SeAMK
SEINÄJOEN AMMATTIKORKEAKOULU
SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

Tanju Holkko, Lea Kivenmäki ja Bumeh Oorehphe

Tietoturva osana potilasturvallisuutta hoitotyössä

Kuvaileva kirjallisuuskatsaus

Opinnäytetyö
Kevät 2022
Sairaanhoitaja (AMK)

SEINÄJOEN AMMATTIKORKEAKOULU

Opinnäytetyön tiivistelmä

Tutkinto-ohjelma: Sairaanhoitaja (AMK)

Tekijä: Tanju Holkko, Lea Kivenmäki ja Bumeh Oorehphe

Työn nimi: Tietoturva osana potilasturvallisuutta hoitotyössä: Kuvaileva kirjallisuuskatsaus

Ohjaaja: Marja-Kristiina Store, lehtori, THM ja Tarja Knuuttila, lehtori, TtM

Vuosi: 2022 Sivumäärä:48 Liitteiden lukumäärä:

Opinnäytetyön tavoitteena on tuottaa näyttöön perustuvaa tietoa hoitotyöntekijöille tietoturvaan liittyvistä tekijöistä, haittatapahtumien ennaltaehkäisystä ja tietoturvan edistämisestä hoitotyössä. Opinnäytetyön tarkoituksena on perehtyä tutkittuun tietoon ja tuottaa kuvaileva kirjallisuuskatsaus tietoturvasta osana potilasturvallisuutta hoitotyössä. Opinnäytetyön tehtävänä on etsiä vastauksia seuraaviin kysymyksiin: Mistä asioista tietoturva hoitotyössä muodostuu? Millaiset tekijät vaarantavat hoitotyössä tietoturvaa? Miten voidaan ennaltaehkäistä haittatapahtumia?

Menetelmänä on kuvaileva kirjallisuuskatsaus, joka toteutetaan sekä koti- että ulkomaisten artikkeleiden ja tutkimusraporttien perusteella.

Katsaukseen pohjautuen voidaan päätellä, että tietoturvan ylläpitäminen vaatii hoitohenkilökunnalta valppautta välttää tietoturvariskit ja tunnistaa poikkeavuudet, uusien työntekijöiden ja opiskelijoiden hyvää perehdyttämistä tietoturvakäytäntöihin, henkilöstön kouluttamista, sekä organisaation johdon hyvää kouluttautumista turvallisuuskulttuurin johtamiseen.

[1] Asiasanat: Tietoturva, tietosuoja, kyberturvallisuus, potilasturvallisuus, asiakasturvallisuus, hoitotyö

SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

Thesis abstract

Degree programme: Degree Programme in Nursing

Author/s: Tanju Holkko, Lea Kivenmäki and Bumeh Oorehphe

Title of thesis: Information security part of patient safety in healthcare: Descriptive literature review

Supervisor(s): Marja-Kristiina Store, Lecturer, THM ja Tarja Knuuttila, Lecturer, TtM

Year: 2022 Number of pages:48 Number of appendices:

The aim of the thesis is to provide evidence-based information for nurses on information security related factors, to prevent harmful events and to promote the information security in nursing. The purpose of the thesis is to investigate the researched data and to produce a descriptive literature review with information security as part of patient security in nursing. The target of the thesis is to seek answers to the following questions: What are the aspects that information security consists of? What are the aspects that endanger information security in nursing? How to prevent harmful events?

The method is to produce a descriptive literature review based on both domestic and foreign articles and research reports.

Based on the review, it can be inferred that maintaining information security requires healthcare staff to be vigilant in avoiding information security risks and identifying anomalies, good orientation for new employees and students about information security policies, educate the staff, and good training for the organization's management in the management of safety culture.

[1] Keywords: Information security, data safety, cyber security, patient safety, customer security, healthcare

SISÄLTÖ

Kuvio- ja taulukkoluettelo

Käytetyt termit

Asiakasturvallisuus tarkoittaa sosiaali- ja terveydenhuollossa toimivien henkilöiden ja organisaatioiden periaatteita ja toimintoja, joilla varmistetaan hoidon, hoivan ja palvelujen turvallisuus ja suojataan asiakkaita tai potilaita vahingoittumasta.

Henkilötiedot tarkoittavat kaikkea tietoa, jotka liittyvät tunnistettuun tai tunnistettavissa olevaan henkilöön. Esimerkiksi nimi, puhelinnumero, sijaintitieto ja terveystiedot.

Kyberturvallisuus tarkoittaa sähköisen ja verkotetun yhteiskunnan turvaamista. Kyberturvallisuudessa pyritään tunnistamaan, ehkäisemään ja varautumaan sähköisten ja verkotettujen järjestelmien häiriöiden vaikutuksiin yhteiskunnan kriittisiin toimintoihin.

Potilasturvallisuus tarkoitetaan toimintaperiaatteita ja -tapoja, joilla varmistetaan hoidon turvallisuus ja suojataan potilasta vahingoittumiselta.

Tietosuoja on perusoikeus, joka turvaa yksilön oikeudet henkilötietojen käsittelyssä. Tietosuoja rajaa, milloin ja millä edellytyksillä henkilötietoja voidaan käsitellä ja millaisia oikeuksia yksilöllä on omiin tietoihinsa. Tarkoituksena on estää tietojen luvaton saanti, säilyttää luottamuksellisuus ja suojata henkilöä vahingoittavalta käytöltä.

Tietoturva tarkoittaa tietojen, tietojärjestelmien ja tietoliikenteen turvaamista.

Tietoturvallisuus tarkoittaa yksityisyyden, ennen kaikkea tiedon laadun ja eheyden koskemattomuuden säilyttämiseen ja suojaamiseen kohdistuvia toimenpiteitä. Tietoturvallisuus liittyy keskeisesti riskienhallintaan, hallintoon ja palveluihin, kehittämiseen, resurssien suunnitteluun sekä toiminnan sisäiseen että ulkoiseen tarkastukseen.

1 JOHDANTO

Tietosuoja kuuluu jokaisen henkilön perusoikeuksiin (Terveyskylä, 2020). Tietosuoja sisältää henkilötietojen yksityisyyden turvaamisen niitä käsiteltäessä. Potilastiedot ovat henkilötietoja, koska tietojen perusteella henkilö voidaan tunnistaa. Tietojen käsittely ja säilytys tulee tapahtua yksityisyyttä vaarantamatta. Tietoturva käsittää tietosuojattujen tietojen turvaamisen. Terveydenhuollossa on tärkeää päästä tarvittaviin potilastietoihin, että potilasta voidaan hoitaa mahdollisimman hyvin. Potilastietoja saa katsella vain ammattilaiset, joilla on siihen lupa. Tietoturva kattaa muun muassa e-terveyspalveluissa käytössä olevan vahvan tunnistautumisen Kanta-palveluun.

Tietosuoja on lakiin perustuva oikeus, joka turvaa viranomaisten ja yksityisten tahojen ylläpitämien henkilötietorekisterien tiedot salassapitovelvollisuudella (Suomen lääkäriseura Duodecim, 2017). Henkilöllä on myös oikeus tutustua hänestä kirjattuihin tietoihin ja saada niihin tarvittaessa poistoja ja korjauksia. Hyvä tietosuojaosaaminen terveydenhuollon toiminnassa hyödyttää kaikkia. Työntekijän oikeusturva paranee samoin kuin tietosuojakin, kun työntekijän tietoja, esimerkiksi terveystietoja tai sairauslomatietoja, käsitellään oikeaoppisesti. Osaamisella voidaan vaikuttaa työviihtyvyyteen ja saada hyötyä myös muille elämänalueille. Organisaatiotasolla hyvä tietosuojaosaaminen parantaa toiminnan laatua ja lisää luottamusta toimintaan. Kun tietoja osataan käsitellä oikein, säästyy aikaa ja resursseja. Tiedon oikeaoppinen käsittely vähentää riskien todennäköisyyttä ja vaikutuksia, jolloin vältytään valvontaviranomaisen puuttumiselta organisaation toimintaan sekä sakoilta ja muilta sanktioilta. Asiakkaan kannalta oikein mitoitettu tietosuoja lisää joustavuutta ja parantaa toiminnan laatua. Myös luottamus organisaation toimintaan ja toiminnan lainmukaisuuteen kasvaa.

Sosiaali- ja terveysministeriön (2017) mukaan potilasturvallisuus on keskeinen osa hoidon laatua. Potilasturvallisuuteen kuuluu sosiaali- ja terveydenhuollon osaava henkilökunta sekä tilojen, laitteiden, tarvikkeiden ja lääkkeiden tarpeenmukaisuus ja oikea käyttö. Sosiaali- ja terveydenhuollon dokumentoinnin ja tiedonkulun tulee olla turvattua. Tarkoituksena on varmistaa hoidon ja palvelujen turvallisuus sekä suojata potilaita vahingoittumasta. Potilasturvallisuus ja laadun edistäminen on osa sosiaali- ja terveydenhuollon järjestämisvastuuta. Palvelun tuottajien vastuuseen kuuluu, että potilasturvallisuus varmistetaan käytännössä.

Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (784/2021, 1 luku 1 §) määrää tarkoituksen edistää ja mahdollistaa sosiaali- ja terveydenhuollon tuottamien asiakastietojen ja asiakkaan itsensä tuottamien hyvinvointitietojen tietoturvallista käsittelyä terveydenhuollon ja sosiaalipalveluiden järjestämisen ja tuottamisen käyttötarkoituksissa (Valvira, 2021). Lain tarkoituksena on myös edistää asiakkaan tiedonsaantimahdollisuuksia asiakastietojensa käsittelystä. Sama laki määrittelee yleiset vaatimukset tietojärjestelmille ja niiden valmistajille sekä sosiaali- ja terveydenhuollon palvelun antajille. Valvira valvoo sosiaali- ja terveydenhuollon asiakas- ja potilastietojen käsittelyyn tarkoitettujen tietojärjestelmien olennaisten vaatimusten toteutumista. Tietojärjestelmällä tarkoitetaan sosiaali- tai terveydenhuollon asiakastietojen sähköistä käsittelyä varten toteutettua ohjelmistoa tai järjestelmää, jonka avulla tallennetaan ja ylläpidetään asiakas- tai potilasasiakirjoja ja niissä olevia tietoja.

Etelä-Pohjanmaan sairaanhoitopiirin (EPSHP) Steppi-hanke (2016–2020) on ollut perushoidon laadun tutkimus- ja kehittämishanke, jonka jälkeen on käynnistynyt Steppi2 (Etelä-Pohjanmaan sairaanhoitopiiri i.a.). Tämä opinnäytetyö liittyy Steppi2:een, jonka teemana on laadukas kirjaaminen, hoitotyön päätöksenteko ja potilaan voinnin muutosten huomiointi ja kuvaaminen kirjaamisessa. Steppi2 - Terveyttä tuottava perushoito (2021–2025) on perushoidon kehittämiseen ja tutkimukseen keskittynyt avoin verkosto. Mukana Steppi-hankkeessa on useita sairaanhoitopiirejä ja eri koulutustahoja.

Tässä opinnäytetyössä käsitellään pääosin tietoturvallisuutta ja sitä, kuinka potilasturvallisuutta voidaan edistää tietoturvallisuuden näkökulmasta, huomioiden myös kyberturvallisuus, jonka vaaran mahdollistaa langattomien nettiyhteyksien ja pilvipalvelun käytön lisääntyminen. Tietoturvallisuus hoitotyössä käsittää sekä paperisen että sähköisen henkilötietojen käsittelyn, asiakirjojen laatimisen, käytön, dokumentoinnin, säilytyksen, hävityksen ja tietojen luovutuksen.

2 TIETOTURVALLISUUS OSANA HOITOTYÖTÄ

Turvallisten ja laadukkaiden palvelujen toteuttaminen sosiaali- ja terveydenhuollossa edellyttää toimivaa tiedonhallintaa, koska käytettävissä oleva tieto on hoitoihin ja palveluihin liittyvien päätöksien perusteena (Kurki ym. 2021, s. 117). Tiedonhallinta on monivaiheinen prosessi, jonka muodostaa yksilön ja organisaation tiedontarpeen määrittely, tarvittavan tiedon hankinta, tiedon organisointi ja tallentaminen, tiivistäminen ja esittäminen sekä levittäminen ja käyttö sosiaali- ja terveydenhuollon palveluissa. Asiakasturvallisuus toteutuu parhaiten, jos tiedonkulku ja kirjaaminen eivät poikkea toisistaan eri yksiköissä. Varsinkin asiakkaan tai potilaan siirtyessä yksiköstä tai organisaatiosta toiseen yhtenäinen kirjaamismalli helpotta tiedonkulkua (mts. 118).

Tietoturvan ja tietosuojan kehittäminen ja ylläpito sekä sen seuranta ovat osa yleistä turvallisuustoimintaa ja riskien hallintaa sekä sisäistä valvontaa (EPSHP, 2021, s. 3). Tietoturva perustuu tiedon luottamuksellisuuteen, käytettävyyteen, saatavuuteen, eheyteen ja kiistämättömyyteen sekä tietojen käsittelyn valvontaan. Tietoturvan hallintaan liittyvät käsittelijöiden toimintatavat, tietojen turvaamisen menetelmät, tietoturvaorganisaatio, välineet ja toimenpiteet, työhön osoitetut resurssit sekä välineistön ja tilojen tietoturvaominaisuudet (mt.).

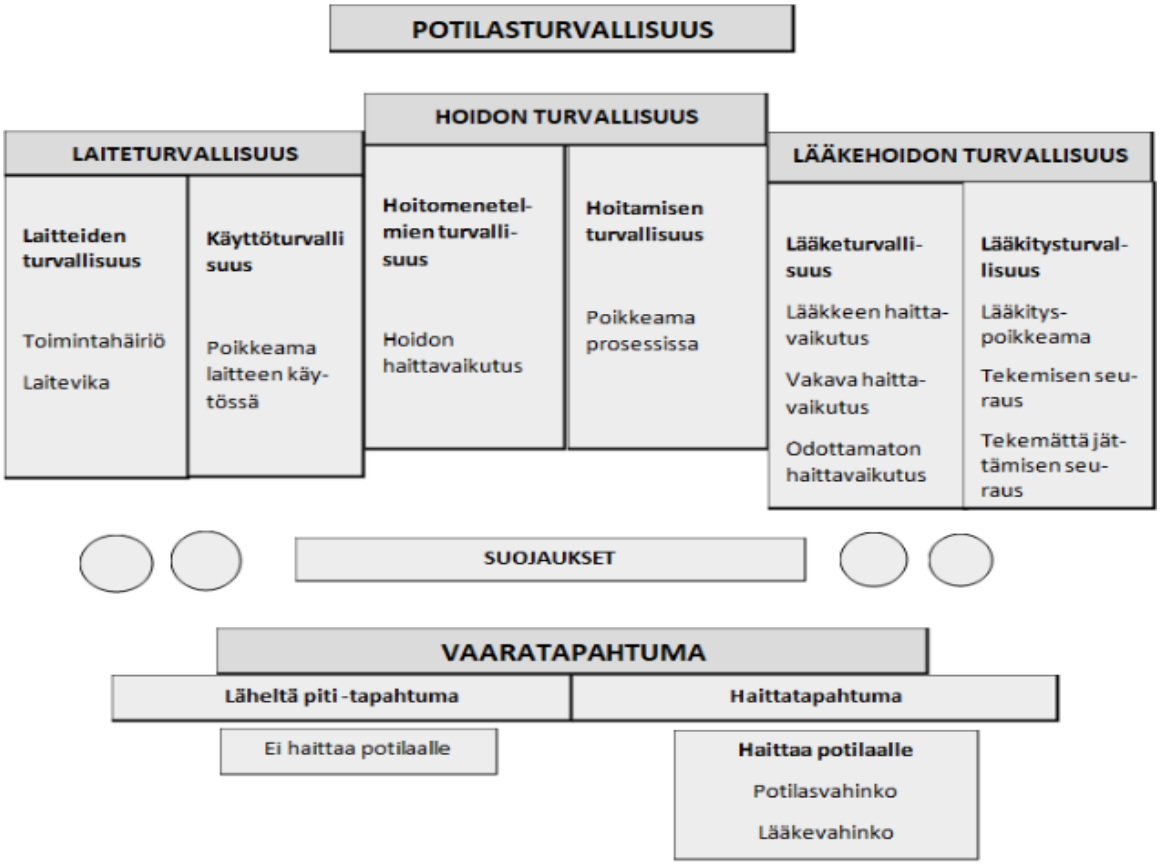
2.1 Tietoturva osana potilasturvallisuutta

Tietoturva tarkoittaa palvelujen, järjestelmien, tietojen ja tietoliikenteen suojaamista (EPSHP, 2021, s. 1). Tietosuoja on tietoturvallisuuden oleellinen osa. Tietosuoja tarkoittaa henkilön luottamuksellisten tai arkaluonteisten tietojen ja muiden henkilötietojen suojaamista. Tietosuoja on rekisteröidyn henkilön oikeutettujen oikeuksien ja vapauksien tehokasta toteuttamista. Tietosuojan keskeiset periaatteet ovat lainmukaisuus, läpinäkyvyys ja kohtuullisuus (mts. 2).

