Pohjois-Savon sairaanhoitopiirin kuntayhtymä

Lausunto

02.06.2022

Asia: VN/14455/2020-VM-28

Digitaalisen turvallisuuden yhteistoiminta- ja hallintamalliselvitys

Lausunnonantajan lausunto

Voitte kirjoittaa lausuntonne alla olevaan tekstikenttään

Pohjois-Savon sairaanhoitopiirin kuntayhtymä kiittää mahdollisuudesta antaa lausunto Julkisen hallinnon digitaalisen turvallisuuden yhteistoiminta- ja hallintamalliselvitykseen. Lausunto on yhteinen Pohjois-Savon hyvinvointialueen kanssa. Kiitämme myös mahdollisuudesta osallistua selvitykseen liittyvään haastatteluun aiemmin. Haluamme lausua selvityksestä seuraavat havainnot ja kehittämiskohteet.

Nykytilan kuvaus

Yhdymme erityisesti raportin ”Digitaalisen turvallisuuden strategiat ja säädösvalmistelu” -teeman havaintoihin siitä, että regulaatiota ja ohjausta tietoturvallisuuteen ja tietosuojaan tulee aivan liian monelta taholta. Osa näistä on keskenään ristiriitaista ja voimakkaasti tulkinnanvaraista.

”Suositukset, ohjeet, vaatimukset ja työkalut” -teeman havaintojen mukaisesti erilaisia suosituksia, ohjeita, työkaluja ja vaatimuksia on laajalti. Havaintojemme mukaan erilaiset ohjeet ovat varsin hajanaisia ja osin myös päällekkäisiä tai ristiriitaisia. Lisäksi koottu tiedottaminen suosituksista, ohjeista ja vaatimuksista tuntuu jääneen vajavaiseksi. Käytännön työssä erityisesti tietosuojanäkökulmasta positiivisesti on näkynyt VAHTI- työryhmän tekemä työ ja tiedottaminen.

Suosituksia, ohjeita ja vaatimuksia tulisi yhtenäistää kansallisella tasolla. Lisäksi suositusten ja vaatimusten velvoittavuus tulisi ilmaista selkeästi osana ohjeistusta. Sovellettavan lainsäädännön, ohjeiden ym. kokoaminen yhteistyöverkoston käyttöön esimerkiksi tiedotus-verkkosivuille auttaisi myös vähäi-semmillä resursseilla toimivia organisaatioita saamaan kokonaiskuvan tärkeimmistä noudatettavista vaatimuksista. Tällä hetkellä kokonaiskuvan saaminen on vaikeaa ja jää pitkälti yksittäisten asiantuntijoiden sekä asiantuntijoiden oman organisaationsa sisällä tekemän tiedottamisen varaan. Näitä tulisi ehdottomasti kyetä konsolidoimaan. Nykyinen sekava tilanne johtaa epävarmuuteen siitä toteutetaanko kaikki regulaation vaatimukset ja sovelletaanko varmasti oikeita ohjeita ja vaatimuksia. Tämä nostaa merkittävästi kustannuksia riskien lisäksi, kuten viivästyttää ICT-hankkeita merkittävästi.

”Digitaalisen turvallisuuden hankinnat” -teeman havaintojen mukaisesti kannatamme valmiiksi kilpailu-tettua laajaa palvelutarjoamaa, josta tulevat hyvinvointialueet voisivat täydentää omaa osaamista, resursseja ja kyberturvallisuuden sekä tietosuojan palveluita. Hankintojen yhteinen kilpailuttaminen vahvistaisi myös tietojärjestelmien yhteentoimivuutta. Turvallisuushankintojen toteuttaminen on erityisesti pienemmissä organisaatioissa haasteellista resurssisyistä. Alueellinen yhtenäinen ’perustaso’ digitaalisessa turvallisuudessa mahdollistaisi tasalaatuista asiakkaan tietoturvan ja -suojan toteuttamista.

”Digitaalisen turvallisuuden palvelut”- teeman osalta huomautamme, että palveluiden kehittäminen useissa erilaisissa tai eri pituisissa ohjelmissa voi johtaa erilaiseen tai jatkuvasti muuttuvaan ohjeistukseen. Hallinnonalojen tulisi pyrkiä vahvistamaan vuoropuhelua yhtenäisen linjan löytämiseksi.

”Digitaalisen turvallisuuden osaaminen” -teeman mukaisesti kannatamme, että eOppivaan rakennettaisiin riittävä kokonaisuus hyvinvointialueiden luottamushenkilöiden, johtavien viranhaltijoiden, riskienhal-linnasta vastaavien, tietosuojasta vastaavien, tietoturvasta vastaavien, terveydenhuollon, pelastustoi-men ja sosiaalitoimena ammattialaisille sopivat koulutuspaketit. eOppivan integrointi organisaation omaan HR järjestelmään ja identiteettien hallintaan (esimerkiksi Azure AD /ADFS) olisi tärkeää koulutusten seurantaan ja ylimääräisten tunnusten välttämisen kannalta.

