Etätyötä tekevien sairaanhoitajien kyberturvallisuusosaaminen

Integratiivinen kirjallisuuskatsaus

Pauliina Lehto

Opinnäytetyö, ylempi AMK
Toukokuu 2025
Terveyden edistäminen YAMK

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Kuvailulehti

Lehto, Pauliina

Etätyötä tekevien sairaanhoitajien kyberturvallisuusosaaminen – Integratiivinen kirjallisuuskatsaus

Jyväskylä: Jyväskylän ammattikorkeakoulu. **Toukokuu 2025**, 44 sivua

Terveys- ja hyvinvointialat, Sairaanhoitaja (YAMK), Terveyden edistäminen, opinnäytetyö, ylempi AMK

Julkaisun kieli: suomi

Julkaisulupa avoimessa verkossa: kyllä

Tiivistelmä

Digitalisaation myötä terveydenhuollon etätyön lisääntyminen on pakottanut pohtimaan hoitohenkilöstön kyberturvallisuustaitoja, sillä aikaisemmat tutkimukset kyberturvallisuudesta sosiaali- ja terveydenhuollossa ovat olleet niukkoja.

Tehtävänä oli integratiivisen kirjallisuuskatsauksen avulla kartoittaa, millä tekijöillä etätyötä tekevien sairaanhoitajien kyberturvataidot kehittyvät ja millaisia puutteita osaamisessa on. Toteutustapana aineistohaussa käytettiin viittä tietokantaa (CINAHL, MEDIC, Cochrane, PubMed, ProQuest) sekä harmaata kirjallisuutta ja mukaan valikoitui kahdeksan artikkelia, jotka analysoitiin induktiivisella sisällönanalyysilla.

Tuloksissa tunnistettiin viisi keskeistä teemaa: asenteet ja käyttäytyminen, digitaalisten taitojen merkitys, organisaation ja johdon rooli, etätyön vaikutus käytäntöihin sekä koulutuksen ja teknologian saatavuus. Johtopäätöksissä todettiin, että etätyön kyberturvariskit edellyttivät sekä teknisen osaamisen että tietoisuuden vahvistamista, ja korostettiin räätälöidyn jatkuvan koulutuksen ja selkeiden toimintamallien tarvetta. Lisäksi organisaation tuen ja johdon sekä teknisen henkilöstön vuorovaikutuksen nähtiin olevan ratkaisevaa turvallisen etätyöympäristön varmistamisessa.

Avainsanat (asiasanat)

Etätyö, kyberturvallisuus, sairaanhoitajat, integratiivinen kirjallisuuskatsaus, sisällönanalyysi

jamk

Description

Lehto, Pauliina

Cybersecurity Competence of Remote-Working Registered Nurses – An Integrative Literature Review

Jyväskylä: JAMK University of Applied Sciences, May 2025, 44 pages

Health and Welfare, Master of Health Care, Master's Degree in Health Promotion, Master thesis

Permission for open access publication: Yes

Language of publication: Finnish

Abstract

The rapid spread of remote work in healthcare, accelerated by digitalisation and the COVID-19 pandemic, highlighted a lack of comprehensive research on nurses' cybersecurity skills within social and healthcare settings. The aim was to conduct an integrative literature review to identify factors influencing cybersecurity competence among remote-working registered nurses and to uncover existing skill gaps.

A systematic search of five databases (CINAHL, MEDIC, Cochrane, PubMed, ProQuest) and manual citation tracing yielded eight relevant studies. Selected articles were evaluated and synthesised using inductive content analysis.

In results five main themes emerged: attitudes and behaviour in cybersecurity, the role of digital skills, organisational and managerial support, the impact of remote work on security practices, and the availability of training and technology. Findings indicated that ensuring secure remote nursing required both technical competence and heightened awareness. Tailored, continuous training programmes and clear procedural models were deemed essential. Furthermore, effective collaboration between leadership, IT personnel, and nursing staff was identified as critical to maintaining a safe remote work environment.

