenpiteissä mahdollisesti vaadittavat tietoverkkoa hyödyntävät laitteet (esim. väliaikaiset työasemat tms.) liitetään tietoverkkoon?	Hallinnollinen
Ohjelmistoturvallisuus	Sisältääkö laite käyttäjän käyttöliittymän tai -liittymiä?	Fyysinen
	Miten laitteen toiminta varmistetaan ja palautetaan (toipuminen)?	Fyysinen
	Sisältääkö laite järjestelmäriippuvuuksia (rajapintoja)	Fyysinen

	toisiin järjestelmiin?	
	Onko laitteessa kiinteä/siirrettävä muisti?	Fyysinen
	Voiko laitteessa toteuttaa käyttäjä- ja käyttövaltuushallintaa ja millä tasolla? Onko laitteen käyttäjä tarpeen tunnistaa ja todentaa? Voidaanko laitetta liittää keskitettyyn käyttäjähallintaan?	Looginen
	Voiko laitteessa toteuttaa pääsynhallintaa ja millä tasolla? Voidaanko ohjelmiston käyttämistä estää?	Looginen
	Tarvitaanko yhteiskäyttötunnuksia tai -salasanoja?	Looginen
	Onko salasanoihin asetettu ehtoja (esim. pituus, muoto, kesto, vaihtaminen)?	Looginen
	Onko tiedon syöttökenttien kokoa rajoitettu ja mikä vaikutus sillä on tietojen luotettavuuteen?	Looginen
	Voidaanko laitteen ohjelmistoa päivittää ja miten päivitykset toteutetaan?	Looginen
	Sisältääkö laite järjestelmäriippuvuuksia (rajapintoja) toisiin järjestelmiin?	Looginen
	Ovatko laitteen tietoturvaominaisuudet kierrettävissä tai käyttäjien muutettavissa? Voidaanko tämä estää?	Looginen
	Voiko laitteeseen liittää haittaohjelmien torjuntaa?	Looginen
	Onko oletusarvoiset turvattomat tehdasasennukset ja oletusasetukset (esim. oletustunnukset ja -salasanat) käyty läpi ja laite konfiguroitu tarvittavaa tietoturvatasoa vastaaviksi?	Looginen
	Millaisia lokeja laitteeseen muodostuu?	Looginen
	Onko laiteohjelmiston ylläpito suunniteltu ja dokumentoitu ajantasaisuuden ja luotettavuuden varmistamiseksi?	Hallinnollinen
	Onko korjaus- ja tietoturvapäivityksiä varten olemassa dokumentoitu prosessi?	Hallinnollinen
	Voidaanko todentaa, että valmistaja on noudattanut jotakin tunnettua ohjelmistotuotannon kehitysmallia tai standardia (esim. CMM, SPICE)? Onko varmistettavissa, että ohjelmistokehityksessä on hyödynnetty haavoittuvuustietokantoja (esim. OVSDB, NVD) tai metriikoita (esim. CVSS)?	Hallinnollinen
	Hyödynnetäänkö laitteessa web-sovellusta? Mitä webpalvelinta käytetään ja miten ohjelmiston ja palvelimen tietoturvapäivitykset toimivat yhteen?	Looginen
	Onko laitteen riippuvuudet muihin ohjelmistoihin ja järjestelmiin kuvattu?	Hallinnollinen
Tietoaineistoturvallisuus	Tallennetaanko laitteeseen potilastietoa? Tallennetaanko tietoa kuinka pitkäksi ajaksi?	Fyysinen
	Tallennetaanko laitteeseen salasanoja ja tallennetaanko ne suojaamattomina vai salattuina?	Looginen
	Joudutaanko laitteeseen tallennettavaa tietoa tulostamaan tai siirtämään toiseen mediaan?	Fyysinen
	Millä välineellä tiedon tulostaminen tai siirtäminen tehdään? Onko tulostaminen suositeltavaa vai kiellettyä?	Fyysinen