Hyvinvointialueiden välinen yhteistoiminta

Selvityksessä (kohta 2.3) todetaan, että tietoturvasta ja asiakkaan tietosuojasta on huolehdittava palvelun koko elinkaaren ajan. Hyvinvointialueilla on tietoturvan kannalta erilaisia osa-alueita, kuten julkista päätöksentekoa, julkisia ohjeita, sosiaali- ja terveysalan asiakas- ja potilastietoa sekä turvallisuustoiminnan piirissä olevaa pelastusalan tietoa. Hyvinvointialueet huolehtivat itsenäisesti palveluihin liittyvästä digitaalisesta turvallisuudesta. Myös selvityksessä tunnistettu riski tietojärjestelmien suuren määrän ja tietoverkkojen rakenteen osalta on perusteltu.

Hyvinvointialueille tuodaan yhteen erittäin laajoja kokonaisuuksia, mikä aiheuttaa haasteita digiturvallisuuden/koulutuksen/ohjeistusten yhtenäisyydelle. Myös luovuttajaorganisaatioiden lähtötasot digiturvallisuudessa voivat olla todella erilaisia. Tietoturva- ja tietosuoja ovat nykyään erittäin korostuneessa roo-lissa terveydenhuollossa. Havaittujen kehittämistarpeiden vuoksi onkin erittäin tärkeää, että hyvinvointialueiden rahoituksessa huomioidaan korostunut tarve tietosuoja- ja tietoturvaosaamiselle. Digiturvallisuus ei voi perustua pelkkään tekniseen toteutukseen, vaan tärkeässä roolissa ovat myös substanssi-asiantuntijat, jotka kykenevät viestimään tietoturvasta ja -suojasta henkilökunnalle ja asiakkaille.

Tavoitetilan kuvaus

Digitaalisten palveluiden ja turvallisuuden tavoitetilaa kuvataan selvityksen 4. luvussa. Pidämme tärkeänä, että selvityksessä esiin tuotu vahva tarve tehtävien organisoinnille, osaamisen kehittämiselle ja tiedon jakamiselle otetaan asianmukaisesti huomioon hyvinvointialueiden rahoituksessa. Selvityksessä todetaan kannatettavasti: ” Hyvinvointialueilla on vastuullaan infrastruktuurit, joiden ylläpito ja digitaalisen turvallisuuden kehittäminen edellyttävät osaamista ja resursseja. Hyvinvointialueet tarvitsevat osaavaa henkilöstöä, joka ymmärtää kriittiseen

infrastruktuuriin liittyvät turvallisuusvaatimukset sekä tavat, joilla ne voidaan toteuttaa.” Sote ja pelastustoimen sektoreilla tietosuojan ja tietoturvan merkitystä ei voi liikaa korostaa ja myös resursoinnin tulee olla riskitasoon nähden riittävällä tasolla.

Pidämme erittäin tärkeänä, että hyvinvointialueeseen sovellettavat digitaalisen turvallisuuden säännökset yhdenmukaistetaan. Hyvinvointialue toimii jatkossa sekä julkisen hallinnon toimijana että sosiaali- ja terveyspalvelujen tarjoajana. Yhtenäisen ohjauksen ja ”yhden luukun periaatteen” toteuttaminen tiedon jakamisessa on erittäin tärkeää johtuen rajallisista resursseista. Pidämme myös erittäin tärkeänä sen määrittämistä, milloin ohjeistuksessa on kyse lainsäädäntöön verrattavasta linjauksesta ja milloin suosituksesta. Materiaalipankki, jossa olisi esimerkiksi sopimusmalleja ja tarkastuslistoja vapaaseen käyt-töön, on erinomainen ja kannatettava ajatus. Yhtenäiset mallipohjat ja toimintatavat toimijoiden välillä parantavat tietoturva- ja tietosuojatasoa. Kehittämistoimintaan (ohjeistukset, tietojärjestelmien yhteishankinnat) tulisi myös osallistaa käytännön toimijoita siten, että käytännön työn näkökohdat tulevat otetuksi huomioon.

Julkisen hallinnon toimijoille yleisesti, että sosiaali- ja terveyspalelujen tarjoajille erityisesti asetettujen vaatimusten tulisi olla ristiriidattomia. Tällä hetkellä tämä ei toteudu ja sen seurauksena resursseja haaskataan vaatimusten tulkintaan ja toteuttamiseen.