Keywords

Remote work, cybersecurity, nursing, integrative literature review, content analysis

Sisältö

Taulukot

1 Johdanto

Kyberturvallisuuden yhteys sosiaali- ja terveydenhuoltoalalle on aikaisemmin ollut hyvin epämääräistä. Digitalisaation ulottuessa terveydenhuoltoon, on tullut tarve myös pohtia kyberturvallisuutta. COVID 19- pandemian sekä etätyöhön siirtymisen myötä aihe on tullut tutuksi ja viimeistään Ukrainan sodan alettua tältä ei enää ole kukaan sosiaali- ja terveydenhuoltoalan työntekijä voinut välttyä. Maailmanpoliittinen epävarmuus ja soteuudistuksen tuomat paineet luovat turvattomuutta myös terveydenhuoltoalalle. Suomi on jo entuudestaan niittänyt mainetta kansainvälisesti julkisissa sähköisissä asiointipalveluissa ja tulevaisuuden tavoitteet ovat vielä korkeammalla (Neittaanmäki, Pöyhönen & Lehto 2019, 16, 20).

Terveydenhuolto kuuluu yhteiskunnan kriittiseen infrastruktuuriin, jota kautta pystytään häiritsemään yhteiskunnan toimivuutta ja vieläpä kohtuullisen pienellä vaivalla (Lekshimi 2022, 2). Lisääntyvät kyberhäirinnän hyökkäykset haastavatkin sote-alan osaajat päivittämään osaamistaan kyberturvallisuusasioissa (Ravelin, Laukka, Heponiemi, Kaihlanen, Kanste 2021, 221-231).

Kyberturvallisuus nähdään terveydenhuoltoalalla kokonaisuutena, josta tietoturva on vain yksi osa-alue. Terveydenhuollon digitalisaation myötä on noussut esiin myös laiteturvallisuuden näkökulma ja häiriötilanteet näissä (Giansanti 2020, 1). Tiedonkulku ei enää ole fyysisesti rajattua sairaalan tai hoitopaikan seinien sisälle. Niin tallennettu tieto kuin esim. lääkintälaitteiden reaaliajassa välittyvä tieto siirtyy verkkoja pitkin toisaalle. Koulutuksen ja tiedotuksen on oltava keskeisiä näkökohtia terveydenhuollon kyberturvallisuudessa (Giansanti 2020, 3).

Hoitohenkilökunnan kyberturvallisuustaitojen tutkimus on ollut melko vähäistä verrattuna yleisempään kyberturvallisuuden- tai terveydenhuollon tietoturvaan liittyvään tutkimukseen. Kyberturvallisuustaitojen tutkimus hoitohenkilökunnan keskuudessa on alue, joka on saanut viime vuosina kasvavaa huomiota, mutta siitä on silti saatavilla rajallisesti tutkimustietoa. Jonkin verran löytyy tutkimusta, joka tarkastelee hoitohenkilökunnan kyberturvallisuustaitoja erityisesti terveydenhuollon näkökulmasta. Näissä tutkimuksissa on keskitytty hoitajien ja muiden terveydenhuollon ammattilaisten tietoturvaosaamisen arviointiin, koulutustarpeiden tunnistamiseen ja kyberturvallisuustietoisuuden lisäämiseen. (He, Aliyu, Evans, Luo 2021, 2.)

Vaikka kyberturvallisuustaitojen tutkimus hoitohenkilökunnan keskuudessa on vielä melko rajallista, on se tärkeä aihe, joka on herättänyt kasvavaa kiinnostusta terveydenhuollon tietoturvassa (Norri-Sederholm, Laitinen, Lehto, Kari 2019, 96). Tulevaisuudessa voidaan odottaa aiheen tutkimuksen lisääntyvän sekä panostusten ohjattavan hoitohenkilökunnan kyberturvallisuustaitojen arviointiin ja kehittämiseen, jotta voidaan varmistaa potilastietojen ja organisaatioiden tietoturvan suojaaminen.