Potilaan turvallisuutta uhkaavat laitteiden häiriöt ja käyttöongelmat, hoitoprosessissa sattuvat poikkeamat ja lääkevirheet (Kinnunen & Helovuo, 2019). Suurin osa lääkevirheistä tapahtuu lääkehoidon prosesseissa. Jos potilaalle aiheutuu haittaa lääkehoidosta, kyse voi olla lääkehoidossa tapahtuvasta poikkeamasta tai lääkevalmisteen haitallisesta vaikutuksesta. Laitteista aiheutuvissa haittatapahtumissa ongelma saattaa johtua laitteen

toiminnasta tai sen käytöstä. Jokaisella käyttäjällä tulee olla asianmukainen perehdytys laitteen turvalliseen käyttöön, jonka laki terveydenhuollon laitteista ja tarvikkeista 629/2010 vaatii (mt.).

Potilasturvallisuus tarkoittaa sitä, että potilaalle ei saa aiheutua haittaa hoidosta (Autti & Keistinen, 2013, s.141). Potilaalle tämä tarkoittaa, että hän saa tarvitsemansa ja oikean hoidon, josta tulee mahdollisimman vähän haittaa. Kinnunen ja Helovuo (2019) kuvastaa potilasturvallisuuteen kuuluvan hoidon turvallisuus, lääketurvallisuus ja laiteturvallisuus (kuvio 1).



Kuvio 1. Potilasturvallisuus (mukaellen Kinnunen ja Helovuo, 2019)

2.2 Tietoturvallisuus hoitotyössä

Useimmille sosiaali- ja terveydenhuollon ammattilaisille sähköisessä muodossa olevien asiakas- ja potilastietojen käsitteleminen kuuluu osana päivittäistä työtä (Konttinen & Mykkänen, 2016, s.134). Mikäli organisaatio on liittynyt Kanta-palveluun, tietoja voidaan

luovuttaa eri palveluntuottajien välillä valtakunnallisesti. Tietojen luovuttamiseen eri rekisterinpitäjien välillä tarvitaan potilaan suostumus. Potilaalla on lakisääteinen oikeus antaa suostumus omien terveystietojensa luovutukseen tai kieltää luovuttaminen. Potilastietojen sähköisessä käsittelyssä suostumuksella on oleellinen merkitys. Omakanta-palvelun kautta kansalaisen on mahdollista tarkistaa terveydenhuollon organisaatiot, joissa hänen tietojaan on käsitelty ja luovutettu (mt.). Sosiaali- ja terveydenhuollon asiakas- ja potilastietojen rekisterinpitoa, rekisterinpitäjien vastuita sekä arkaluonteisen tiedon käsittelyä koskevat säädökset ovat henkilötietolaki (523/1999), laki asiakastietojen sähköisestä käsittelystä (159/2007, myöhemmin asiakastietolaki), terveydenhuoltolaki (1326/2010) sekä niihin liittyvät asetukset (Konttinen & Mykkänen, 2016, s.134).

Tietoturvallisuuden kannalta tärkeimmät turvattavat kohteet ovat henkilöt, tilat, tietoliikenne, tietojärjestelmät, ohjelmistot, laitteet, palvelut sekä tiedot ja tietoaineistot kaikissa olomuodoissaan (EPSHP, 2021. s. 6). Näiden kohteiden turvaamisen tavoitteena on operatiivisten järjestelmien ja sisäisen tietojenkäsittelytoiminnan ja tietosuojan turvaaminen. Tavoitteisiin kuuluu myös palvelujen tuottaminen normaalioloissa ja normaaliolojen häiriötilanteissa, sekä poikkeustilanteissa.

Hoitotyössä potilaan hoidon kannalta tarvittavien tietojen hyvä ja perusteellinen kirjaaminen on pohja hyvälle tiedonkululle, johon laadukas ja turvallinen hoito perustuu (Helovuo, ym. 2011, s. 72). Dokumentointia ohjaavat lainsäädäntö sekä erilaiset ohjeistukset. Hoitotyössä dokumentointi on ammattilaisten keskeinen työtehtävä. Kirjaaminen tulee tehdä selkeästi ja välittömästi. Katkeamattomalla tiedonkululla ja välttämällä väärinymmärryksiä voidaan ehkäistä haittatapahtumia esimerkiksi silloin, kun potilas siirtyy yksiköstä toiseen.

Sähköisten potilastietojärjestelmien tavoitteellinen tehtävä on tuottaa tarvittavia tietoja ja raportteja potilaasta terveydenhuollon työntekijöiden käyttöön välittömästi (Helovuo, ym.2011, s.73). Tietotekniikan ja kehittyneen teknologian käyttö vaatii varautumista ja suunnitelmaa tilanteeseen, jossa potilastietojärjestelmä mahdollisesti kaatuisi. On oltava valmiiksi selvitettynä, että kuinka kriittiset potilastiedot, esimerkiksi lääkitys, voidaan selvittää poikkeustilanteessa (mt.).

Andreasson ym. (2013, s. 45) kirjoittaa ohjeet organisaation tietoturva- ja tietosuojasta. Ohjelmistoja ei saa asentaa tai tehdä muutoksia, ellei se kuulu työtehtävään. Tehty työ tulee tallentaa mieluiten verkkopalvelimen levylle. Suojaamaton ja ei säännöllisesti varmuuskopioitu tietokoneen paikallinen kovalevy on huonoin vaihtoehto tallentaa tietoja. Organisaation laitetta, verkkoa tai sähköpostia käytettäessä tulee muistaa, että työntekijä näkyy ja esiintyy tietoverkossa aina tahtomattakin organisaation edustajana. Aineistoa siirrettäessä muistitikulle tai muuhun muistivälineeseen tulee valvoa siirtoa aina henkilökohtaisesti. Siirron jälkeen tulee poistaa huolellisesti tiedot. Tietoturvallisuuteen tai tietosuojaan liittyvistä ongelmatilanteista ja havaituista uhkista sekä suojapuutteista tulee ilmoittaa välittömästi esimiehelle tai sovitulle tukihenkilölle (mt.).

2.2.1 Tietojärjestelmiin tunnistautuminen

Tietojärjestelmiin tunnistaudutaan monivaiheisen tunnistuksen kautta sekä sisällön mukaan (Tenhunen, 2018, s. 11). Monivaiheisessa tunnistuksessa käytetään kahta tai useampaa tunnistusmenetelmää varmennettaessa käyttäjän identiteettiä. Tällä pyritään estämään järjestelmän luvaton käyttö. Lähes kaikki kaappausyritykset voidaankin estää käyttämällä kahta tai useampaa tunnistautumistapaa (Traficom i.a.). On myös huolehdittava, että käytettävän tietokoneen suojaus on kunnossa. Tunnistautuminen aloitetaan yleensä ilmoittamalla oma käyttäjätunnus ja salasana, jolloin henkilöllisyys varmistetaan. Koska käyttäjätunnus on usein sähköpostiosoite ja salasana jokin helposti arvattavissa oleva, esimerkiksi henkilötunnus ja sama salasana voi olla käytössä useissa palveluissa, on suuri vaara joutua tietomurron uhriksi. Yksilöivän tiedon käyttö, esimerkiksi matkapuhelimeen lähetetty kertakäyttöinen koodi, mobiilivarmenne, sormenjälkitunnistus sekä tunnistautumispalvelun käyttö käyttäjätunnuksen ja salasanan lisäksi vahvistavat tietosuojan vaikeasti murrettavaksi. Monivaiheinen tunnistautuminen suositellaankin otettavaksi käyttöön palveluissa, joissa on henkilö- tai maksutietoja sekä yritysten käytössä olevilla tileillä.

2.2.2 Tietojärjestelmien valvonta hoitotyössä

Sosiaali- ja terveydenhuollon organisaatiossa asiakas- ja potilastietojärjestelmien käyttövaltuuksien, tietojärjestelmiin pääsyn ja käytön seuranta kuuluu säännöllisen omavalvonnan toteuttamiseen (Konttinen & Mykkänen, 2016, s.142). Omavalvonnan toteuttamisen tueksi

laki velvoittaa sosiaali- ja terveydenhuollon palveluntuottajat, apteekit, itsenäiset ammatinharjoittajat, Kansaneläkelaitoksen ja Kanta-välityspalveluiden tuottajat laatimaan omavalvontasuunnitelman (mts.135). Omavalvontasuunnitelmassa määritellään päivittäiset toimet tietoturvan ja –suojan toteutumisen varmistamiseksi ja seurannan toteuttamiseksi. Jokaisen asiakas- ja potilastyötä tekevän on vastattava siitä, että noudattaa tietosuoja- ja tietoturvaohjeita omassa toiminnassaan (mts.136). Omavalvontasuunnitelman laatimisesta ja toimimisesta sen mukaisesti vastaa organisaation johto, joka myös vastaa, että organisaatiossa on nimetty tietosuojavastaava. Johto huolehtii, että organisaatiossa kaikki asiakas- ja potilastietoja käsittelevät työntekijät ovat tietoisia omavalvontaan kuuluvista toimenpiteistä ja tietojärjestelmän käyttölokista, johon jää jälki kaikesta asiakas- ja potilastietojen sähköisestä käsittelystä, tietävät tahallisten väärinkäytösten seuraamukset sekä ovat perehtyneet tietosuoja- ja tietoturvaohjeisiin (mts.135).

Tietojärjestelmäpalvelun tuottajien on asiakastietolain (159/2007) mukaan osoitettava ennen Kanta-palveluihin liittymistä, että kansalliset tietosuoja- ja tietoturvavaatimukset täyttyvät (Konttinen & Mykkänen, 2016, s.135). Järjestelmän sertifiointiin kuuluu myös ilmoitus käyttötarkoituksesta, yhteensopivuuden testaus muihin Kanta-palveluihin liittyvien järjestelmien kanssa sekä järjestelmän kirjaaminen Valviran rekisteriin. Tietoturvan ja tietosuojan toteutumiseksi sosiaali- ja terveydenhuollon palveluntarjoajat, apteekit, itsenäiset ammatinharjoittajat, Kansaneläkelaitoksen ja Kanta-välityspalvelujen tuottajat ovat velvoitetut laatimaan omavalvontasuunnitelman, jonka avulla ylläpidetään ja kehitetään tietoturvaa ja tietosuojaa organisaatiossa.

Asiakas- ja potilastietojärjestelmien käytön seuranta on organisaatioiden velvoite (Konttinen & Mykkänen, 2016, s.142). Käyttöä seurataan automaattisten ajojen avulla terveydenhuollon toimintayksiköissä (Rajaniemi, 2020, s. 2493). Säännöllisessä omavalvonnassa käytön seuranta kuvataan ja toteutetaan nojautuen lokitietoihin, joita syntyy käytettäessä järjestelmiä ja luovutettaessa tietoja (Konttinen & Mykkänen, 2016, s.142). Tenhusen (2018, s. 12) mukaan lokitiedoista pitäisi selvitä kenen tunnuksella potilastietoja on käsitelty, mitä kohdetta on käsitelty sekä milloin ja mistä tiedosto on avattu. Käyttöä myös valvotaan (mt.). Lokitietojen tarkastuksia tehdään yhä useammin myös potilaiden pyynnöstä (Rajaniemi, 2020, s. 2493). Epäasiallinen ja luvaton tietojen käyttö johtaa seuraamuksiin, mikä kaikkien organisaatiossa asiakas- ja potilastietoja käsittelevien tulee tietää (Konttinen & Mykkänen,

2016, s. 142). Myös mahdollisen lainvastaisen tietojenkäsittelyn varalle on oltava toimintamalli.

Kirjauduttaessa järjestelmään käyttäjä tunnistetaan ja todennetaan (Konttinen & Mykkänen, 2016, s. 142). Kirjautumisessa tunnukset ovat henkilökohtaisia. Yhteiskäyttöisiä käyttäjätunnuksia ja salasanoja järjestelmään ei saa olla, jotta käyttäjien, ammattilaisten ja asiakkaiden oikeusturva väärinkäytös- ja vahinkotilanteissa säilyisi. Oikean kirjautumiskäytännön on oltava tiedossa ja kaikkien selvillä siitä, että käyttöä seurataan omavalvonnalla.

Ammattikorttia käytettäessä on tärkeä noudattaa erityistä huolellisuutta, koska se antaa mahdollisuuden päästä moniin potilastietojärjestelmissä oleviin tiedostoihin, esimerkiksi Kannassa oleviin lääkitystietoihin (Rajaniemi, 2020, s. 2493). Pin-koodi ja ammattikortti on turvallista säilyttää erillään, koneen luota poistuttaessa tietojärjestelmä tulisi lukita tai sulkea ja ammattikorttia ei pitäisi jättää lukulaitteeseen edes omassa työhuoneessaan (mt.).

Seppänen (2020, s. 2820) kirjoittaa Lääkärilehdessä, että potilastietojärjestelmien tietoturvallisuuden arvioinnissa on paljon vaihtelua. Julkisen terveydenhuollon toimijat, sekä toimijat, joilla on käytössä sähköinen resepti tai potilastiedon arkisto, kuuluvat A-luokkaan, jossa tietoturvallisuuden arvioinnin tekee ulkopuolinen arvioitsija ja järjestelmä on integroitu Kanta-palveluun. Kaikki muut potilastietojärjestelmät kuuluvat B-luokkaan, joissa tietoturvallisuuden arviointiin ei tarvita ulkopuolista arviointia, oma ilmoitus riittää. B-luokkaan kuuluvista järjestelmistä osa on yhteydessä Kantaan välittäjäpalvelun avulla (mt.). Yksityisellä sektorilla, pienillä toimijoilla voi olla käytössä järjestelmä, joka on itse tehty eikä ole liitettynä Kantaan. Myös hyvin vanhoja järjestelmiä, jotka eivät ole A- tai B-luokkaa, on käytössä. Jotta voidaan varmistua tietoturvavaatimusten täyttymisestä, käytössä oleva potilastietojärjestelmä pitäisi löytyä Valviran ylläpitämästä rekisteristä (mts. 2821). Työnantajalta voi myös tiedustella onko tietoturvasuunnitelmaa ja riskiarviota tehty sekä kuka on tietoturvavastaava. Nämä tiedot pitäisi olla saatavilla, muutoin voi päätellä, että tietoturva-asioissa luotetaan pelkästään hyvään onneen.

2.2.3 Muita tietoturvatoimia

Tietokoneen tiedostot olisi hyvä varmuuskopioida niin organisaatiossa kuin kotikoneellakin (Palmu, 2019). Tietokone voi joutua varkauden kohteeksi tai hävitä, tallennuslevy (SSD tai kovalevy) voi hajota tai jokin haittaohjelma tekee tiedostot käyttökelvottomiksi tai salaa ne, jolloin varmuuskopiolta saadaan palautettua tärkeät tiedot. Varmuuskopiointi voi tapahtua käyttämällä USB-muistia tai tietokoneella olevaa varmistusohjelmistoa, joka internetin kautta varmistaa tiedostot tietyistä kansioista niiden muuttuessa tai uusien syntyessä. Tiettyyn kansioon tallennusta voidaan myös käyttää, jolloin tiedostot synkronoidaan esimerkiksi yrityksen verkkolevylle. Suositeltavaa olisi käyttää kahta varmuuskopiointimallia samanaikaisesti.

Levynsalauksella estetään ulkopuolisen pääsy tiedostoihin, esimerkiksi laitteen hävitessä (Palmu, 2019). Levynsalaus voi olla jo valmiiksi päällä uudessa koneessa, mutta ellei ole, olisi hyvä laittaa. Nykyisin levynsalaus ei vaadi enää erillistä ohjelman asentamista.

Sosiaali- ja terveydenhuollossa työskenneltäessä salassapitoon liittyvien asioiden ymmärtäminen on avainasemassa (Andreasson ym., 2013, s. 22). Tärkeimmät päämäärät ovat potilaan hoidon onnistumisen turvaaminen ja luottamuksellisessa hoitosuhteessa yksilön yksityisyyden suojaaminen. Salassapito tarkoittaa asiakirjasalaisuuden säilyttämisvelvollisuutta ja vaitiolovelvollisuutta. Vaitiolovelvollisuus sisältää asiakirjan salassa pidettävän sisällön ilmaisun kieltämistä. Ilmaiseminen tarkoittaa tiedon antamista ja paljastamista suullisesti sekä passiivisesti ulkopuolisille. Esimerkiksi asiakirjan, mikä sisältää salassa pidettävää tietoa, jättäminen ulkopuolisten saataville, voi loukata asiakirjasalaisuuden säilyttämisvelvollisuutta. Kaikkia sosiaali- ja terveydenhuollossa työskenteleviä koskee aina juridinen salassapitovelvollisuus, mukaan lukien harjoittelijat, opiskelijat, siviilipalvelusmiehet jne. (mts. 23). Muita kuin työtehtäviä varten salassa pidettävien tietojen selville ottaminen on ehdottomasti kiellettyä ja teko on rangaistava (mts. 26). Jos tietoja käsittelee ilman oikeuksia, teosta voi seurata rikos-, työ-, ja vahingonkorvausoikeudellisia seuraamuksia. Työskentelyn päättymisen jälkeenkin salassapitovelvollisuus jatkuu. Asiakkaan kuoleman jälkeen asiakirjat ja tiedot ovat salassa pidettäviä. Kaikkia salassa pidettäviä tietoja koskee salassapitovelvollisuus (riippumatta siitä, millä tavalla tieto on saatu tai mihin tai miten ne on tallennettu).