	Miten tulostaminen voidaan estää?	
	Millaisia medioita laitteeseen voi liittää (esim. USB)?	Fyysinen
	Miten tiedostojen hallinta on laitteessa toteutettu?	Looginen
	Onko laitteessa omaa tietokantaa ja miten sitä käytetään ja hallitaan (selaimet)? Miten tietokanta on suojattu ja kenelle tarvitaan siihen pääsy? Millainen vaikutus käytettävällä tietokannalla (rakenne) on tietojen luotettavuuteen? Onko tarvetta ottaa tietokannoista varmuuskopioita?	Looginen
	Sisältääkö laite potilaan yksilöivää tunnistetietoa?	Looginen
	Käytetäänkö laitetta tieteelliseen tutkimuskäyttöön? Miten tutkimusaineistoja käsitellään?	Looginen
	Onko tarvetta anonymisoida tai pseudonymisoida laitteen keräämää dataa (potilas- ja henkilötiedot)?	Looginen
	Onko tarvetta salata laitteen keräämiä potilas- ja henkilötietoja?	Looginen
	Millaisia toimenpiteitä tarvitaan tiedon eheyden ja sen muuttumattomuuden varmistamiseksi (esim. todennukset, tiedon siirtovirhelokit, tarkistussummien tms. käyttö)?	Looginen
	Miten laitteeseen tallennetut tiedot poistetaan ja hävitetään? Onko tarvetta sopia menettelytavasta, jolla tieto siirretään tai poistetaan esim. keskusjärjestelmään?	Looginen
	Tukeeko laite lääketieteellisiä luokituksia, sanastoja tai koodistoja? Ovatko ne standardien mukaisia? Miten niiden ajanmukaisuudesta huolehditaan?	Looginen
	Millaista tietovälinepolitiikkaa laitteessa noudatetaan? Onko tiedon tallennusvälineiden (ml. siirrettävät mediat, esim. CD-ROM, levyke, flash-muisti) käyttöä rajoitettu ja käyttörajoitukset ohjeistettu?	Hallinnollinen
	Onko laitteen välittämät tai siihen tallennettavat tiedot (potilastiedot) kuvattu (esim. tietovirtamallinnus, tietoauditointi tms.)?	Hallinnollinen
Käyttöturvallisuus	Onko laitteen luvaton käyttö on estettävissä?	Fyysinen
	Asettaako laite millaisia vaatimuksia käyttöympäristön turvallisuudelle (esim. julkinen tila, omahoitolaitteet, erityissuojattu tila)? Tuleeko laitteen käyttöympäristö suojata tietoturvasyistä minkälaisilla toimilla?	Fyysinen
	Onko laitteelle määritetty kuluva ja täyttyvä käyttö- tai varastointi-ikä tms. toiminta-aika, jota tulee seurata? Onko laitteessa sisäinen kello tms. automaattinen määrä-ajan kulumisen ilmoitus?	Looginen
	Onko laitteen käytöstä poistolle olemassa toiminnan (käyttökonteksti, toiminnalliset tarpeet) huomioiva protokolla tai työmalli?	Hallinnollinen
	Onko laitteelle tehty laitekohtainen riskianalyysi?	Hallinnollinen
	Onko tehty riskiarviota laitteen aiheuttamalle potilasvahingolle?	Hallinnollinen
	Onko laitteessa tai tukimateriaaleissa oleva informaatio	Hallinnollinen

	riittävä esim. käytön rajoituksista?	
	Onko laitteelle tarvetta suorittaa tietoturvakatselmointia tai esim. penetraatiotestausta? Ovatko testausmenetelmät suunniteltu ja dokumentoitu?	Hallinnollinen
	Onko laitteessa ominaisuuksia, jotka heikentävät tietoturvan toteutumista? Onko ne kuvattu?	Hallinnollinen
	Onko valmistajan/toimittajan tuotedokumentaatiossa kuvattu laitteen tietoturva- ja tietosuojaominaisuudet?	Hallinnollinen
	Onko arvioitu laitteen tuote- ja toimitusdokumentaation kattavuus ja riittävyys?	Hallinnollinen
	Onko laitteen tietoturvallisen käytön vaatimat koventamistoimet dokumentoitu? Onko laitetta käyttävän henkilöstön tietoon saatettu tarvittavat koventamistoimet ymmärretysti?	Hallinnollinen
	Miten laitetta käytetään poikkeusolojen aikana?	Hallinnollinen
	Onko laitteelle olemassa toipumissuunnitelmaa (häiriöt, katkokset, laiterikot)? Mikä vaikutus laitteen toiminta-häiriöllä on tieto- ja potilasturvallisuuteen? Kuinka kauan aikaa laite voi olla käytöstä pois ja onko sille olemassa korvaavaa laitetta tai toimintaa?	Hallinnollinen
	Onko laitteelle nimetty käyttäjien edustama laitevastaava tai laiteasiantuntija? Kuka omistaa laitteen käyttöprosessin?	Hallinnollinen
	Minne laitteen käyttöön liittyvät vaaratilanneilmoitukset dokumentoidaan?	Hallinnollinen
	Miten sovitaan laitteen ja laitejärjestelmän ohjelmistojen haavoittuvuuksien (haavoittuvuusjulkaisut) ja valmistajan turvallisuustiedotteiden seuranta? Miten näiden tiedonvälitysprosessi järjestetään?	Hallinnollinen
	Onko pääsyoikeuksien ja käyttövaltuuksien myöntämisprosessi kuvattu ja miten prosessin toteutuminen on katselmoitavissa?	Hallinnollinen
	Onko laite ensiasennuksen myötä otettu muutoksenhallintaprosessiin mukaan?	Hallinnollinen
	Miten tapahtumanhallintaa sovelletaan laitteen käytön aikana?	Hallinnollinen
	Onko laitteelle asetettu käytettävyys- ja palvelutasotavoitteet?	Hallinnollinen
	Edellytetäänkö käyttäjältä todistettavissa olevaa erityisosaamista (pätevyys, laiteajokortti tmv.)?	Hallinnollinen
	Voidaanko laitteen käytössä noudattaa organisaation tietoturvapolitiikkaa aukottomasti? Jos ei, niin missä tapauksissa ja tilanteissa joudutaan joustamaan?	Hallinnollinen
	Onko laitteen elinkaarta määritelty ja dokumentoitu? Onko laitteen valmistajan erittelemä toiminta-aika tai käyttö- tai varastointi-ikä merkitty tuotedokumentaatioon ja/tai laitteen merkintöihin? Onko ikä- ja aikatiedoille sovittu seurantamenettely (ilmoitukset)?	Hallinnollinen