Opinnäytetyön tarkoituksena on kirjallisuuskatsauksen turvin tutkia, millaista tietoa on etätyön vaikutuksesta sairaanhoitajien kyberturvataitoihin ja millaisilla tekijöillä voidaan vaikuttaa etätyötä tekevien sairaanhoitajien kyberturvataitoihin. Tästä saatua tietoa voidaan käyttää päätöksenteon tukena laadittaessa ohjeistuksia tai koulutustarpeen kartoittamisessa tai järjestämisessä. Tavoitteena on löytää tähän saakka tutkitusta tiedosta mahdollisimman kattavasti tekijät, jotka etätyötä tehdessä vaikuttavat sairaanhoitajien kyberturvataitojen kehittymiseen, löytää tutkimustarpeita ja tätä kautta edistää terveydenhuollon kyberturvallisuutta.

2 Digitalisaatio

Edelleen käynnissä oleva digitalisaatio on todennäköisesti suurin ja kokonaisvaltaisin muutos yhteiskunnassa ja tämän vaikutukset ovat koskeneet laajalti niin yksilöitä, organisaatioita kuin yhteiskuntaa yhteisesti. Se on muuttanut niin työelämää, ihmisten arkipäivää kuin sosiaalista kanssakäymistäkin. Samalla kun se on tarjonnut rajaamattomia mahdollisuuksia, on se myös tuonut uudenlaisia yhteiskunnallisia haasteita kuten digisyrjäytyminen, digitaalisen eriarvoisuuden sekä kyberuhat (Heponiemi, Jormanainen, Leeman, Manderbacka, Aalto, Hyppönen 2020, 1, 9; Neittaanmäki, Lehto, Savonen 2021, 180; Richardson, Lawrence, Schoenthaler, Mann 2022, 1.). Digitalisaatiossa on kyse yhteiskunnallisesta prosessista, jossa hyödynnetään teknologisen kehityksen tuomia mahdollisuuksia ja jossa integroidaan digitaalitekniikka osaksi elämän jokapäiväisiä toimintoja niin yksilö- kuin yhteisötasolla (Neittaanmäki ym. 2021, 9). Digitalisaatiolla tarkoitetaan palvelujen ja toimintojen sähköistämistä, niiden siirtymistä verkkoon. Digitalisaatiolla haetaan ratkaisuja eri yhteiskunnan osa-alueille ja tämä edellyttää uutta toimintakulttuuria, kehittämistä, uusia toimintaprosesseja sekä uudenlaista johtamista (Ahonen, Kinnunen, Kouri, Liljamo, Saranto 2016, 231; Herukka, Tuohimaa, Kiviniemi, Koivunen 2021, 1). Tiedonhankinta, sen käsittely ja tiedolla johtaminen korostuvat entisestään (Neittaanmäki ym. 2021, 180).

2.1 Terveydenhuollon digitalisaatio

Digitalisaation avulla pyritään myös ratkaisemaan alati pahenevaa ja syvenevää terveydenhuollon resurssipulaa. Selvää onkin, että parhaiten toteutuessaan tämä keventääkin ja järkevöittää hoitohenkilökunnan työtaakkaa. Sosiaali- ja terveydenhuollon palveluissa käytetään tietojärjestelmiä, informaatio- ja viestintäteknologiaa sekä sähköistä tiedonhallintaa (Argaw, Troncoso-Pastoriza, Lacey, Florin, Calcavecchia, Anderson, Burleson, Vogel, O`Leary, Eshaya-Chauvin, Flahault 2020, 2.) Sähköiset palvelut ovat olennainen sekä näkyvä osa SOTE-uudistusta ja näillä tavoitellaan paremmin saatavilla olevia ja yhdenvertaisia palveluja (Ahonen, Kinnunen, Kouri, Liljamo, Saranto 2016, 231). Palvelujärjestelmän vaikuttavuutta ja tehokkuutta lisätään sähköisen tiedonhallinnan avulla (Neittaanmäki ym. 2021, 64).