Henkilöstöturvallisuuden tavoitteena on varmistaa ennen työsuhteen alkua, että ulkopuoliset käyttäjät, toimittajat ja työntekijät ymmärtävät velvollisuutensa ja ovat sopivia heille harkittuihin tehtäviin (Andreasson ym., 2013, s. 35). Tavoitteena on myös vähentää petoksia, varkauksia sekä riskejä palvelujen väärinkäytöstä (mts. 36). Riskien ehkäisemiseksi yksi keino on tarkistaa ulkopuolisten käyttäjien, toimittajien ja työntekijöiden tausta noudattaen lakeja, eettisiä normeja ja määräyksiä. Tavoitteena on, että työnsuhteen aikana ulkopuoliset käyttäjät, toimittajat ja työntekijät ovat tietoisia tietoturvallisuuteen kohdistuvista uhkista ja niiden merkityksestä sekä omista velvollisuuksistaan ja vahinkovastuustaan. Tavoitteena on, että tehdessään normaalia työtään heillä on keinot tukea organisaation turvallisuuspolitiikkaa. Inhimillisen erehdyksen riskin vähentäminen on myös tavoitteena. Tärkeimpiä kohtia ovat johdon vastuu, koulutukset, sanktiomenettelyt sekä tietoturvaan liittyvät ohjeet. Työsuhteen päättymisen tai muuttamisen yhteydessä tulee varmistaa, että organisaatio tai työsuhde jätettäessä toimitaan järjestelmällisellä tavalla. Kaikki organisaation suojattavat asiakirjat tai muut kohteet palautetaan työsuhteen tai sopimuksen päättyessä. Käyttöoikeudet tietoon ja tietojenkäsittelypalveluihin tulee poistaa tai korjata muutosten mukaisesti työsuhteen tai sopimuksen päättyessä.

Luvaton tunkeutuminen organisaation toimintoihin ja tietoaineistoihin estetään turva-alueilla, samoin kuin niiden vahingoittuminen ja toiminnan häiriintyminenkin (Andreasson ym., 2013, s. 36). Toimitiloja pitäisi suojata asianmukaisella kulunvalvonnalla ja laitteiden fyysisellä turvallisuudella (mts. 37). Ominaisuuden häviäminen, varastaminen, vahingoittuminen, vaarantuminen ja organisaation toiminnan keskeyttäminen estetään laiteturvallisuudella. Laitteistot tulee suojata ja sijoittaa siten, että luvattoman tunkeutumisen ja ympäristövaarojen riskejä vähennetään. Laitteistoja pitäisi suojata sähkökatkoilta ja muilta peruspalveluiden katkosten aiheuttamilta häiriöiltä. Salakuuntelulta ja vaurioilta tulee suojata tietoliikennekaapeloinnilla. Laitteistojen huollosta on huolehdittava eheyden ja asianmukaisen käytettävyyden ylläpitämiseksi. Kaikki laitteen osat, mitkä sisältävät tallennettua tietoa tulee tarkistaa, jotta voidaan varmistua siitä, että tekijänoikeuden suojaamat ohjelmat ja arkaluontoinen tieto on turvallisesti poistettu tai tuhottu ennen laitteen poistamista käytöstä.

Toimitilojen tulee olla turvallisia, jolloin tietokonelaitteita, asiakirjoja ja tietoja käsitellään ja säilytetään asianmukaisesti turvallisissa tiloissa (Andreasson ym., 2013, s. 50). Kulunvalvonta, tekninen valvonta ja vartiointi, murto-, ilmastointi-, sähkö-, vesi- ja palovahinkojen

torjunta sekä tietoaineistoja sisältävien lähetysten ja lähettipalvelujen turvallisuuden varmistaminen kuuluu toimitilojen turvallisuuden varmistamiseen samoin asiakaspalvelupisteessä tai -tilanteissa harkitusti suunnattu tietokoneen näyttö. Kulunvalvonnasta annettuja ohjeita tulee noudattaa (mts. 51). Organisaation toimitiloissa tulee käyttää kuvallista henkilökorttia, jos sellainen on annettu. Vierailuihin käytetään neuvottelu- ja kokoustiloja ja huolehditaan, ettei neuvottelutiloissa ole asiaankuulumatonta materiaalia esillä. Neuvottelun päättyessä tulee huolehtia, ettei tilaan jää luottamuksellista aineistoa. Kannettavaa tietokonetta ja matkapuhelinta ei tule jättää ilman valvontaa ja laitteita tulee säilyttää lukitussa tilassa mukaan lukien muistitikut, CD- ja DVD-levyt ja paperitulostimet. Työpöydällä ei tule säilyttää salassa pidettäviä tietoja. Vierasta ei pidä jättää yksin työhuoneeseen tai muihin toimitiloihin ilman valvontaa. Vieraat ja eksyneet ohjataan aina oikeisiin paikkoihin. Aina olisi varmistettava, että lukittavat ovet menevät lukkoon niistä kuljettaessa.

Andreasson ym. (2013, s. 40) kirjoittaa, että tietojärjestelmien turvallisuusvaatimuksilla tulee varmistaa, että tietojärjestelmät kehitetään turvallisiksi. Tavoitteena on estää sovellusten sisältämän tiedon virheet, katoaminen, luvaton muuttaminen ja väärinkäyttö. Tätä voidaan estää syöttötietojen oikeellisuuden tarkistuksilla, viestien aitouden ja eheyden varmistamisella, sisäisen käsittelyn valvonnalla sekä varmistamalla tulostustietojen oikeellisuus. Salakirjoitusmekanismeilla tulee suojata tiedon luottamuksellisuus, alkuperäisyys tai eheys. Järjestelmätiedostojen turvallisuutta pitäisi varmistaa valvomalla ohjelmien lähdekoodit sekä tuotannossa käytettäviä ohjelmistoja ja suojaamalla testiaineistot. Tuki- ja kehitysprosessien turvallisuus on kokonaisuus. Tuki- ja kehitysprosessin tavoitteena on sovellusjärjestelmien ohjelmien ja tietojen turvallisuuden ylläpito, ja tähän kuuluvat muutosten valvonta menettelyt ja tietovuotojen mahdollisuuksien ehkäiseminen sekä tarkastukset. Ajantasaista tietoa tulee hankkia käytettävien tietojärjestelmien teknisistä haavoittuvuuksista. Organisaation altistuminen näille haavoittuvuuksille tulee arvioida ja riskit käsitellä asianmukaisilla toimenpiteillä.

2.2.4 Koko käsittelyketjun tietoturvallisuudesta varmistuminen

Päijät-Hämeen kyberhyökkäyksen aikana jouduttiin katkaisemaan verkkoyhteys työasemilta vahinkojen ehkäisemiseksi, ulkopuolisiin verkkoihin tai internettiin yhteys katkaistiin kokonaan (Sand, 2019). Verkon katkaiseminen johti häiriöihin asumispalvelujen turvalaitteissa, lääkintälaitteissa sekä sähköisissä lukitus- ja hälytysjärjestelmissä. Työntekijöiden

pääsy Käypä hoito -suositukseen, vanhoihin Effica -kantoihin, verkkotulostimiin ja myrkytyskeskuksen ohjeisiin estyi (mt.).

Sand (2019) kirjoittaa artikkelissaan, että vuonna 2019 Päijät-Hämeen kyberhyökkäystapauksessa ei tullut yhtään vakavaa potilas- tai asiakasvahinkoa. Lievempiä vahinkoja ja läheltä piti- tilanteita kuitenkin syntyi. Tapauksesta opittiin, että kyberhyökkäyksessä johtamisen tulee olla keskitettyä ja suoraviivaisempaa kuin normaalioloissa, yhteistyötahot, henkilöstö sekä väestö tulee pitää ajan tasalla. Tiedottaminen on tärkeässä roolissa, vaikka aina ei olisi uutta kerrottavaa. Varautuminen kriisiin perusteellisilla ohjeistuksilla ja harjoituksilla on ehdoton edellytys. Tietoliikenneuhilta ei voi olla suojassa, mutta varautuminen pienentää riskiä, sekä samalla varmistaa toipumisen nopeammin.

Phillion (2021, s. 5) kirjoittaa artikkelissaan, että kyberhyökkäykset kohdistuvat kaikkiin toimialoihin koko ajan ja terveydenhuolto ei ole poikkeus. Tuoreen IBM-tutkimuksen mukaan terveydenhuollon kyberhyökkäystä kohti keskimääräiset kustannukset ovat noin 7 miljoonaa dollaria. C-sviitin tärkein prioriteetti ei useinkaan ole kyberturvallisuus, luvuista huolimatta. Miten sairaaloiden ja muiden terveydenhuollon organisaatioiden CISO:t voivat osoittaa vahvan kyberturvallisuuden arvon, kun taas monet muut asiat vievät johdon huomion? Lääkärit ja muut ammattilaiset, jotka näkevät potilaita jokapäiväisissä askareissa, eivät välttämättä ajattele kyberturvallisuutta potilasturvallisuuden kannalta. Tämä saa salasanavaatimukset, turvallisuuskoulutus- ja muut vaatimukset näyttämään vähäksytyltä potilaiden hoitoon ja turvallisuuteen liittyen, vaikka ovat itseasiassa olennainen osa sitä.

Samassa artikkelissa Wright:n (i.a) mukaan Phillion (2021, s. 5) toteaa, että tapa korjata tämä on varmistaa, että kyberturvallisuuden noudattaminen ja kliininen tehokkuus paranevat yhdessä. Ilman jälkimmäistä, henkilökunta palaa entiseen malliin. Terveydenhuollon IT ammattilaiset syyllistyvät yritykseen saada ihmiset hyppäämään melko raskaiden vanteiden läpi kyberturvallisuuden nimissä. Avain on tehdä oikea asia ja oikea asia tässä on varmistaa, että asiat ovat kybersuojattuja. Kyberturvallisuuden parantaminen terveydenhuollossa edellyttää tietenkin enemmän koulutusta, mutta kyse on myös siitä, että aiheelle annetaan oikea painoarvo (mts. 6). Lääkäreiden täytyy tietää, että

kyberturvallisuus on yhtä suuri potilasturvallisuusongelma kuin maskin käyttö tai neulanpistojen estäminen.

Phillion (2021, s. 7) kirjoittaa artikkelissaan, että jos joku murtautuu organisaation sähköisiin potilastietoihin, mitä he voivat tehdä tiedoilla? On pahimpia skenaarioita, kuten allergiatietojen tai muiden synkkien mahdollisuuksien poistaminen ja taloudellinen veruke, kuten väestötietojen myyminen pimeillä markkinoilla. Kiristysohjelmahyökkäysten kaltaisista tapauksista on kuitenkin tullut niin yleisiä, että pelko arvovallan menettämisestä hyökkäyksen jälkeen (kerran vahva terveydenhuollon kyberturvallisuuden motivaattori) on vähentynyt. Loppujen lopuksi, tarkoituksena on saada kaikki samalle sivulle: Kyberturvallisuutta ei voi erottaa potilasturvallisuudesta, vaan se on olennainen osa sitä. Wright i.a mukaan Phillion (2021, s. 7,) toteaa, että kyberturvallisuuteen ei keskitytä, koska ajatellaan sen olevan ”siisti” asia. Sitä tehdään, koska se on yhtä suuri potilasturvallisuuskysymys kuin mikä tahansa muukin.

2.3 Haittatapahtumat, ennaltaehkäisy ja ilmoittaminen

Sosiaali- ja terveysministeriön (STM) potilas- ja asiakasturvallisuusstrategian (2017) linjauksen mukaan potilasturvallisuutta ja laatua parannetaan riskienhallinnan avulla haittatapahtumien ennakoimiseksi. Turvallisuusongelmien ennakoinnilla pyritään estämään vahinkoja, vaaratilanteita ja toiminnan kannalta kielteisiä tapahtumia. Säännöllisesti tehtävät riskikartoitukset ja vaaratapahtumien raportointi ovat käytännön keinoja riskien tunnistamiseen. Turvallisuusriskejä esiintyy erityisesti tiedonhallinnassa ja muutosprosessien yhteydessä, kuten organisaatiouudistuksissa sekä uuden teknologian, digitalisaation, menettelytapojen ja uusien hoitokäytäntöjen käyttöönotossa. Digitalisaation avulla voidaan myös parantaa tiedonkulkua ja turvallisuutta. Kuitenkin digitalisaation kehittyessä uudet tietojärjestelmät voivat käyttää pilvipalveluja, jolloin tieto saattaa olla tallennettuna pilvessä Yhdysvalloissa tai EU:n ulkopuolella, joissa tietosuojalainsäädäntö poikkeaa eurooppalaisista säädöksistä (Tolonen & Vepsäläinen, 2020, s. 2012). Uusia laitteita hankittaessa hankintaprosessin ennakkotyön osuus onkin tärkeä vaihe, jota ei saa laiminlyödä. Hankittavasta laitteesta ja sen toimintaperiaatteista olisi välttämätöntä muodostaa kokonaiskuva hankintatiimissä, jonka voi muodostaa lääkäri, organisaation tietoturva-asiantuntijat ja hankintayksikkö.

Ossolan (2015) mukaan Middaugh (2016, s.131) toteaa artikkelissaan Medsurg nursing-lehdessä, että usein tietojärjestelmät ovat langattomassa yhteydessä nettiin samoin kuin tulostimet, kopiokoneet, puhelimet ja lääkinnälliset laitteet, jotka kommunikoivat serverien eli palvelimien kanssa. Laitteiden etähallinta on mahdollista, jolloin hakkerit voivat murtautua potilastietoihin muuttaen lääkekirjauksia ja hoitosuunnitelmaa tai varastaen potilastietoja. Potilastietojen sisältämien henkilötietojen (kuten osoite, syntymäaika, sosiaaliturvatunnus, perhesuhteet sekä lääkityshistoria) avulla voidaan luoda vääriä identiteettejä ja luottolinjauksia (mts. 132).

Medsurg nursing-lehden artikkelissaan (2016, s. 131) Middaugh toteaa, että selvitystyön tuloksena eräissä insuliinipumpuissa todettiin olevan viallisen koodin, joka mahdollisti hakkereiden pääsyn hallitsemaan laitetta, jolloin hakkerit saattoivat ohjelmoida laitteen luovuttamaan kuolettavan annoksen insuliinia. Samoin mm. röntgenlaitteet, magneettikuvauslaitteet, sydämen tahdistimet ja sisäkorvaistutteet insuliinipumppujen lisäksi ovat alttiita hakkeroinnille muodostaen riskin potilasturvallisuudelle (mt.).

Commins`n (2015) mukaan hoitaja voi tehdä virheen kytkemällä luvattoman laitteen, esimerkiksi matkapuhelimen, lääkintälaitteen USB-porttiin, joka lääkinnällisessä laitteessa on tarkoitettu informaation jakamiseen (Middaugh, 2016, s. 132). Älypuhelimen lataaminen USB-portissa voi aiheuttaa toimintahäiriön: monitorin uudelleen käynnistymisen, potilaan monitoroimisen lopettamisen tai epäonnistuneen hälytyksen.

Organisaatioissa tulisi olla henkilöstölle järjestettävästä koulutuksesta koulutussuunnitelma, jonka mukaisesti henkilöstön perehdytys asiakas- ja potilastietojen tietosuojaan ja tietoturvaan toteutetaan (Konttinen & Mykkänen, 2016, s.137). Myös tietojärjestelmien käyttöön tarvittava ohjaus ja perehdytys tulee sisältyä suunnitelmaan, jotta järjestelmien käyttö olisi tarkoituksenmukaista. Työntekijöiden omalla vastuulla on joko osallistua koulutuksiin tai hankkia vastaava tieto muulla tavoin (mts.138). Selkeät käyttöohjeet organisaatiossa olevasta järjestelmästä tulisi olla henkilöstön saatavilla. Samoin pitäisi toimia nettiyhteydessä olevien laitteiden kohdalla. Jokaisen käyttäjän tulisi saada koulutusta käyttämiinsä laitteisiin (mt.). Uudessa, helmikuussa 2022 voimaan tulleessa STM:n ”Asiakas- ja potilasturvallisuusstrategia ja toimeenpanosuunnitelma 2022–2026” -julkaisussa kiinnitetään huomiota

henkilöstön ammatilliseen osaamiseen, jota vahvistetaan osaamisen ylläpidolla koko työuran ajan (STM, 2022, s. 27).

Sosiaali- ja terveydenhuollon ammattilaiset, asiakkaat ja viranomaiset tuottavat useita tarvittavia tietolähteitä ja tietotyyppejä, joita asiakas- ja hoitotyössä hyödynnetään (Kurki ym. 2021, s. 118). Ongelmia voi tuoda kuitenkin tietojärjestelmien keskinäinen sopivuus sekä monialainen, sosiaali- ja terveydenhuollon rajat ylittävä yhteistyö. Tiedon tallentaminen muotoon, josta ammattilainen vaivattomasti saa kuvauksen senhetkisestä tilanteesta, on hyödyllistä, koska tietoa on runsaasti saatavilla ja lähteitä useita (mts. 118). Tarvittaessa olennainen tieto tulisi olla tunnistettavissa ongelmitta. Kurjen ym. (2021, s. 118–119) mukaan Kanta-palvelut on hyvänä esimerkkinä palvelukokonaisuudesta, joka on sosiaali- ja terveydenhuollon palveluntuottajien lisäksi apteekkien ja kansalaisten käytössä.