Kehitysehdotuksessa 1. todetaan seuraavasti: ”Esimerkiksi Suomessa hyvinvointialueilla tulisi tulevaisuudessa olla käytössä enintään 2-3 toistensa kanssa yhteentoimivaa asiakas- ja potilastietojärjestelmää, mikä mahdollistaisi järjestelmien ja niiden digitaalisen turvallisuuden tason kustannustehokkaan ylläpidon ja kehittämisen sekä varautumisen kannalta riittävän hajauttamisen”. Tätä kirjausta pidämme hieman ongelmallisena mm. kilpailun rajoittamisen vuoksi (hankintalaki). Tietoturvallisuutta ja tietosuojaa voidaan myös ketterästi toteuttaa riskilähtöisesti arvioimalla, teknisellä testauksella ja asianmukaisilla sopimuksilla tietoturvasta ja henkilötietojen käsittelystä. Tämäntyyppinen kirjaus voi johtaa siihen, että vain hyvin suuret tietojärjestelmätoimittajat voivat toimittaa järjestelmiä hyvinvointialueille. Tämä voi myös johtaa hyvin vanhojen teknologioiden ja prosessien käyttämiseen. Nämä puolestaan altistavat erilaisille vaikeasti hallittaville haavoittuvuuksille sovelluskoodin määrän kasvaessa ja teknologioiden vanhetessa. Ehdotamme tämän kirjauksen poistamista raportilta tai sen muokkaamista.

Ehdotus: ”Hyvinvointialueiden digitaalisen turvallisuuden yhteistoimintamalli tulee valmistella ja ottaa käyttöön. Hyvinvointialueille tulee tarjota tukea, johon sisältyy mm. suosituksia, ohjeita ja vaatimuslisto-ja digitaaliseen turvallisuuteen liittyvien vastuiden kuvaamiseen infrastruktuureihin liittyvien digitaalisen turvallisuuden vaatimusten määrittämiseen. Tuen antamiseen tarvitaan vastuutaho, joka ymmärtää operatiivista toimintaa ja kykenee toimimaan strategisen ja operatiivisen toiminnan välimaastossa nämä yhdistävänä tekijänä. Vastuutaho vastaa siitä, että annettava tuki on ajan tasalla.” Tämä on erittäin kannatettava ehdotus, mutta korostamme sitä, että tämä yhteistoiminta ei saa olla sanelua esimerkiksi ministeriön, viraston tai esimerkiksi Kelan toimesta. Hyvinvointialueet tuntevat käytännön haasteet tietoturvallisuuteen ja tietosuojaan sekä regulaatioon liittyen. Hyvinvointialueet ovat myös parhaat tahot haasteita ratkaisemaan. Tätä haasteiden ratkaisemista tulee tukea ministeriöiden, virastojen ja esimerkiksi Kelan toimesta. Sama

vastuutaho voi koota tilannekuvaa hyvinvointialueiden tietoturvallisuuden ja tietosuojan tilanteesta. Tunnistaa ja priorisoida kansallisia kehityshankkeita ja selvittää näiden rahoitusta kansallisesti.

”Virastoilla on velvoite arvioida riskejä, mutta riskiarviointia ei toteuteta systemaattisesti, eikä yhteistä mallia riskien arvioimiseksi ja hallinnoimiseksi, yhteistä näkymää arvioituihin riskeihin tai toimintamallia riskitiedon jakamiseksi ja laaja-alaiseksi hyödyntämiseksi ole.” Tässä kohtaa raportti viittaa virastojen riskienarviointiin, mutta lienee kuitenkin tarkoitus viitata myös esimerkiksi sairaanhoitopiireihin ja tuleviin hyvinvointialueisiin. Tulee huomioida, että riskien arvioiminen on lakisääteistä esimerkiksi tietosuoja-asetuksen ja tiedonhallintalain myötä.

Riskeihin, turvallisuusjärjestelyihin ja varautumiseen liittyvät tiedot ovat julkisuuslain 24 § 7 ja 8 kohtien perusteella pääosin salassa pidettäviä. Näiden jakaminen yksityiskohtaisella tasolla ei näin ollen ole perusteltua muille organisaatioille, eikä edes organisaation sisällä kuin asiaomaisille tahoille. Organisaation riskienhallintakäytäntöjen pääasiallinen tarkoitus on hallita organisaation riskejä asianmukaisesti kyseisen organisaation tarpeisiin ja tavoitteisiin peilaten. Yhteiset riskienhallintamallit ja riskirekisterit voivat johtaa riskienhallinnan osalta lopputulokseen, joka ei palvele organisaatiota parhaalla tavalla, koska sitä ei ole mukautettu organisaation toimintaan. Yhteiset riskirekisterit voivat helposti johtaa riskien kuvaamiseen liian ylätasolla, ja tähän liittyvät myös edellä mainitut julkisuuslain mukaiset salassapitoperusteet.