2.2 Terveydenhuollon etäasiointipalvelut

Digitalisaation myötä terveydenhuollon etäpalveluja on kehitetty lisääntyvässä määrin vastaamaan niin asiakkaiden kuin palveluntarjoajien tarpeita sekä mahdollisuuksia. Valvira on määritellyt, että etäpalveluilla tarkoitetaan terveydenhuollossa sitä, että potilaan tutkiminen, diagnostiikka, tarkkailu, seuranta, hoitaminen, hoitoon liittyvät päätökset tai suositukset perustuvat esim. videon välityksellä verkossa tai älypuhelimella välitettyihin tietoihin ja dokumentteihin (Potilaille annettavat terveydenhuollon etäpalvelut 2022). Terveyden ja hyvinvoinninlaitos (2021) on puolestaan raportissaan määritellyt etäasiointipalvelun niin reaaliaikaiseksi kuin ei-reaaliaikaiseksi asioinniksi, joka toteutetaan puhelimitse, kirjeitse tai internetissä, esimerkiksi chatissä, videoyhteydellä tai verkkopalvelussa. Heinonen, Lindfors ja Nygård (2022, 129) käyttävät kotihoitoon kohdistuneessa tutkimuksessaan käsitettä etähoito, jossa on määritelty asiakkaan hoito, ohjaus ja tukeminen terveyteen ja hyvinvointiin liittyvissä asioissa tietoverkkoja ja muuta tekniikkaa hyödyntämällä. Etäpalveluiden avulla pystyttiin välttämään fyysisiä kontakteja epidemia-aikana (Ravelin ym. 2021, 221).

THL:n Avohilmo-rekisteriin on kerätty pääasiassa julkisen avoterveydenhuollon käyntitietoja, mutta viime vuosina tähän on lisätty myös yksityinen sektori. Raportista ilmenee, että sairaanhoitajat ja terveydenhoitajat hoitavat suurimman osan avoterveydenhuollon etäkontakteista. Vuonna 2020 sairaanhoitajilla ja terveydenhoitajilla etäkontakteja oli yhteensä 7,1 miljoonaa. Tämä tarkoitti heidän työstään 38 prosenttia, kun taas lääkäreillä tämä oli 22 prosenttia. (Terveyden ja hyvinvoinninlaitos 2021.)

3 Terveydenhuollon kyberympäristö

Kyber (cyber) -sana on etuliite, jota käytetään yleensä yhdyssanan määriteosana ja joka tarkoittaa digitaalista kokonaisuutta, joka kohdistuu pääosin digitaaliseen järjestelmään ja/tai sisältöön. Kyberympäristöllä tarkoitetaan toimintaympäristöä, joka koostuu yhdestä tai useammasta digitaalisesta tietojärjestelmästä tai -sisällöstä. (Turvallisuuskomitea 2018.)

Sosiaali- ja terveydenhuollon ammattilaiset käyttävät digitaalisia välineitä ja palveluja työssään lisääntyvässä määrin päivittäin. Palveluiden toteutuksessa tukeudutaan merkittävästi tieto- ja vies-

tintäteknologiaan. (Argaw ym. 2020, 1.) Teknologian nopea kehitys on lisännyt uudenlaista rikollisuutta ja tämä lisää haasteita tuottaa palveluita tietoturvallisesti ja vaatimusten mukaisesti (Neittaanmäki ym. 2021, 131). Tietojärjestelmiin liittyvät häiriötilanteet ovatkin nousseet viime vuosina julkisuuteen aiempaa herkemmin (Vuorinen 2019, 13). Toukokuussa 2017 levisi internetin kautta WannaCry-kiristyshaittaohjelma saastuttaen yli 200 000 konetta yli 150 maassa muutaman vuorokauden aikana ja aiheuttaen arviolta 4 miljardin dollarin kustannukset (Lekshimi 2022, 1; Neittaanmäki ym. 2021, 132). Suomessa tunnetuin näistä lienee Vastaamon tapaus vuonna 2020, jossa yli 30 000 asiakkaan hoitotiedot levisivät rikolliseen käyttöön (YLE Uutiset 2023).