Riskienhallinnassa tulisi laajemmin huomioida tiedonhallintaa ja tietosuojaa koskevat riskit sekä arvioida riskien yhteisvaikutuksia potilas- ja asiakasturvallisuuteen (STM, 2017). Ennakoivan riskienhallinnan tavoitteena on varautua tunnistettuihin riskeihin, välttää haittatapahtumia ja lisätä potilasturvallisuutta. Potilas- ja asiakasturvallisuuden kehittymisen edellytyksenä on kaikkien vaaratapahtumien raportointi ja niiden analysointi, jonka tulisi olla laissa säädetty velvollisuus (hallintaan ei ole vahvaa lain velvoitetta kuten työturvallisuuslaissa työn vaarojen selvittäminen ja arviointi).

Sosiaali- ja terveydenhuollossa tietoja käsittelevien on noudatettava toimintamallia, jossa asiakkaan tai potilaan tiedot säilyvät luottamuksellisina ja muuttumattomina (Konttinen & Mykkänen, 2016, s.137). Omavalvontasuunnitelman mukaisen toimintamallin noudattamista valvoo organisaatiossa olevat asiantuntijat. Asiantuntijoiden tehtävänä on myös kouluttaa ja ohjata ammattilaisia toimintamallien hyödyntämiseen omassa työssään.

Havaittaessa verkko- tai tietoliikenneongelmia, tietoturva- ja tietosuojauhkia tai järjestelmien käyttöön liittyviä ongelmia on oltava toimintaohjeet (Konttinen & Mykkänen, 2016, s.139). Kaikilla järjestelmää käyttävillä tulisi olla tiedossa, minne otetaan yhteyttä ja miten ongelmatilanteessa toimitaan. Konttisen & Mykkäsen (2016) mukaan on huomattava, että jokaisella virheen tai ongelman huomanneella on vastuu ilmoittaa havainnostaan ja mikäli epäillään ongelmia tai häiriöitä Kanta-palveluissa, tulee organisaatioiden huomioida kansalliset

ohjeet. Potilasturvallisuusriskin ollessa merkittävä on organisaation tehtävä ilmoitus järjestelmävalvojalle ja Valviralle.

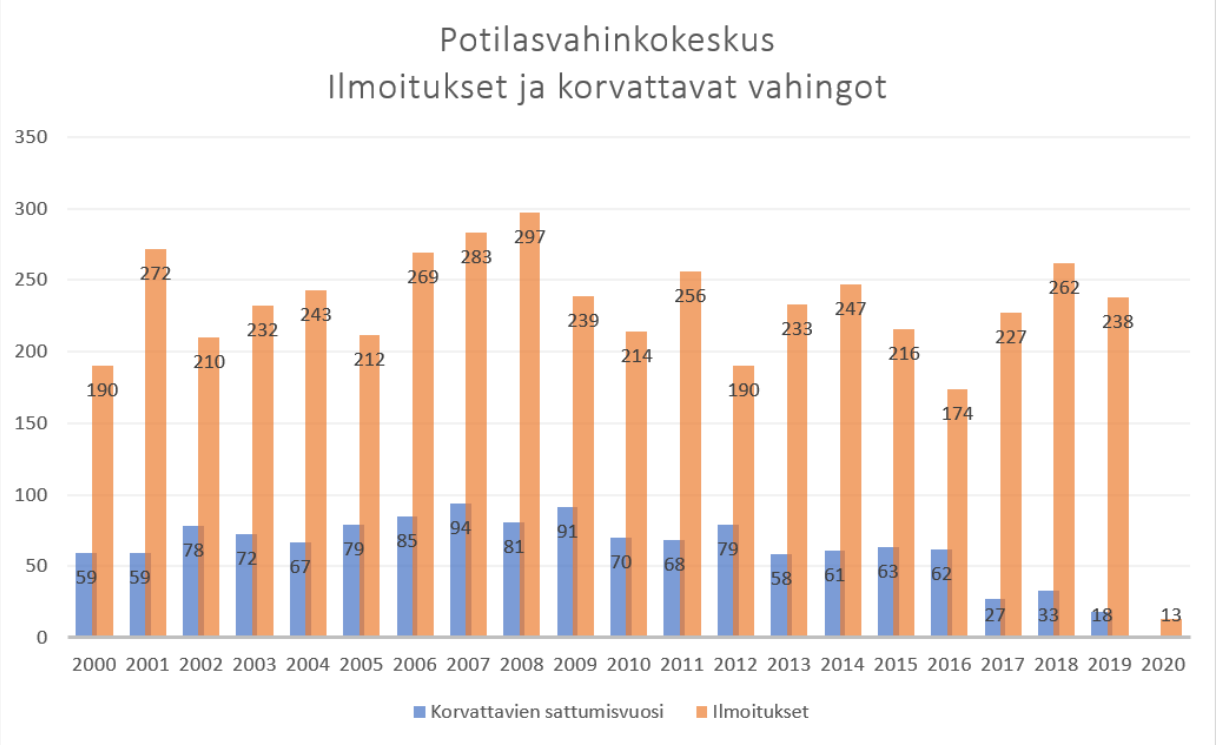
Vaaratilanteiden, haittatapahtumien ja poikkeamien sattuessa niistä raportoidaan ja vahingoista kertynyttä tietoa hyödynnetään toiminnan kehittämisessä ja virheistä oppimisessa (THL, 2011, s. 28). Organisaatiossa henkilöstön tulee raportoida haittatapahtumista sekä läheltä piti -tilanteista käytössä olevan raportointimenettelyn, esimerkiksi HaiPron kautta. Tieto ilmoitetuista vaaratapahtumista tiedotetaan työyhteisössä säännöllisesti, tapahtumia tarkastellaan ja kehittämistoimia pohditaan yhdessä moniammatillisesti (mts. 29). Valtakunnallisella tasolla haittatapahtumien, kuten komplikaatiodiagnoosit ja lääkehaittavaikutukset, ilmoittaminen tehdään sairaaloiden hoitoilmoitusjärjestelmä HILMOon (mts. 30). Ilmoittaminen on lakisääteistä.

Haipro on vaaratapahtumien raportointijärjestelmä (Kinnunen ym., 2013 s. 260). Sana Haipro on lyhennetty sanoista haittatapahtumien raportointiprosessin kehittäminen terveydenhuollon organisaatioissa. Lääkelaitoksella ja Valtion teknillisellä tutkimuskeskuksella oli yhteistyö 2000-luvulla, josta alkoi järjestelmän kehitystyö. Lääkityksen virheiden yleisyydestä (taulukko 2) heräsi tarve hallita näitä ja muita hoidon haittoja tietotekniikkaa hyödyntäen ja systemaattisesti. Järjestelmän ensimmäisessä kehitystyön vaiheessa oli mukana vain kolme terveydenhuollon organisaatiota. Toisessa vaiheessa tuli mukaan 30 terveydenhuollon toimijaa vuosina 2006–2007. Tällöin sosiaali- ja terveysministeriö tuli mukaan kehitystyön kumppaniksi ja rahoittajaksi. Sen jälkeen haittatapatumista alettiin puhua vaaratapahtumina, jotka käsittävät sekä haittatapahtumat, että läheltä piti -tilanteet (mt.).

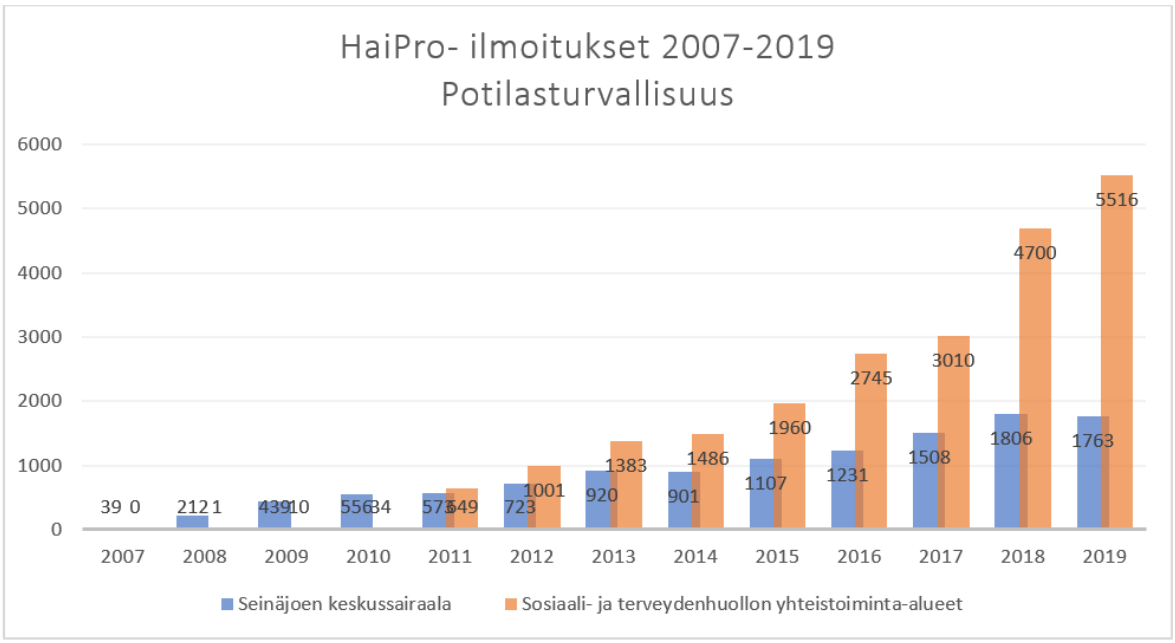
Vaaratapahtumien raportointi etenee vaiheittain siten, että ensimmäisessä vaiheessa tunnistetaan vaaratilanne, toisessa vaiheessa tehdään ilmoitus, kolmannessa vaiheessa tapahtuu ilmoituksen vastaanotto, luokittelu ja analysointi, neljäs vaihe on jatkotoimista päättäminen ja viides vaihe on seuranta ja arviointi (Kinnunen ym., 2013, s. 260). Raportoinnin ensimmäisessä vaiheessa vaaratilanne tunnistetaan. Raportointijärjestelmässä tapahtumatyyppi luokitellaan, mikä helpottaa ilmoitettavien tapahtumien tunnistamista. Raportoinnin toisessa vaiheessa tehdään ilmoitus sähköiselle lomakkeelle, jonka ilmoittaja täyttää (mts. 261). Raportoinnin kolmas vaihe on ilmoituksen vastaanottaminen, luokitteleminen ja analysoiminen. Luokituksen ja analysoinnin tekee käsittelijä, ja hän huomioi käsittelijän

lomakkeelle ilmoitetun tapahtuman syntyyn vaikuttavat tekijät. Ilmoituksen käsittelijät toimivat usein työparina, kuten esimerkiksi yksikön vastuulääkäri ja osastonhoitaja. Raportoinnin kaksi viimeistä vaihetta ovat jatkotoimista päättäminen, seuranta ja arviointi, eli tapahtumista saatua tietoa hyödynnetään ja seurataan muutoksia. Koko työyhteisön tulisi saada tietoa järjestelmään kootuista tiedoista, mikä on tärkeää tiedon hyödyntämistä. Avoin keskustelumahdollisuus vaaratapahtumista antaa hyvän perustan muutoksille (mt.). Kuviossa 1 on kuvattu potilaskeskukseen tulleet ilmoitukset ja korvattavat vahingot.

1. Taulukko Potilasvahinkokeskus ilmoitukset ja korvattavat vahingot. (mukaellen EPSHP. 2020)



2. Taulukko HaiPro ilmoitukset 2007–2019, Potilasturvallisuus (mukaellen EPSHP, 2020)



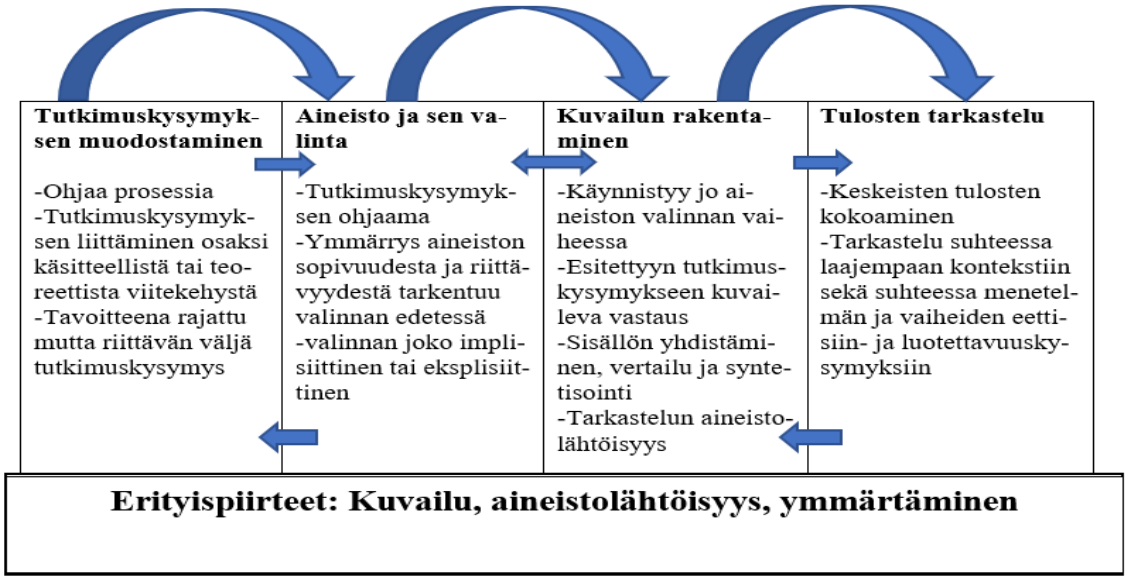
31.12.2019

3 OPINNÄYTETYÖN TAVOITE, TARKOITUS JA TEHTÄVÄ

Opinnäytetyön tavoitteena on tuottaa näyttöön perustuvaa tietoa hoitotyöntekijöille tietoturvaan liittyvistä tekijöistä, haittatapahtumien ennaltaehkäisystä ja tietoturvan edistämisestä hoitotyössä. Opinnäytetyön tarkoituksena on perehtyä tutkittuun tietoon ja tuottaa kuvaileva kirjallisuuskatsaus tietoturvasta osana potilasturvallisuutta hoitotyössä. Opinnäytetyön tehtävänä on etsiä vastauksia seuraaviin kysymyksiin: Mistä asioista tietoturva hoitotyössä muodostuu? Millaiset tekijät vaarantavat hoitotyössä tietoturvaa? Miten voidaan ennaltaehkäistä haittatapahtumia?

4 OPINNÄYTETYÖN TOTEUTUS

Opinnäytetyö toteutetaan kuvailevana kirjallisuuskatsauksena, jonka perustana on tutkimuskysymys. Valittuun aineistoon perustuen tuotetaan kuvaileva ja laadullinen vastaus. Kangasniemen ym. (2013, s.291) mukaan kuvaileva kirjallisuuskatsaus on aineistolähtöistä ja kuvailemalla ilmiötä pyritään sen ymmärtämiseen. Kuvailevan kirjallisuuskatsauksen vaiheet ovat tutkimuskysymyksen muodostaminen, aineiston valitseminen, kuvailun rakentaminen ja tuotetun tuloksen tarkasteleminen. Muihin kirjallisuuskatsauksiin verrattuna kuvailevan kirjallisuuskatsauksen erityispiirteenä on koko prosessinaikainen vaiheiden osittainen päällekkäin eteneminen tutkimuskysymyksestä tuotetun kuvailun tarkasteluun (Kangasniemi ym. 2013, s. 292).



Kuvio 2. Kuvailevan kirjallisuuskatsauksen vaiheet ja erityispiirteet (mukaellen Kangasniemi, 2013, s.294).

4.1 Tutkimuskysymyksen muodostaminen

Tutkimuskysymys on keskeinen kuvailevassa kirjallisuuskatsauksessa, ja se ohjaa koko tutkimusprosessia (Kangasniemi ym. 2013, s. 294). Tutkimuskysymys voidaan määritellä alustavan kirjallisuuskatsauksen avulla, jolloin se liitetään laajemman käsitteellisen tai teoreettisen kehyksen osaksi. Tutkimuskysymys voi olla kysymyksen muodossa ja kysymyksen tarkastelu voi tapahtua yhdestä tai useammasta näkökulmasta. Riittävän täsmällinen ja rajattu kysymys mahdollistaa syvällisen tarkastelun, kun taas väljän tutkimuskysymyksen ilmiötä voidaan tarkastella eri näkökulmista (mts. 295).

Kangasniemen ym. (2013, s. 295) mukaan menetelmä soveltuu myös kliinisessä kysymyksenasettelussa käytettäväksi arvioitaessa nykyisiä käytäntöjä, kehitettäessä ja päivitettäessä käytännön suosituksia sekä kehitettäessä työhön liittyviä menettelytapoja. Kuvailevan kirjallisuuskatsauksen avulla voidaan hajanaisista tai pirstaleisista aiheista tuottaa tietoa hyvien käytäntöjen edistämiseksi kliinisessä työssä ja koulutuksessa (mt.).