”Tarvitaan mahdollisesti säädös, jossa edellytetään digitaaliseen turvallisuuteen liittyvän roolia jokaises-sa virastossa.” Tässä kohdassa myös puhutaan virastosta, vaikka lienee tarkoitus myös viitata tuleviin hyvinvointialueisiin ja kuntiin. Digitaalisen turvallisuuteen liittyvän roolin määrittelyssä tulee huomioida, että roolista ei tule tietoturvariskien omistajaa missään tapauksissa. Koordinoiva päällikkötason tehtävä on hyvä olla kaikissa organisaatioissa. Mallia on hyvä ottaa esimerkiksi tietosuojavastaavan tehtävänkuvasta. Koordinointivastuu voisi sisältää vastuun organisoida tietoturvanhallintajärjestelmät ja tietoturvaan liittyvien riskien hallinta. Rooli ei kuitenkaan voi vastata esimerkiksi yksittäisten järjestelmien, rekisterien tai vaikka sovelluskehityksen tietoturvallisuudesta tai tietosuojasta. Tällä tavoin vastuut riskeistä saadaan menemään niille tahoille, joilla on mahdollisuus budjetoida ja aidosti hallita riskejä. Ylin vastuu tietoturvallisuudesta on yleensä organisaation hallituksella ja ylimmillä viranhaltijoilla (johtajilla). On tärkeää, että vastuuta ei tällä roolilla siirretä organisaatiossa alaspäin, johtaen näin negatiiviseen kehi-tykseen tietoturvallisuudessa ja tietosuojassa.

Lopuksi

Digitaalisen turvallisuuden osaamisen kehittäminen on tärkeää mutta tulee huomioida, että kehittäminen vaatii aina resursseja. Myös teknisen tason tietoturvallisuuden kehittäminen vaatii rahoitusta.

Haluamme erityisesti kiinnittää huomiota hyvinvointialueiden rahoitukseen. Viime vuosina on tullut merkittävää lainsäädäntöä ja määräyksiä, jotka vaikuttavat digiturvallisuuden vaatimuksiin

merkittäväs-ti. Esimerkkeinä mainittakoon Euroopan Unionin yleinen tietosuoja-asetus (EU 2016/679), kansallinen tietosuojalaki (1050/2018), laki sosiaali- ja terveystietojen toissijaisesta käytöstä (552/2019) sekä laki julkisen hallinnon tiedonhallinnasta (ns. tiedonhallintalaki, 906/2019). Hyvinvointialueita velvoittavan lainsäädännön lisäksi on myös annettu erilaisia määräyksiä ja suosituksia, jotka on otettava terveyden-huollon toiminnassa huomioon - esimerkkinä THL määräys 3/2021: Tietoturvasuunnitelmaan sisällytet-tävät selvitykset ja vaatimukset. Lainsäädännön asettavat velvoitteet (osoitusvelvollisuus, dokumentointivelvoitteet, lokitusvelvoitteet, koulutusvelvoitteet) asettavat merkittäviä vaatimuksia hyvinvointialueille sekä teknisesti että henkilöstöhallinnollisesti. Vaatimusten asianmukaisen toteuttamisen elinehtona on riittävä rahoitus, jolla voidaan turvata asianmukainen henkilöstöresurssi sekä tekniset tietoturvatoi-menpiteet. Rahoituksen arviointi tästä näkökulmasta on välttämätöntä.

Näiden vaatimusten toteuttaminen vaatii merkittävästi organisaation resursseja ja rahoitusta. Nämä eivät kuitenkaan ole lisänneet kuntayhtymien rahoituspohjaa. Tämä kaikki on pois lakisääteisten palveluijen tuottamisesta. Tämä tulee erityisesti huomioida hyvinvointialueiden rahoituksessa ja osoittaa erityisesti tietoturvallisuuden ja tietosuojan toteuttamiseen kohdistettua rahoitusta.

Kuopiossa 2.6.2022

Tuomo Pekkarinen tietohallintojohtaja PSSHP, muutosjohtaja Pohjois-Savon hyvinvointialue

Marko Ruotsala, tietoturvapäällikkö PSSHP

Katri Harjuveteläinen, lakimies PSSHP

Auli Mikkonen, tietosuojavastaava PSSHP, tietosuojavastaava Pohjois-Savon hyvinvointialue

Ruotsala Marko
Pohjois-Savon sairaanhoitopiirin kuntayhtymä