Tyypilliset kyberhyökkäykset terveydenhuoltoa kohtaan ovat hakkerointeja ja viruksia, laitteiden varastamista sekä palvelunestohyökkäyksiä. Nämä aiheuttavat merkittävää häiriötä terveydenhuollossa ja usein ne huomataan vasta jälkikäteen, jolloin niiden selvittäminen on haastavaa ja tiedot ovat jo vuotaneet (Lehto, Pöyhönen & Lehto 2019, 11). Terveydenhuoltoalan puutteellinen varautuminen muihin toimialoihin verrattuna on nostettu useissa lähteissä merkittäväksi tekijäksi niin taloudellisten resurssointien kuin henkilöstön puutteellisen koulutuksen vuoksi (Argaw ym. 2020, 1, 5; Kruse, Frederick, Jacobson, Monticone 2017,1, 4).

Terveydenhuollon tekee erityisen haavoittuvaksi se, että potilaan hoito on täysin riippuvainen koko sairaalaympäristön toimivuudesta ja huomioon on otettava sairaalaan kytkeytyvä digitaalinen järjestelmä- ja laiteympäristö (Lehto ym. 2019, 16). Monien tapauksien taustalla on myös henkilöstön tietämättömyys tietoturvasta ja se aiheuttaa huonojen päätöksien tekemisen (Lekshimi 2022, 2; Neittaanmäki ym. 2021, 139). Henkilöstön jatkuva koulutus sekä vuoropuhelu eri toimijoiden välillä ovat tärkeitä keinoja lisätä tietoisuutta ja vähentää eri hyökkäyksien onnistumista (Leksimi 2022, 4; Lehto ym. 2019; 45-46; Blek & Solankallio-Vahteri 2022, 360; Argaw 2020, 5).

3.1 Kyberuhka

Kyberuhka on määritelty Turvallisuuskomitean Kyberturvallisuuden sanastossa (2018, 25) mahdollisesti toteutuvaksi haitalliseksi tapahtumaksi tai kehityskuluksi, joka tapahtuu tai kohdistuu kybertoimintaympäristöön ja vaarantaa siitä riippuvaisen toiminnon. Se voi aiheutua toteutuneista tietoturvauhkista mutta myös digitaalisessa viestintäympäristössä toteutettavista, yhteiskuntaa vaarantavista teoista. Kyberuhat voivat kohdistua yhteiskunnan elintärkeitä toimintoja, kansallista

kriittistä infrastruktuuria tai kansalaisia vastaan joko suoraan tai välillisesti. Uhat voivat olla peräisin maan rajojen sisältä tai ulkopuolelta. (Turvallisuuskomitea 2018, 25.) Terveystoimiala on kyberhyökkäysten yleisin kohde (Norri-Sederholm ym. 2019, 90).

3.1.1 Haittaohjelmat

Haittaohjelmat ovat ohjelmia, jotka voivat tarkoituksellisesti vahingoittaa tai varastaa tietoja tietojärjestelmässä tai sen osassa (Sanastokeskus 2009). Tällaisia ovat esimerkiksi erilaiset madot, virukset, sekä vakoilu- ja kiristysohjelmat. Yleensä haittaohjelmat leviävät sähköpostien liitetiedostojen, haittaohjelmilla saastutettujen verkkosivustojen sekä haavoittuvien palvelinten kautta (Kyberturvallisuuskeskus 2020). Haittaohjelmia voidaan levittää joko väärennetyillä sovelluksilla tai väärennetyillä päivityksillä. Haittaohjelmia saattaa tarttua myös suojaamattomilla sivustoilla vieraillessa (Traficom 2023). Haittaohjelmahyökkäykset voivat vaarantaa potilastietojen luottamuksellisuuden, eheyden ja saatavuuden (Obaid, Salman 2022, 31).