4.2 Tiedonhaku

Tietokantahakuja varten tarvitaan oikeat hakusanat. Opinnäytetyön asiasanoja ovat mm. tietoturva, tietoturvallisuus, tietosuoja, potilasturvallisuus, hoitotyö, haittatapahtumat, joilla haetaan MOT:stä ja YSO:sta aiheeseen liittyviä sanoja. Näin sanastoa saadaan laajennettua, ja sanoja käytetään hakusanoina tutkimusartikkeleiden ja lähdekirjallisuuden löytämiseksi. Aiheen keskeisiä hakusanoja ovat potilasturvallisuus, asiakasturvallisuus, tietoturvallisuus, tietoturva, tietosuoja, terveydenhuolto, hoitotyö, kohtaaminen, potilas, hoitoympäristö, salassapito, vaitiolovelvollisuus, dokumentointi, kirjaaminen, kyberturvallisuus, haittatapahtumat sekä patient security ja patient care, patient safety, information security, data security, cyber security, lainsäädäntö sosiaali- ja terveysalalla sekä EU:n yleinen tietosuoja-asetus.

Uusi käsite, asiakasturvallisuus, löytyi "potilasturvallisuus" -hakusanalla. Kurjen ym. (2021, s. 7) mukaan asiakasturvallisuus käsitteenä ja teemana on potilasturvallisuuden lähikäsite. Alkuvuonna 2019 julkisuuteen nousi keskustelua ikääntyneiden asumisyksiköissä tarjottavan palvelun laadusta hoivassa ja huolenpidossa. Uutiskynnyksen ylityksen jälkeen ilmaantui julkisuuteen lukuisia tapauksia hoivan puutteellisuudesta, jopa kaltoinkohtelusta. Tätä

Kurki ym. (2021, s. 7) pitävät termin ”asiakasturvallisuus“ ulostulona laajempaan tietoisuuteen, vaikkakin jo aiemmin, vuonna 2017 päivitetyssä kansallisessa potilas- ja asiakasturvallisuusstrategiassa asiakasturvallisuus ilmiönä mainittiin potilasturvallisuuden rinnalla (mts. 8). Yhtenä lähteenä opinnäytetyössä käytetään Kurjen ym. (2021, s.117–120 aineistoa.

Tiedonhaku suoritettiin uusinta tietoa hakien (vuosilta 2012–2022) aihetta käsittelevästä kirjallisuudesta. Tiedonhaussa hyödynnettiin kirjastoa ja eri tietokantoja kuten Cinahl, Medic, Terveysportti, Finna sekä ajankohtaisia verkkolähteitä, artikkeleita (esim. Hoitotiede-lehdestä) ja muita ajankohtaisia julkaisuja. Myös kaikille tarkoitetusta Duodecimin Terveyskirjastosta ja asiantuntijoiden kirjoituksista löydettiin tietoa opinnäytetyöhön. Tiedonhaussa tavoiteltiin uusinta näyttöön perustuvaa tietoa, huomioiden lähdekritiikin ja tutkimuksen eettisyyden. Opinnäytetyössä käytettiin myös englanninkielistä, Cinahl-haulla saatua tutkimusmateriaalia.

Englanninkielisiä tutkimuksia löytyi useita, mutta niistä viittä on hyödynnetty opinnäytetyössä. Lisäksi englanninkielisiä, hyviä artikkeleita löytyi ja niistä kahta on käytetty lähteenä. Myös kahta englanninkielistä verkkolähdettä käytettiin käsitteiden selvittelyyn. Kotimaisia artikkeleita löytyi SeAMK Finnasta, Medicistä, Artosta ja Elektrasta. Kotimaisia lähteitä löytyi hyvin ja niistä neljää artikkelia käytettiin opinnäytetyön teoriaosuutta varten. Kuitenkin kotimaisia tutkimusartikkeleja löytyi vähemmän, joista pystyimme hyödyntämään yhtä, koska muiden sisältö ei vastannut tutkimuskysymyksiin.

4.3 Aineiston valitseminen ja arviointi

Kuvailevassa kirjallisuuskatsauksessa aineistona käytettiin aiemmin julkaistua, tutkimusaiheen kannalta merkityksellistä tutkimustietoa, jonka riittävyyden määrittää tutkimuskysymyksen laajuus (Niela-Vilén & Hamari, 2016, s. 25). Tarkoitus oli löytää ja tunnistaa kaikki tutkimuskysymykseen vastaava materiaali, ensisijaisesti alkuperäistutkimukset. Sähköisissä tietokannoissa tehtävät haut ovat kustannustehokkaita, mutta eivät välttämättä tavoita kaikkia katsaukseen soveltuvia tutkimuksia, joten käytimme lisäksi myös manuaalista tiedonhakua (mt.).

Aineistoa valittaessa huomioitiin, että kuvaileva kirjallisuuskatsaus on menetelmänä luonteeltaan aineistolähtöinen ja ymmärtämiseen pyrkivä (Kangasniemi ym. 2013, s. 295). Alkuperäistutkimuksien rooliin tutkimuskysymykseen vastaamisessa kiinnitettiin huomiota, esimerkiksi täsmentävätkö ja miten, jäsentävätkö, kritisoivatko vai avaavatko tutkimuskysymystä. Kuvailevassa kirjallisuuskatsauksessa käytettäväksi sopivat muutkin kuin tieteelliset artikkelit (esim. konferenssijulkaisut tai pääkirjoitukset), mikäli se on perusteltua katsauksen kysymyksenasettelun kannalta (mts. 296).

Niela-Vilénin ja Hamarin (2016) mukaan hakuprosessin perusteella valittujen tutkimusten kriittinen arviointi on kirjoittajan vastuulla. Tarkoitus on tarkastella alkuperäistutkimuksista saadun tiedon kattavuutta ja tulosten luotettavuutta. On myös syytä miettiä vastaako tutkimuksista saatu tieto omaan tutkimuskysymykseen? Aineistoa tulee arvioida alkuperäistutkimuksen julkaisuvuoden, artikkelin kirjoittajan, julkaisumaan ja julkaisufoorumin perusteella (mts. 29).

4.4 Kuvailun rakentaminen

Aineiston analyysin ja synteesin tarkoituksena on järjestää ja tehdä yhteenveto tutkimusten tuloksista (Niela-Vilén & Hamari, 2016, s.30). Tutkimusten arviointi ja analyysivaihe ovat sidoksissa toisiinsa ja niitä tehdään toisinaan yhtä aikaa. Etenkin tilanteessa, jossa valittujen tutkimusten tulokset ovat ristiriitaisia, niin laadunarviointi on otettava huomioon myös katsauksen tulosten analysoinnissa. Tutkimusten yhteenveto on suositeltua tehdä taulukkomuotoon kokonaiskuvan saamisen tueksi (mts. 31).

Kuvailun rakentamisen käsittelyosassa on Kangasniemen ym. (2013, s. 296) mukaan menetelmän ydin, jossa vastaaminen tutkimuskysymykseen on tavoitteena. Sisältöä eri tutkimuksista yhdistellään, analysoidaan kriittisesti ja syntetisoidaan, mikä voi johtaa uuden tulkinnan syntymiseen, mikä ei tarkoita alkuperäisen tiedon muuttamista. Kuvailevassa kirjallisuuskatsauksessa ilmiötä kuvastavat seikat ryhmitellään sisällöllisiksi kokonaisuuksiksi, joita voidaan tarkastella teemoittain, kategorioittain tai suhteessa kategorioihin, käsitteisiin tai teoreettiseen lähtökohtaan. Menetelmä edellyttää käyttäjältä syvällistä valitun aineiston tuntemista ja kokonaisuuden hallintaa (mts. 297).

5 OPINNÄYTETYÖN TULOKSET

Viimeinen vaihe kuvailevassa kirjallisuuskatsauksessa on tulosten tarkasteleminen. Siinä pohditaan sekä sisältöä että menetelmää ja arvioidaan tutkimuksen eettisyyttä ja luotettavuutta (Kangasniemi ym. 2013, s. 297). Myös tutkimuksen tuottamat tulokset tiivistetään ja tarkastellaan niitä. Esitettyä tutkimuskysymystä voidaan kritisoida, käsitteiden abstraktiotasoa nostaa, tulevaisuuden haasteita ja kysymyksiä hahmotella sekä esittää jatkotutkimushaasteet ja johtopäätökset.

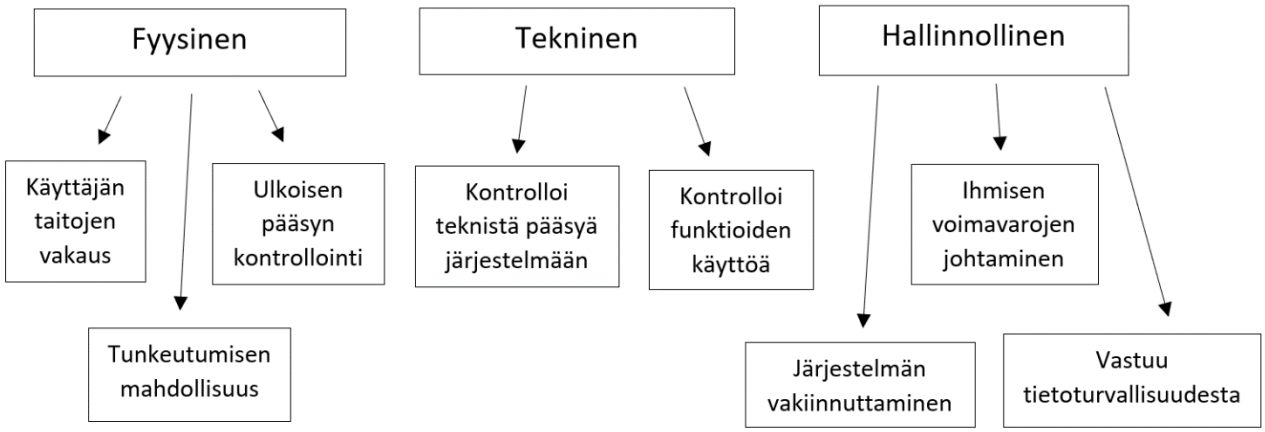
5.1 Tietoturvan muodostuminen hoitotyössä

Kyytsönen ym. (2020, s. 250) toteavat sairaanhoitajien työssä keskeisiä työvälineitä olevan asiakas- ja potilastietojärjestelmät. Heidän Finnish Journal of eHealth and eWelfare:n julkaisema tutkimus osoittaa, että sairaanhoitajat olivat tyytyväisiä etenkin tietojärjestelmien kykyyn tukea yhteistyötä ja tiedonkulkua sairaanhoitajien kesken organisaation sisällä sekä sairaanhoitajien ja lääkärien välillä. Vastaajat tunnistivat järjestelmissä kuitenkin enemmän työtä hankaloittavia kuin toimivia ominaisuuksia. Tietojärjestelmien kehityssuunta vaikutti positiiviselta. Nähtiin kuitenkin kehitettäviä asioita ja systemaattista seurantaa on syytä jatkaa. Potilastietojärjestelmien käyttö voi johtaa turvallisuushaasteisiin, sillä järjestelmän käytön osaamattomuus ja tietoturvaan liittyvä tietämättömyys on yhteydessä potilasturvallisuuteen (mts. 250–251).

Kang (2020, s. 28) kirjoittaa, että hoitotyössä tietoturvallisuuden pitäisi perustua koko organisaation ponnisteluun paremman turvallisuuskulttuurin kypsymiseksi. Myös Suomalainen lääkäriseura Duodecim toteaa, että jokaisen on toiminnallaan pyrittävä minimoimaan tiedon joutuminen vääriin käsiin. Tietoturva muodostuu paperisten ja sähköisten henkilötietojen käsittelystä, asiakirjojen laatimisesta ja käytöstä. Dokumentointi, raportointi, tietojen säilytys, luovutus ja hävitys kuuluvat tietoturvaan. Tietoturva muodostuu myös asiakkaan luotettavasta tunnistamisesta. Hoitotyössä on vaatimus tunnistaa ja varmistaa kenen tietoja käsitellään. Tunnistaminen koskee kaikkia osapuolia: hoidossa oleva potilas, potilaan vointia kysyvä omainen, muu henkilökunta sekä viranomaiset.

Tietoturva sisältää aineiston ja laitteen suojaamisen luvattomalta pääsyltä, käytöltä ja tiedon siirrolta, tietokatkoilta, tiedon muunnoksilta ja hävittämiseltä (Kang 2020, s. 20). Tiedon luottamuksellisuuden, koskemattomuuden ja käytettävyyden ylläpitämiseksi tarvitaan tietoturvatoimia. Ongelmat yksityisyyden suojaamisessa hoitotyössä ovat kasvaneet tietokoneiden käytön laajentuessa, ja potilastietojen käyttö vääriin tarkoituksiin lisääntynyt. Lääketieteellisiä palveluja tarjoavat instituutiot ovat vastuussa potilastietojen suojauksesta ja turvaamisesta. Turvatoimia ylläpitämällä varmistetaan, ettei tietoa jaeta ilman potilaan lupaa (mt.).

Kang (2020, s. 25) tutkii tietoturvaa hoitotyössä kolmesta näkökulmasta, fyysisestä, teknisestä ja hallinnollisesta aspektista, pyrkimyksenä helpottaa hoitajia tunnistamaan tietoturvan merkitys käytännön työssä (kuvio 3). Fyysinen näkökulma tarkastelee käyttäjän taitojen vakautta sekä kontrolloi ulkoisen pääsyn tai tunkeutumisen mahdollisuutta. Tekninen näkökulma kontrolloi teknistä pääsyä järjestelmään ja funktioiden (tehtävien) käyttöä. Hallinnolliseen näkökulmaan kuuluu järjestelmän vakiinnuttaminen, ihmisen voimavarojen johtaminen sekä vastuu tietoturvallisuudesta. Sairaanhoitajan eettinen velvollisuus on potilaan yksityisyyden säilyttäminen, minkä tietosuoja -säännösten toteuttaminen mahdollistaa (Kang, 2020, s. 21).



Kuvio 3. Tietoturva hoitotyössä kolmesta näkökulmasta. (Kang 2020, s. 25)

Kang (2020, s. 20) tutkimustuloksissaan toteaa, että asiakas- ja potilastietoja käsittelevien tietoisuus lääketieteellisten tietojen tärkeydestä ja koulutuksen sekä harjoittelun tarpeesta on alkanut organisaatioiden hallinnossa korostua. Harjoittelun tarve, etenkin johtavaa henkilöstöä koskien, on oivallettu. Pysyvyys, vakaus ja ammatillinen vastuullisuus (kuvio 4) ovat piirteitä, joilla hallinnoivan tahon tietoturvanäkökulmaa kuvailtiin (mts. 24). Pysyvyydellä tarkoitetaan jatkuvan koulutuksen tärkeyttä ja tietoturvan hallintaa sekä tietoisuutta tietoturvasta. Hoitajien täytyy laajentaa tietoisuuttaan tarpeellisilla pätevöitymiskoulutuksilla, jotta he voisivat soveltaa turvallisuustoimenpiteitä. Vakaus lääketieteellistä informaatiota käsiteltäessä auttaa hoitajia tunnistamaan yksityisyyden loukkauksen, tiedostamaan tietoturvan ylläpitämisen tarpeellisuuden sekä lääketieteellisen tiedon oikean käsittelyn merkityksen. Kang (mts. 25) on havainnut, että ammatillisen vastuullisuuden noudattaminen sairaanhoitajan työssä heijastuu työtyytyväisyytenä ja potilaiden emotionaalisena vakautena.

Pysyvyys	• Jatkuvan koulutuksen tärkeys • Tietoturvan hallinta • Tietoisuus tietoturvasta	Vakaus	• Yksityisyyden loukkauksen tunnistaminen • Tietoturvan ylläpitämisen tarpeellisuuden tiedostaminen • Lääketieteellisen tiedon oikean käsittelyn merkityksen tiedostaminen	Ammatillinen vastuullisuus	• Työtyytyväisyys • Potilaiden emotionaalinen vakaus

Kuvio 4. Hallinnoivan tahon tietoturvanäkökulman kuvaileminen (Kang 2020, s.20)

Morris ym. (2021, s. 42) toteutti tutkimuksen, jossa potilaita, huoltajia/omaishoitajia ja hoitohenkilökuntaa pyydettiin osallistumaan yhteistyöhön potilasturvallisuus -oppaan kehittämiseksi perusterveydenhuoltoon. Tutkimustuloksena todettiin kommunikaation tärkeys, roolien ja vastuiden ymmärtäminen sekä kumppanuuden kehittyminen potilaiden ja terveydenhuollon henkilökunnan välille, jotta potilaat aktiivisesti osallistuisivat potilasturvallisuus asiaan (mt.).

5.2 Tietoturvaa vaarantavat tekijät hoitotyössä

Suomalainen lääkäriseura Duodecim (Oppiportti i.a.) on koonnut tietoa vaitiolovelvollisuudesta ja siihen vaikuttavista tekijöistä. Tietoturva potilashuoneissa voi vaarantua, esimerkiksi päivystyksen vuodepaikoilla voi olla hankalaa säilyttää potilastietojen luottamuksellisuus. Keskustelu potilastiedoista on sallittua ainoastaan hoitoon osallistuvien ammattihenkilöiden kesken tai tietojen käsittelyn liittyessä työtehtäviin. Potilastietoja ei ole sopivaa käsitellä yleisissä tiloissa, kuten sairaalan julkiset tilat. Paperimuodossa olevat tiedot on huomioitava käsitellä myös tietoturvaa vaarantamatta. Papereita ei tule unohtaa tulostimeen tai paikkaan, josta ohikulkijat voivat nähdä ne. Asiakkaan suostumus tarvitaan tietojen luovuttamiseen eri yksiköille, erimerkiksi muille hoitoa antaville hoitotahoille. Myös vapaa-ajalla ja työsuhteen päätyttyä vaitiolovelvollisuus on edelleen voimassa. Tietosuojaloukkaukset voivat johtaa rikosoikeudellisiin seuraamuksiin. Suomalainen lääkäriseura Duodecim kirjoittaa

myös asiakkaan luotettavasta tunnistamisesta ja automaatti-ilmoittautumisen haasteista. Esimerkiksi, kun Kela-kortissa ei ole kuvaa, kuinka voidaan varmistua kortin haltijan ja kortin tietojen yhteenkuuluvuudesta?

Suojaamattomat tietojärjestelmät, ohjelmistot, laitteet, palvelut, tietoaineistot, tietoliikenne ja huonosti suunnitellut tilat ovat tietoturvaa vaarantavia tekijöitä. Medsurg nursing -lehdessä Middaugh (2016, s. 132) kirjoittaa, että monissa lääkinnällisissä laitteissa (tietokonetomografia skanneri, magneettikuvauslaitteet, kardiopulmonaarinen ohitusleikkaus kone/sydänkeuhkokone/CPB-pumppu, ECMO- pumppu, hengityskoneet ja dialyysi-laitteet) on osoittautunut olevan käytössä päivittämätön, suljettu tai muunneltu turvajärjestelmä, joka mahdollistaa ”hyökkääjälle” avoimen pääsyn järjestelmässä oleviin muihin laitteisiin ohittaen turvajärjestelmät samalla saastuttaen myös lääkinnällisen laitteen. Niccolai (2015 mukaan) Middaugh (2016, s. 132) toteaa, että potilasturvallisuuden vaarantamiseen ei aina tarvita pahansuopaa hakkeria, vaan potilaat voivat itsekin oppia murtautumaan omaan lääkintälaitteeseen nostaakseen kipulääkeinfuusion annostusta.

Helovuo ym. (2011, s. 76) toteaa, että kyky käsitellä tietoa ja toimia sen perusteella perustuvat inhimilliseen toimintaan. Ihminen havaitsee ja tarkkailee asioita, ja aikaisempien opittujen sekä koettujen asioiden perusteella hän tekee ratkaisuja (s.77). Inhimillisistä tekijöistä puhuttaessa viitataan tiedonprosessin rajoituksiin. Tarkkaavaisuus, muisti, erehdykset, unohdukset ja muut inhimilliset virheet ovat rajallisuuden ja rajoituksien seurausta. Ihmisinä, emme pysty käsittelemään suuria määriä asioita yhtä aikaa. Aistiemme havaitsemat asiat kuormittavat tiedonkäsittelyä ja vievät osan huomioistamme pois varsinaisesta tehtävästä. Institute of Medicine on suosittanut Yhdysvalloissa, että luottamusta muistiin ja valppauteen tulisi välttää. Tämä perustuu siihen, että kiireessä, rauhattomassa ympäristössä ja monien yhtäaikaisten vaatimusten mukaan toimittaessa on epäreaalista, että kaikki asiat tulevat tehdyksi vain muistin varassa. Helovuon ym. (2011, s. 78) mukaan muistia tukevia ratkaisuja ja riittävästi varmistavia työvaiheita voidaan kehittää toiminnan tueksi, jolloin unohduksia huomataan aiemmin.

Asioiden tekeminen ja tekemättä jättäminen, väärinkäsitykset ja unohdukset ovat inhimillisiä virheitä (Helovuo ym. 2011, s.76). Jälkeenpäin havaitaan, että inhimillinen virhe olisi ollut vältettävissä, jos huomioidaan saatavilla oleva tieto, varmistetaan toimenpiteen oikeellisuus

tai olisi toimittu toisin. Turvallisuuden kehittämistoimissa kohdistetaan huomio herkästi ihmisten toimintaan arvioimatta sitä, mikä sai toimimaan kyseisellä tavalla. Liiallisen työkuorman ja stressin välttäminen sekä riittävän vireystilan varmistaminen ja väsymyksen hallinta ovat edellytyksiä suoriutua tiedonkäsittelytehtävistä mahdollisimman hyvin (mts. 79). Paineet ja liiallinen työkuorma voivat aiheuttaa henkistä uupumusta ja sillä on vaikutusta yksilön hyvinvoinnille. Stressi ja kiihtymys heikentävät suoritustasoa varsinkin tehtävissä, missä vaaditaan ajattelukykyä. Stressin vaikutuksesta tarkkaavaisuus heikkenee ja huomiokyky pienenee (mts. 80). Vuorokauden valvominen vastaa promillen humalatilaa suorituskyvyssä, puolentoista vuorokauden valvominen puoltatoista promillea jne. (mts. 81).

Teknologian kehitys tuo uusia mahdollisuuksia hoitotyöhön ja edistää potilasturvallisuutta, mutta sen monimuotoisuus altistaa uudenlaisille riskeille ja vaaratapahtumille (Helovuo ym., 2011, s.73). Kehittyneen teknologian ja tietotekniikan käyttö vaatii erityistä tietoisuutta niiden tuomista uusista haasteista. Haasteisiin on varauduttava suunnitelmalla, jos sähköinen potilasjärjestelmä kaatuu, kuinka saadaan selville kriittiset potilastiedot (mt.).

Numminen (2016, s. 128) kirjoittaa, että älykkäät mittalaitteet vaativat sairaanhoitajilta osaamista, mutta samalla antavat uusia tapoja ja mahdollisuuksia olla asiakkaan tukena. Terveydenhuollon tulevaisuuden haasteena on datan lisääntyvä määrä, mitä asiakkaat tuottavat (mts. 129). Suuri määrä yksityiskohtaisia tietoja, esimerkiksi askeltietojen sekuntitasolla tapahtuva seuranta, luotettavuus ja valmiiden analyysien puute voivat tuottaa ongelmia. Laitteiden määrä lisääntyy ja niiden mittaustiedot halutaan hyödyntää ja näyttää terveydenhuollossa asioidessa. Asiakkaiden kiinnostus omaan hyvinvointiinsa kertoo heidän innostuksestaan, ja se on heidän voimavaransa ja heitä tulisi kannustaa enemmän. Tämän päivän ja tulevaisuuden teknologia kasvattaa ja antaa mahdollisuuden asiakkaiden oman vastuun ottamiseen (mts. 130). Tiedon muuttaminen teoksi on yhä haasteena. Teknologia mahdollistaa inhimillisen ja aidon kohtaamisen paikasta ja ajasta riippumattomaksi. Sairaanhoitajan tarkoitus on edistää asiakkaan terveyttä ja teknologia mahdollistaa sen (mts. 131).

Tekoälyn ja robotiikan kehittyminen tuovat muutoksia terveydenhuoltoon mahdollistaessaan julkisten palvelujen digitalisoitumisen. Sosiaali- ja terveysministeriön digitalisaatiolinjaukset 2025 (STM, 2016, s. 26) -julkaisun mukaan kaikkien tarpeet on huomioitava kehitettäessä palveluita. Uudet sukupolvet ovat tottuneet hyödyntämään digipalveluita, jolloin ne ovat

heille välttämättömiä (mts. 4). Myös ikäihmisten palvelussa digitalisaatiota hyödynnetään. STM:n julkaisussa (2016, s. 9) todetaan, että tietoturvallisuus huomioidaan digitaalisia palveluja tuotettaessa ja yksityisyyden suoja turvataan.

Cilliers (2020, s. 4) toteutti tutkimuksessaan puettavista laitteista: yksityisyys ja tietoturva ongelmista. Puettavat laitteet sisältävät tässä tutkimuksessa erilaiset terveysmonitorit, kuntomittarit sekä älykellot. Yli puolet vastaajista (51,89 %) totesivat, etteivät ole tietoisia omistamiensa mobiiliterveyslaitteiden tietoturvakäytännöistä eivätkä siitä, kuinka heidän tietojaan ja yksityisyyttään suojataan. Sama määrä vastaajista kuitenkin ymmärsi terveystietojen olevan arka tai luottamuksellinen aihe. Vastaajista 52,83 % ei ole tietoisia, kuinka heidän mobiililaitteensa lähettää, käsittelee ja merkitsee arkaluonteisia tietoja (mts. 5). Tutkimuksessa 47,17 % vastaajista ei ole huolestunut terveystietojen rehellisyydestä tai siitä kuka pääsee kerättyyn tietoon käsiksi. Kun taas enemmistö vastaajista (66,04 %) harkitsivat luottamuksellisuutta tai anonymiteettiä heidän terveystiedoillensa, koska ne ovat tärkeitä. Yli puolet (55,66 %) vastaajista ymmärsi, että hyödyttääkseen terveystietojensa kerääjää, niiden täytyy olla koko ajan saatavilla. Tulevaisuudessa uhkana voi olla vaara tiedon siirtymisessä puettavasta laitteesta mobiilisovellukseen tai tietokoneohjelmiston ohjelmaan. Yli kolmasosa vastaajista (34,91 %) oli vahvasti sitä mieltä, että ovat tietoisia siirtyvistä tiedoista, ne mitkä lähetetään tai tallentuvat heidän mobiililaitteeseensa. Alle puolet (43,40 %) vastaajista ei ole tietoisia siitä, kuinka salattuja arkaluonteiset tiedot ovat, kun ne siirtyvät puhelimeen tai tietokoneelle. Yli puolet vastaajista (56,61 %) eivät olleet tietoisia keneen ottaa yhteyttä tietoturvaloukkausta epäillessään. Vastaajista 25,29 % varmuuskopioivat kriittisiä tai arkaluonteisia tietoja rutiininomaisesti ja testasivat jaksottaisesti (mt.).

Bani ym. (2020, s. 1) toteutti tutkimuksen sairaanhoitajille elektronisten terveysmittareiden käyttöön liittyen Yhdistyneissä Arabiemiirikunnissa. Tutkimuksessa oli mukana 562 osallistujaa (70 % kutsutuista), joista vain 7 (1,2 %) oli Emiraateista (mts. 7). Muiden kansalaisuudet olivat arabeja, intialaisia ja pakistanilaisia sekä filippiiniläisiä (mt.). Tutkimuksen kohteena olivat yksityisyys, luottamuksellisuus, tietoturva sekä potilasturvallisuus (mts. 1). Tutkimus toteutettiin kyselylomakkeella sekä ryhmähaastatteluina. Suurimmalla osalla hoitajista (58,5 %) oli työkokemusta enemmän kuin kymmenen vuotta (mts. 7). He raportoivat käyttävänsä keskimäärin 2,33 +/- 0,66 tuntia kirjaamiseen työvuoron aikana

(mt.). Hoitajat myös ilmaisivat huolensa sähköisten terveysmittareiden turvallisuudesta (mts. 1). Useimmin raportoidut puutteet olivat hallinnointiin liittyvä tietoturvallisuus, koulutuksen puute ja tuntemattoman käyttäjän pääsy tiedostoon. Potilasturvallisuuteen vaikuttavia puutteita ilmoitettiin olevan erityisesti tuntemattomien henkilöiden pääsy järjestelmään, johdon suorittaman auditoinnin puute järjestelmässä esiintyvien virheiden poistamiseksi, huono kommunikointi tavarantoimittajien kanssa sekä kirjaamiseen tarvittavan ajan pituus (mts. 11). Tutkimuksessa todetaan, että sairaanhoitajien täytyy opiskella lakiin perustuvia sekä eettisiä näkökantoja potilastietojen turvallisesta tallentamisesta lisäten ammatillista tietämystään ja turvata potilastiedot (mt.).

Tolonen ja Vepsäläinen Lääkärilehden (2020, s. 2012) artikkelissa toteavat, että erityisesti lääkintälaitteiden ja tietojärjestelmien kyberturvaan voidaan vaikuttaa etenkin hankintavaiheessa. He kokevat lääkärin asiantuntemuksen olevan tarpeen hankintoja tehdessä, koska monet uudet laitteet esitellään ensimmäisenä lääkäreille. On tarpeen keskustella hankinnasta organisaation tietoturva-asiantuntijoiden ja hankintayksikön kanssa. Hankinnan esivaiheeseen kuuluu laitteen tietojenkäsittelyyn liittyvien toimintaperiaatteiden läpikäynti. Uusien tietojärjestelmien tallentaessa tietoja pilvipalveluun ne eivät ole enää vain yhdessä paikassa. Tiedot saattavat sijaita ympäri maailmaa, jos pilvi sijaitsee esimerkiksi Yhdysvalloissa tai muualla EU:n ulkopuolella.

> ”Sairaalassa laitteet ovat yhä useammin kytkettyjä internettiin, sairaaloiden tietoverkkoihin ja toisiin laitteisiin, mikä osaltaan lisää tietoturvariskejä. Tilannetta heikentää se, että aiempi lääkintälaitteisiin liittyvä lainsäädäntö ei ottanut suoraan kantaa tietoturvariskeihin, joten markkinoilla on vielä pitkään laitteita, joissa voi olla vakaviakin tietoturvapuutteita”, Tolonen ja Vepsäläinen kirjoittaa.

Vahinkoa haluavan hyökkääjän ei tarvitse suoraan päästä käsiksi sairaalan tietoverkkoon vaan hyökkääminen onnistuu ”lennosta” (Tolonen ja Vepsäläinen, 2020, s. 2013). Hyökkääjä voi halutessaan rikkoa laitteen käyttökelvottomaksi tai ohittaa tietoturvatoimintoja päästäkseen muuttamaan laitteen asetuksia, esimerkiksi lääkeannoksien suuruutta. Nämä tilanteet vaarantavat potilasturvallisuuden (mt.).

Tolonen ja Vepsäläinen Erikoislääkäri-lehden (2020, s. 10) katsauksessa ovat kirjoittaneet otsikolla ”Vaarantuuko potilasturvallisuus kyberuhkien edessä?” ja pohtivat

varautumista kyberuhkiin. Kyberuhkien mahdollisuus pitää ottaa huomioon jokapäiväisessä työskentelyssä. Uudet lääkinnälliset laitteet, robotiikka ja tekoäly sekä älykkäät sensorit ja ohjelmistot yhdistettynä uusiin tehokkaampiin tietoverkkoihin ja pilvipalveluihin muodostavat yhä laajempia kokonaisuuksia. Terveydenhuollon nopea tietotekninen murros edellyttää myös tietoturvan huomioimista uudella tavalla, koska heikko tietoturva vaarantaa potilasturvallisuuden monin eri tavoin. Käyttämällä USB-muistitikkua eri laitteiden ja tietojärjestelmien välillä on mahdollista tartuttaa virus laitteesta toiseen (mts. 10–12).

> ”Potilastietojen muuttuminen tietojärjestelmissä vahingossa tai tahallisesti voi johtaa vääriin diagnooseihin. Tietoturvaa on myös se, että kaikki tarvittava potilastieto on saatavilla ja käytettävissä silloin, kun hoitotoimenpiteistä päätetään. Esimerkiksi tietojärjestelmän käyttökatkoksen aikana ei välttämättä saada hoitopäätöksiin tarvittavaa potilastietoa silloin, kun sitä tarvittaisiin.”, Tolonen ja Vepsäläinen kirjoittavat.

Langer (2017, s.122) kirjoittaa, että ”hakkeri”, joka on halukas sijoittamaan merkittäviä resursseja yhtä kohdetta vastaan, ja kun otetaan huomioon todennäköisyys, että jollakin vaaditulla palvelulla on dokumentoimaton ja hyödynnettävissä oleva vika, mikään verkkotietokone ei voi koskaan väittää olevansa täysin luodinkestävä. Valppautta tarvitaan jatkuvasti. Paras yksittäinen toimenpide, jonka mikä tahansa sivusto voi tehdä, on suorittaa tietoturvaharjoituksia. Valitettavasti kyberturvallisuus ei ole vitsi, vaan se on tappavan vakava asia, jossa vuorotellen ”mustavalkoiset hatut” vastustavat toistensa liikkeitä (mts.123). Mustat hatut (Black Hats): ovat ihmisagentteja, jotka pyrkivät saamaan hallinnan muiden tietokoneisiin tai laitteisiin laittomin tarkoituksin. Valkoiset hatut (White Hats): ovat ihmisagentteja, jotka yrittävät estää Mustien Hattujen toimintaa. He voivat olla organisaation työntekijöitä tai urakoitsijoita (mts. 118).

Hoitotiede-lehti (2019, s. 274) on julkaissut Saarikosken ym. monimenetelmäisen tutkimuksen potilasturvallisuudesta hallituksen päätöksenteossa. Tutkimuksen kohteena oli neljä sairaanhoitopiiriä ja siinä selvitettiin sairaanhoitopiirien hallitusten jäsenten ymmärrystä potilasturvallisuudesta, potilasturvallisuudesta saadun tiedon käyttöä päätöksenteossa sekä sitä, miten potilasturvallisuus näkyy sairaanhoitopiirien hallitusten pöytäkirjoissa. Jäsenillä ei ollut yhdenmukaista käsitystä siitä, mitä potilasturvallisuus tarkoittaa. Eniten tunnistettiin hoidon turvallisuuteen liittyviä asioita. Lääkehoidon turvallisuus ja laiteturvallisuus olivat vieraampia. Jollain tasolla potilasturvallisuuteen liitettiin tietosuoja,

tietoturva sekä salassapitosäännökset. Yksittäisinä asioina mainittiin vaaratapahtumien raportointi ja toimintatavat niissä. Laajalti käytössä olevan vaaratapahtumien HaiPro-raportointijärjestelmän tunnisti vain muutama. Sairaanhoitopiirien hallitusten jäsenet pitivät tärkeänä, että asiantuntijat kävisivät kertomassa heille potilasturvallisuudesta ja tämä näkyi myös tutkimuksen johtopäätöksissä (mts. 274–275).

5.3 Tietoturvaan liittyvien haittatapahtumien ennaltaehkäisy

Uudessa, helmikuussa 2022 voimaantulleessa STM:n Asiakas- ja potilasturvallisuusstrategiassa vuosille 2022–2026-julkaisussa (STM,2022) on runsaasti linjauksia, joilla pyritään lisäämään potilasturvallisuutta ja ennaltaehkäisemään haittatapahtumien syntyä. Yhdeksi tavoitteeksi on nimetty ammattilaisten osaamisen ylläpitäminen koko työuran ajan sekä opiskelijoiden riittävä perehdytys turvallisuuskäytäntöihin harjoittelujakson alussa (mts. 27). Uusia työntekijöitä perehdytettäessä käytäisiin läpi omavalvontasuunnitelma tai asiakas- ja potilasturvallisuussuunnitelma sekä lääkehoitosuunnitelma. Strategiaa toteutettaessa uusille työntekijöille tarjotaan riittävä perehdytys uusiin tehtäviin, työskentely-ympäristöön, organisaation työtapoihin ja -kulttuuriin sekä laitteisiin ja tietojärjestelmiin, joita he työssään tulevat käyttämään. Ongelman yhtenäisten ja potilasturvallisten toimintatapojen käytännöissä sekä laite ja tietojärjestelmän turvallisen käytön kehittämiselle muodostaa henkilöstön vaihtuvuus, sijaisuudet ja satunnainen vuokratyövoima (mts. 28).

Sosiaali- ja terveydenhuollon esihenkilöiden ja johtajien johtamisosaamista työhyvinvoinnin, henkilöstökokemuksen ja turvallisen työkulttuurin ohjaamisessa ja hallinnassa olisi lisättävä koulutuksen avulla (STM 2022, s. 27). Tavoitteena on siirtyä suorituksen johtamisesta valmentavaan johtamiseen, jolloin esihenkilö ottaa huomioon henkilöstön mielipiteitä kysellen, kuunnellen ja kannustaen (mt.). Strategiassa pidetään tärkeänä, että henkilöstö sitoutuu sovittuihin menettelytapoihin, josta kokeneimmat työntekijät ovat vastuussa välittäessään työyhteisön turvallisuuskulttuuria myöhemmin tulleille työntekijöille. Vastuu sovituista käytännöistä poikkeaviin toimintatapoihin puuttumisesta on johdolla (STM 2022, s. 28).

Täydennyskoulutuksen säännölliseen järjestämiseen pidempään töissä olleille työntekijöille tarvitaan alueellisia osaamiskeskuksia, jotka määrittelevät ammattiryhmäkohtaiset kriteerit osaamiselle yhdessä oppilaitosten ja korkeakoulujen kanssa (STM 2022, s. 29). Sosiaali- ja

terveydenhuollon ammattilaisia kouluttavien asiakas- ja potilasturvallisuuskoulutusta lisättäisiin ja jokaisen ammattilaisen oikeutta ja velvollisuutta osaamisen ylläpitämiseksi ja lisäämiseksi korostetaan strategiassa. Työnantajat ovat velvollisia huolehtimaan henkilöstön riittävästä osallistumisesta täydennyskoulutukseen (mt.).

World Health Organization (WHO) (2021, s.57) toteaa uudessa Globaali potilasturvallisuus toimintasuunnitelmassa 2021–2030, että maailman siirtyminen paperipohjaisista järjestelmistä digitaaliseen infrastruktuuriin mahdollistaa potilasturvallisuuden tutkimuksen ja innovaatioiden toteutumisen ajantasaisesti, tehokkaasti sekä kustannustehokkaalla tavalla. Tietotekniikan kehitys terveydenhuollossa tarjoaa mahdollisuuksia tukea hoidon antamista ja itsehoitoa potilaslähtöisesti päätöksenteon tukemisessa. Digitaalisuuteen siirtyminen ei ole riskitön infrastruktuureille, algoritmit tai tietomurrot voivat sotkea kokonaisen populaation. Lähitulevaisuudessa nämä teknologiat tullaan rajaamaan hyvin resursoituihin terveydenhuolto järjestelmiin. Terveydenhuollon tietojärjestelmät ovat kehittyneet potilasturvallisuuden vuoksi. Käsitellessämme uusia teknologioita meidän tulee olla valppaita, jotta tunnistamme tahattomat turvallisuus vaikutukset. Kansallisten digitaalisten strategioiden tulisi sisältää itsenäisiä, muotoilevia arviointiohjelmia. Arvioiden tulisi pyrkiä ymmärtämään digitaalisten järjestelmien käyttämättä jättämisen, koska se on olennainen teknologian käyttöönotolle ja potilasturvallisuudelle, että voidaan ymmärtää niiden käyttö (mt.).

Tapauksessa, jossa yrityksellä on tuhansia laitteita puolustettavana, on otettava käyttöön jokin triage-algoritmi riskin määrittämiseksi ja valvontaresurssien osoittamiseksi vastaavasti (Langer, 2017, s.122). Järjestelmien suojaamisessa voivat auttaa:

- Verkon palomuurien asentaminen.
- Käytäntöjen määrittäminen tietokoneisiin; mikä estää tavallisia käyttäjiä mahdollisuudesta asentaa ohjelmistoja.
- Poista tarpeettomat palvelut kaikilta palvelimilta; jäljellä olevat palvelut sekä liikenteen että lokiliikenteen rajoittamiseksi.
- Suorita kaikkien kriittisten palvelintiedostojen säännölliset tarkistussummat, tallenna tulokset vain liittämistietovälineeseen ja ristiin tarkistus reaaliaikaisen järjestelmän kanssa.

- Tunkeutumistestin kriittiset palvelimet, joilla testataan hyväksikäyttöjä Nessus / Metasploitin kaltaisilla työkaluilla. Tulosten perusteella voit neuvotella kehittäjien kanssa haavoittuvuuksien lieventämiseksi ja oppia ohjelmointikäytäntöjä, jotka välttävät niitä tulevaisuudessa (eli puolustaudu injektiohyödykkeitä vastaan) (mt).
    - Nessus on avoimen lähdekoodin verkon haavoittuvuusskanneri, joka käyttää yleisiä haavoittuvuuksia ja on Tenablen kehittämä (ITperfection, i.a).
    - Metasploit-kehys on erittäin tehokas työkalu, jota sekä verkkorikolliset että eettiset hakkerit voivat käyttää tutkiakseen järjestelmällisiä haavoittuvuuksia verkoissa ja palvelimissa (Petters, 2020).

6 OPINNÄYTETYÖN JOHTOPÄÄTÖKSET JA POHDINTA

6.1 Opinnäytetyön johtopäätökset ja tietoturvan kehittyminen

Tietoturvallisuuden ylläpitämiseksi organisaatiossa on ajantasainen omavalvontasuunnitelma, jonka toteutumisesta vastuu kuuluu organisaation johdolle. Kuitenkin paremman turvallisuuskulttuurin kypsymiseen tarvitaan koko organisaation henkilökunnan ponnistelua. Jokainen henkilöstön jäsen huolehtii, että toimii tietoturvallisesti ja ohjeiden mukaisesti minimoiden riskit tiedon joutumisesta vääriin käsiin. Koulutuksen ja harjoittelun tarve samoin kuin lääketieteellisten tietojen tärkeys on oivallettu ja niiden merkitys on alkanut korostua organisaatioiden hallinnossa. Uudet työntekijät, sijaiset ja opiskelijat perehdytetään järjestelmien ja internetissä langattomasti olevien laitteiden käyttöön ja vaaroista informoidaan. Henkilöstön jatkuvasta kouluttamisesta tulisi huolehtia uusimman näyttöön perustuvan tiedon saamiseksi ja pätevöitymiseksi soveltaa turvallisuustoimenpiteitä. Erityisesti johtavan henkilöstön tietoisuus tietoturvasta, tietoturvan hallinnasta ja jatkuvan koulutuksen tärkeydestä ovat polkuja hyvään turvallisuusjohtamiseen. Opinnäytetyön tutkimusanalyysiä pääsee tarkastelemaan kuviosta 5.

Tietoturvan muodostuminen hoitotyössä	Tietoturvaa vaarantavat tekijät hoitotyössä	Haittatapahtumien ennaltaehkäisy ja tietoturvan kehittyminen
- Sähköisten potilas- ja tietojärjestelmien oikeaoppinen käyttö - Palomuurit ja suojattu verkkoyhteys -Kirjautuminen henkilökohtaisilla tunnuksilla tai ammattikortilla ja monivaiheisen tunnistautumisen käyttö -Paperisten ja sähköisten henkilötietojen käsittely, dokumentointi, raportointi, tietojen säilytys, luovutus ja hävitys -Luotettava tunnistautuminen (potilas, läheinen, henkilökunta ja viranomaiset) -Aineiston ja laitteen suojaaminen luvattomalta pääsyltä, käytöltä ja tiedon siirrolta, tietokatkoilta, tiedon muunnoksilta ja hävittämiseltä -Tilojen tarkoituksenmukaisuus	-Potilasjärjestelmien väärinkäyttö -Järjestelmän käytön osaamattomuus ja tietoturvaan liittyvä tietämättömyys -Tietomurrot -Käytäväkeskustelut, puhelinkeskustelut ja raportointi julkisessa tilassa -Järjestelmän auki jättäminen omilla tunnuksilla -Papereita ei tule unohtaa tulostimeen tai paikkaan, josta ohikulkijat voivat nähdä ne -Suojaamattomat tietojärjestelmät, ohjelmistot, laitteet, palvelut, tietoaineistot, tietoliikenne ja huonosti suunnitellut tilat	-Jokaisen henkilökunnan jäsenen huolehdittava omasta toiminnastaan tietoturvan säilyttämiseksi (salassapitovelvollisuus!) -Organisaatiossa omavalvontasuunnitelman laatiminen ja sen noudattaminen ja valvontatoimet -Uusien työntekijöiden, sijaisten ja opiskelijoiden perehdyttäminen tietoturva-asioihin -Pitkään organisaatiossa olleiden rooli turvallisuuskulttuurin luomisessa, säilyttämisessä ja siirtämisessä uusille ammattilaisille -Jatkuva henkilöstön kouluttautuminen koko työuran ajan ja työntekijöiden sitoutuminen menettelytapoihin -Tiedon luottamuksellisuuden, koskemattomuuden ja käytettävyyden ylläpitämiseksi tarvitaan tietoturvatoimia - Asiakkaan suostumus tarvitaan tietojen luovuttamiseen eri yksiköille, erimerkiksi muille hoitoa antaville hoitotahoille - Turvajärjestelmien säännöllinen päivittäminen: internetissä olevien laitteiden päivityksien hyväksyminen ja vanhojen laitteiden uusiminen, ellei päivityksiä ole enää saatavilla

Kuvio 5. Tiivistelmä tutkimustuloksista

Sairaanhoitajan eettinen velvollisuus on potilaan yksityisyyden säilyttäminen, joka toteutuu tietosuojasäännösten toteutuessa. Lisäksi ammatillisen vastuullisuuden noudattamisen todettiin lisäävän sairaanhoitajan työtyytyväisyyttä ja potilaiden emotionaalista vakautta. Tietoturvan kehittämisen ja riskien ehkäisemiseksi on tärkeää, että potilaat ja terveydenhuollon ammattilaiset tekevät yhteistyötä. Tietoturvan merkitystä tulisi korostaa, koska se on tärkeä osa potilasturvallisuutta.

6.2 Eettisyys ja luotettavuus

Tuomi ja Sarajärvi (2018, s. 163) kirjoittavat, että tutkimustoiminnassa on arvioitava tehdyn tutkimuksen luotettavuutta ja tuloksista syntyneitä johtopäätöksiä. Tutkijan vastuulla on rehellinen tutkimustulosten tulkinta ja tulosten soveltaminen. Tutkijan on olennaista arvioida

kriittisesti jo tehtyjä tutkimuksia aiheesta. Luotettavuuden tarkastelussa on huomioitava muun muassa tutkimuksen kohdetta ja tarkoitusta, tutkijan omaa sitoumusta tutkittavaan aiheeseen, aineiston keruun menetelmiä, tutkimuksen kohderyhmänä toimivia, tutkimuksen kestoa, aineiston analyysiä ja raportointia (mts.164).

Kuvailevassa kirjallisuuskatsauksessa arvioidaan eettisten tavoitteiden toteutuminen alkaen tutkimuskysymyksen muotoilusta ja jatkuen tutkimusetiikan noudattamisena kaikissa katsauksen vaiheissa (Kangasniemi ym. 2013, s. 292). Luotettavuus osoitetaan perustelemalla valittu tutkimuskysymys sekä lähdekirjallisuus, kuvaillaan argumentoinnin vakuuttavuus sekä prosessin johdonmukaisuus. Raportin tekstissä tuodaan esiin luotettavuus ja osuvuus aineiston valinnassa, mikä tarkoittaa, että esitellään valittua kirjallisuutta ja perusteita valinnalle tutkimuskysymykseen nähden. Luotettavuutta heikentää analysoitujen tutkimusten liian vähäinen peilaaminen teoreettiseen taustaan, tutkimustulosten yksipuolinen ja valikoiva tarkastelu, keskittyminen tutkijoihin tutkimuksen sijaan sekä tulevaisuuden tutkimuskohteiden unohtaminen pysähtymällä nykytilanteeseen. Myös tulevaisuuden tutkimuskohteet olisi huomioitava (mts. 298).

Tuomi ja Sarajärvi (2018, s. 165) ovat kirjassaan koonneet luotettavuuden parantamiseen vaikuttavia tekijöitä. Tutkijalla tulee olla riittävästi aikaa tutkimuksen tekoon. On myös puhuttu tutkimusprosessin julkisuudesta, joka tarkoittaisi tutkijan yksityiskohtaista raportointia tekemästään työstä, tutkijakollegat arvioivat prosessia sekä tutkimuksen kohderyhmä arvioi tulosten ja johtopäätösten osuvuutta. On myös mahdollista laskea yksimielisyyskerroin, jolloin kaksi tutkijaa luokittelee saman aineiston ja tuloksia verrataan keskenään. Ulkopuolisen luokittelijan saaminen ei kuitenkaan aina ole kovin helppoa (mts. 166).

6.3 Jatkotutkimuksen aiheet

Tekoälyn ja robotiikan käytön lisääntyminen terveydenhuollossa sekä laitteet, jotka ovat kytkettyjä internettiin, sairaaloiden tietoverkkoihin ja toisiin laitteisiin, lisäävät tietoturvariskejä. Laitteita hankittaessa tarvitaan monipuolista tietoa ja näkemyksiä eri tahoilta, joten asiantuntijaryhmän perustaminen ennen hankintoja on hyödyllistä. Laitteisiin tutustuminen, niiden vertailu ja huomioon otettavat asiat tutkittaisiin ryhmässä, johon kuuluisi asiantuntijoita, jotka käyttävät hankittavaa laitetta (lääkärit, sairaanhoitajat) sekä tietosuojavastaava.

Jatkossa voitaisiin tutkia, kuka tai ketkä organisaatiossa päättävät esimerkiksi lääkintälaitteiden hankinnoista ja millä perusteilla valittuun hankintaan on päädytty. Onko käyttäjien kokemuksia ja vaatimuksia kartoitettu ja huomioitu suunniteltaessa hankintaa.

Toinen kiinnostava aihe on, että kuinka useassa sairaalan ja terveysaseman vuodeosastolla on käytössä vielä kahden tai useamman henkilön potilashuoneet, joissa lääkärinkierrot tapahtuvat toisen potilaan läsnä ollessa. Kuinka kyseiset potilaat ovat itse kokeneet tilanteet ja ovatko pystyneet esimerkiksi tuomaan kaikki mielessä olevat asiat esiin lääkärin kanssa keskusteltaessa. Toinen potilas samassa huoneessa väliverhon takana voi olla este etenkin arkaluonteisen asian jakamiseksi, vaikka se olisi hoidon kannalta olennaista. Lääkärinkierron aikana potilaan henkilökohtaisesta terveydestä ja tilanteesta puhuminen toisen potilaan läsnä ollessa vaarantaa tietoturvallisuutta.

Jatkotutkimuksen aiheeksi voisi olla myös tietoturvan toteutuminen eri organisaatioissa. Tutkimuskysymyksiä voisivat olla seuraavat: Kuinka monessa organisaation osastoissa käytetään samoja tunnuksia koneelle kirjautuessa? Kuinka moni hoitaja tai lääkäri toteuttaa tietoturvallisuutta jokapäiväisessä työssä? Kuinka hyvin uusia työntekijöitä tai opiskelijoita perehdytetään tietoturvallisuuteen? Kuinka usein organisaatiossa toteutetaan tietoturva tarkastuksia? Kuinka usein tietoturvakursseja järjestetään työntekijöille organisaatiossa? Lääkärit ja hoitajat saattavat pitää tietoturvallisuutta itsestään selvänä asiana, jonka takia sitä ei huomioida työarjessa. Tietosuoja ja tietoturvallisuus ovat kuitenkin sidoksissa kaikkeen hoitotyön osa-alueeseen.

7 POHDINTA

Aiheena tietoturvan tarkastelu hoitotyössä on mielenkiintoinen ja tärkeä osa hoitotyötä, jotta potilasturvallisuutta vaarantavat tekijät voidaan huomioida. Henkilöstön jatkuvan koulutuksen merkitys korostuu ja erityisesti organisaation johdon kouluttautumiseen kiinnitetään huomiota. Aihe on nyt erityisen ajankohtainen, kun Suomi neuvottelee Nato-jäsenyydestä ja Venäjän odotetaan vastaavan siihen kyberiskuilla ja tietoliikenteen häirinnällä. Suojautuminen ja erityinen tarkkaavaisuus tietojärjestelmien ja laitteiden käytössä on välttämätöntä. Päivälehti Ilkka-Pohjalaisessa (Kulmala, 9.5.-22 s. 4) oli kirjoitus, jossa digitaalisen markkinoinnin ja viestinnän asiantuntija Joonas Autio neuvoi it-laitteiden käyttäjiä huolehtimaan mobiililaitteidensa päivityksestä hyväksymällä ohjelmantarjoajan päivitykset. Päivittämättömät laitteet voivat luoda tunkeutujalle portin tileille ja esimerkiksi älypuhelimen sisältämiin henkilötietoihin. Samassa raportissa varoitettiin myös vanhoista laitteista, joihin päivitystä ei enää ole saatavilla. Suojaamattomuutensa vuoksi ne ovat alttiita tietoturvarikkomuksille.

Tietosuoja ja tietoturva ovat myös eettisiä kysymyksiä hoitotyössä. Hoitotyöhön on perinteisesti kuulunut vaitiolovelvollisuus sekä potilas- ja asiakastietojen salassapito. Potilaan ja asiakkaan on voitava luottaa siihen, että hän voi luottamuksellisesti kertoa sairauksistaan sekä taustoista kenenkään levittämättä tietoja ulkopuolisille.

Aineiston etsimisen tuloksena ei löytynyt yhtään väitöskirjaa, joka olisi käsitellyt tietoturvaa osana potilasturvallisuutta hoitotyössä. Olisi tärkeää, että tulevaisuudessa aihetta tutkittaisiin ja saataisiin lisää tietämystä ja kokemusta henkilöstön, johtajien ja asiantuntijoiden käyttöön. Tietoturvatoimien tulisi kuulua jokaisen taitoihin, niin jokapäiväisissä työtehtävissä kuin vapaa-ajallakin. Tietoturva-asioista ollaan yhä kiinnostuneempia, kuten Seppänen (2020, s. 2818) artikkelissaan ”Tietoturva kiinnostaa nyt kaikkia” Lääkärilehdessä toteaa. Kiinnostus potilastietojärjestelmien tietoturvaa kohtaan lisääntyi Vastaamon tietovuodon seurauksena. Omien henkilötietojen pysyminen sivullisten ulottumattomissa halutaan varmistaa.

OmaKantaan kirjautumalla voi tutustua tietoihin, joita on kirjattu itsestä ja pyytää tarvittaessa korjauksia tai poistoja tietoihin, mutta organisaation koneella ei ole lupa tarkastella ilman perusteita kenenkään tietoja, edes omia potilastietojaan. Suomalainen lääkäriseura Duodecimkin kirjoittaa tietojen käytöstä ja katselusta, että ainoastaan työtehtävien hoidon

edellyttämiin tietoihin on potilas- ja henkilötietojen käsittelyoikeus. Omien tietojen katselu on siis yksiselitteisesti kiellettyä. Kaikkien tulisi muistaa, että tietojen käsittelyn asianmukaisuutta valvotaan käsittelystä syntyvien lokitietojen avulla.

Sähköinen tiedonhallinta terveyden ja hyvinvoinnin palveluksessa on Suomessa korkealla tasolla, maamme on kansainvälisestikin kärkimaita, josta esimerkkejä ovat Kanta-palvelut ja työsuojeluvalvonnan digitalisaatio (STM 2016:5, s. 4). Digitalisaation avulla pyritään lisäämään tuottavuutta, vaikuttavuutta ja kustannustehokkuutta. Uusi sukupolvi kasvaa digitaalisten palveluiden käyttäjäksi, jolloin ne eivät ole vain pelkkä lisä, vaan pääasia (mt).

Hoitotyöntekijöillä on mahdollisuus pienilläkin asioilla vaikuttaa potilaiden tietosuojan säilymiseen. Esimerkiksi haastattelu- ja neuvontatilanteessa usean hengen potilashuoneessa olevan potilaan kanssa etsitään rauhallinen huone, jossa voidaan keskustella kenenkään ulkopuolisen kuulematta. Keskusteltaessa potilaan asioista hoitajien kesken, huomioidaan ympäristö, jolloin toimisto, ovi suljettuna, olisi turvallisin. Eettiset näkemykset huomioon ottaen keskusteltaisiin vain hoidon kannalta tärkeistä asioista. Myös puhelimeen puhuttaessa huomioidaan kuuloetäisyydellä olevat. Erään hankalan kysymyksen muodostaa lääkärinkierto huoneessa, jossa on useampia henkilöitä. Vaikka väliverhoja laittamalla saadaan näkösuojaa, puhe kuitenkin kuuluu kaikille, varsinkin jos yhden tai useamman potilaan kuulo on alentunut ja lääkärin ja hoitajan on puhuttava äänekkäämmin, jotta potilas kuulisi.

Terveydenhuollon palvelut ovat riippuvaisia tietojen saannista toteutettaessa hoitotyötä. Salassa pidettävien tietojen kanssa työskennellessä nousee suureen rooliin tietosuoja ja tietoturvallisuus. Terveydenhuollossa organisaation yhtenä tehtävänä onkin tietoturvallisuuden sekä tietosuojan kehittäminen ja hallinnointi. Hoitajien työhön kuuluu potilaistietojen käyttö vain olemassa olevien oikeutuksien perusteella. Tietovuodon tai tietoturvariskiin liittyvien tilanteiden sattuessa tulisi olla kaikilla terveydenhuollon ammattilaisilla tiedossa, kuinka toimitaan ja mihin otetaan yhteyttä. Palomuurit, vahvat suojausprotokollat, virustorjuntaohjelmat ja salasanasuojaukset ovat välttämättömiä tietoturvan edistämiseksi.

Jokaisen hoitohenkilökunnan jäsenen tulisi olla kiinnostunut tietoturvallisuuden kehittämisestä hoitötyössä ja sen toteutumiseen vaikuttavista tekijöistä. Omaa arjen tietoturvaosaamista voi kehittää esimerkiksi Duodecim Oppiportin tietoturvakurssien avulla ja

lisäkoulutuksilla. Tietoturvan kokonaisvaltainen toteuttaminen vaatii koko terveydenhuollon organisaation yhteispeliä.

LÄHTEET

Andreasson, A., Koivisto, J. & Ylipartanen, A. (2013). *Tietosuojavastaavan käsikirja.* Tietosanoma.

Autti T., & Keistinen T. (2013). Kansallinen potilasturvallisuusstrategia Suomessa: tausta ja tulevaisuuden haasteet. Teoksessa L-M Aaltonen, & Rosenberg P. (toim.), *Potilasturvallisuuden perusteet (s. 141–156).* Duodecim.

Bani Issa, W., Al Akour, I., Ibrahim, A., Almarzouqi, A., Abbas, S., Hisham, F., & Griffiths, J. (2020). Privacy, confidentiality, security and patient safety concerns about electronic health records. *International Nursing Review*, *67*(2), 218–230. https://doi-org.libts.seamk.fi/10.1111/inr.12585

Cilliers L. (2020). *Wearable devices in healthcare: Privacy and information security issues. Health information management*: journal of the Health Information Management Association of Australia, 49(2-3), 150–156. https://doi.org/10.1177/1833358319851684

Etelä-Pohjanmaan sairaanhoitopiiri (EPSHP). (i.a.). *STEPPI 2 – Terveyttä tuottava perushoito (2021–2025)*. https://www.epshp.fi/ammattilaiselle_ja_opiskelijalle/hoitotyo/steppi_-_terveytta_edistava_perushoito

Etelä-Pohjanmaan sairaanhoitopiiri (EPSHP). (2020). *Asiakkuuskertomus. Etelä-Pohjanmaan sairaanhoitopiirin kuntayhtymä.* https://www.epshp.fi/files/12168/asiakkuuskertomus_2019_86216.pdf

Etelä-Pohjanmaan sairaanhoitopiiri (EPSHP). (2021). *Tietoturva- ja tietosuojapolitiikka.* https://www.epshp.fi/files/3508/Etela-Pohjanmaan_sairaanhoitopiirin_tietoturva-_ja_tietosuojapolitiikka_(ID_5001).pdf

Helovuo, A., Kinnunen, M., Peltomaa, K. & Pennanen, P. (2011). Potilasturvallisuus: *Potilasturvallisuuden keskeisiä kysymyksiä havainnollisesti ja käytännönläheisesti*. Fioca.

Itperfection (i.a). *What is NESSUS and How Does it Work?* What is NESSUS and How Does it Work? - ITperfection - Network Security

Kang, J., & Seomun, G. (2021). Information Security in Nursing: A Concept Analysis. *Ad vances in Nursing Science*, *44*(1), 16–30.

Kangasniemi, M., Utriainen, K., Ahonen, S.-M., Pietilä, A.-M., Jääskeläinen, P., & Liikanen, E. (2013). Kuvaileva kirjallisuuskatsaus*:* Eteneminen tutkimuskysymyksestä jäsennettyyn tietoon. *Hoitotiede*, *25*(4), 291–301.

Kinnunen, M., Aaltonen, L-M., & Malmström, R. (2013). Vaaratapahtumien raportointi. Teoksessa L-M Aaltonen, & Rosenberg P. (toim.), *Potilasturvallisuuden perusteet (s. 257–273).* Duodecim.

Kinnunen, M., & Helovuo, A. (2019). *Potilasturvallisuus*. Terveysportti. https://www.terveysportti.fi/apps/dtk/shk/article/shk04802/search/potilasturvallisuus

Konttinen, R., & Mykkänen, J. (2016). Kuka käyttää digitaalisia terveystietojani? Teoksessa Suomen sairaanhoitajaliitto & K. Pirhonen (toim.). *Teknologia sosiaali- ja terveydenhuollossa (s.133–146).* Fioca

Kurki, T., Jylhä, V. & Kekoni, T. (2021). *Asiakasturvallisuus sosiaali- ja terveysalalla*. Gaudeamus.

Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä 784/2021. https://www.finlex.fi/fi/laki/ajantasa/2021/20210784?search%5Btype%5D=pika&search%5Bpika%5D=tietoturva

Langer S. G. (2017). *Cyber-Security Issues in Healthcare Information Technology. Journal of digital imaging, 30*(1), 117–125. https://doi.org/10.1007/s10278-016-9913-x

Middaugh, D. J. (2016). Nursing Management. Do Security Flaws Put Your Patients' Health at Risk? *Medsurg Nursing,* 25(2), 131–132.

Morris, R. L., Ruddock, A., Gallacher, K., Rolfe, C., Giles, S., & Campbell, S. (2021). Developing a patient safety guide for primary care: A co-design approach involving patients, carers and clinicians. *Health Expectations*, *24*(1), 42–52. https://doi-org.libts.seamk.fi/10.1111/hex.13143

Niela-Vilén, H & Hamari, L. (2016). Kirjallisuuskatsauksen vaiheet. Teoksessa M. Stolt, A. Axelin, & R. Suhonen (toim.), *Kirjallisuuskatsaus hoitotieteessä* (2. p., s. 25–31). Juvenes Print.

Numminen J. (2016). Asiakkaan omamittaus osana hoitotyötä. Teoksessa Suomen sairaanhoitajaliitto & K. Pirhonen (toim.). Teknologia sosiaali- ja terveydenhuollossa (s.123–131). Fioca

Palmu, P. (2019). https://www.etevat.fi/blogi/miksi-varmuuskopiointi-on-tarkeaa-nain-turvaat-tiedostosi

Petters, J. (2020). *What is Metasploit? The Beginner's Guide*. What is Metasploit? The Beginner's Guide (varonis.com). Varonis.

Phillion, M. (2021). *Cybersecurity is patient safety*. *Healthcare Life Safety Compliance, 24*(11), 7–9.

Rajaniemi, T. (2020). Emmehän me ole se heikoin lenkki? *Lääkärilehti, 75(47), 2493.*

Saarikoski, T., Haatainen, K., Roine, R. & Turunen, H. (2019). Potilasturvallisuus sairaanhoitopiirin hallituksen päätöksenteossa. Monimenetelmäinen tutkimus neljässä sairaanhoitopiirissä. *Hoitotiede 2019, 31* (4), 269–280.

Sand J. (2019). *Päijät-Hämeen kyberhyökkäys – mitä opittiin?* Lääkärilehti.

Seppänen A. (2020). *Tietoturva kiinnostaa nyt kaikkia*. Lääkärilehti. https://www.laakarilehti.fi/ajassa/ajankohtaista/tietoturva-kiinnostaa-nyt-kaikkia/

Sosiaali- ja terveysministeriö (STM). (2016). *Sosiaali- ja terveysministeriön digitalisaatiolinjaukset 2025: Digitalisaatio terveyden ja hyvinvoinnin tukena.* http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/75526/JUL2016-5-hallinnonalan-ditalisaation-linjaukset-2025.pdf

Sosiaali- ja terveysministeriö (STM). (2017). *Potilas- ja asiakasturvallisuusstrategia 2017–2021.* http://urn.fi/URN:ISBN:978-952-00-3963-9

Sosiaali- ja terveysministeriö (STM). (2017). *Potilas- ja asiakasturvallisuusstrategia* 2017–2021: Toimeenpanosuunnitelma. http://urn.fi/URN:ISBN:978-952-00-4133-5

Sosiaali- ja terveysministeriö (STM). (2022). *Asiakas- ja potilasturvallisuusstrategia ja toimeenpanosuunnitelma 2022–2026.* http://urn.fi/URN:ISBN:978-952-00-8464-6

Suomalainen Lääkäriseura Duodecim. (04.12.2017). *Tietosuoja terveydenhuollossa*. Haettu 06.11.2021.

Terveyden ja hyvinvoinnin laitos (THL). *Potilasturvallisuusopas 2011*. Potilasturvallisuuslainsäädännön ja -strategian toimeenpanon tueksi. https://thl.fi/documents/10531/104871/Opas%202011%2015.pdf

Terveyskylä. (2020). *Tietosuoja ja tietoturva.* https://www.terveyskyla.fi/terveyskyl%C3%A4n-palvelut/e-terveyspalveluiden-opas/tietosuoja-ja-tietoturva

Tolonen, P., & Vepsäläinen, P. (2020). *Vaarantuuko potilasturvallisuus kyberuhkien edessä? Erikoislääkärilehti 30*(1), 10–12.

Tolonen, P., & Vepsäläinen, P. (2020). *Lääkäri, kuinka varaudut kyberuhkiin hankinnoissa? Lääkärilehti 75(*39), 2012–2013.

Traficom. Liikenne- ja viestintävirasto, Kyberturvallisuuskeskus. (2022). *Monivaiheinen tunnistautuminen suojaa käyttäjätilejäsi*. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/monivaiheinen-tunnistautuminen-suojaa-kayttajatilejasi?toggle=Todennuslaite%20tai%20suojausavain

Tuomi, J., & Sarajärvi A. (2018). *Laadullinen tutkimus ja sisällönanalyysi.* Tammi.

Valvira. (2021). *Sosiaali- ja terveydenhuollon tietojärjestelmät*. Sosiaali- ja terveysalan lupa- ja valvontavirasto. https://www.valvira.fi/terveydenhuolto/sosiaali-ja-terveydenhuollon-tietojarjestelmat

World Health Organization. (2021). *Global patient safety action plan 2021–2030: towards eliminating avoidable harm in health care*. World Health Organization. https://apps.who.int/iris/handle/10665/343477. License: CC BY-NC-SA 3.0 IGO