3.1.2 Tietokalastelu

Huijausviestit, joiden tarkoituksena on varastaa tunnuksia tai tietoja, kutsutaan tietojenkalasteluviesteiksi. Niiden tarkoituksena on saada terveydenhuollon työntekijät tai potilaat paljastamaan arkaluonteisia tietoja, kuten kirjautumistunnuksia, potilastietoja tai maksutietoja. Näitä viestejä voidaan lähettää sähköpostitse, tekstiviesteillä tai jopa puheluiden kautta. Terveydenhuoltojärjestelmissä voidaan käyttää tietojenkalasteluhyökkäyksiä, jotta päästään käsiksi potilastietoihin, vaarantaakseen lääketieteelliset laitteet tai käynnistää kehittyneempiä hyökkäyksiä. (Obaid ym. 2022, 31.) Tietojenkalastelu on yksi johtavista terveydenhuollon tietomurtojen syistä ja nämä vaikuttaisivat olevan nousussa. (Alder 2024.)

3.1.3 Tietomurrot

Tietomurrolla tarkoitetaan henkilö- tai potilastietojen luvatonta käyttöä tai vuotamista, tunkeutumista suojattuun tietojärjestelmään tai suojatussa tietojärjestelmässä olevan tiedon oikeudetonta tarkastelua (Sanastokeskus 2009; Kyberturvallisuuskeskus 2020). Tietomurto on tapahtuma, jossa arkaluonteiset potilastiedot käytetään, julkistetaan tai käytetään ilman lupaa. Näitä voi esiintyä johtuen erilaisista syistä, kuten kyberhyökkäyksen yhteydessä, vahingossa tapahtuvan tietojen menetyksen tai inhimillisen virheen kautta (Obaid ym. 2022, 35).

3.1.4 Palvelunestohyökkäykset

Palvelunestohyökkäyksessä (DDoS) verkkoa kuormitetaan ylimääräisellä tietoliikenteellä yrittäen lamaannuttaa jokin palvelu tai tietojärjestelmä. Usein kohteena on organisaation julkinen internet-sivusto tai asiakkaiden hyödyntämä palvelu. Toiminta on usein kansainvälistä ja pitkälle automatisoitua (Kyberturvallisuuskeskus 2020). Palvelunestohyökkäykset voivat johtaa kriittisten palvelujen häiriintymiseen, potilastietojen saatavuuden häiriöihin ja merkittäviin taloudellisiin menetyksiin (Obaid ym. 2022, 31).

4 Kyberturvataidot

Turvallisuuskomitean kyberturvallisuuden sanasto (2018, 22) on määritellyt kyberturvallisuuden (cyber security) tavoitetilaksi, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan. Siihen kuuluvat toimenpiteet, joilla voidaan ennakoivasti hallita ja tarvittaessa sietää erilaisia kyberuhkia ja niiden vaikutuksia (Turvallisuuskomitea, 2018). Neittaanmäki, Lehto, Savonen (2021, 143) ovat kuvanneet kyberturvallisuutta toimenpiteiksi, joilla suojaudutaan kyberhyökkäyksiä ja niiden vaikutuksia vastaan sekä toteutetaan tarvittavia vastatoimenpiteitä.

Terveydenhuollon kyberturvallisuus tarkoittaa kaikkia toimenpiteitä, teknologioita, käytäntöjä ja politiikkoja, joilla pyritään suojaamaan terveydenhuollon järjestelmiä, tietojärjestelmiä, potilastietoja ja muita digitaalisia resursseja kyberuhilta, kuten tietomurroilta, haittaohjelmilta, palvelunestohyökkäyksiltä ja tietovuodoilta (Giansanti 2021,1). Koska terveydenhuollossa käsitellään erittäin arkaluontoista ja henkilökohtaista tietoa, tietoturvaloukkaukset voivat aiheuttaa vakavia seurauksia yksilöiden yksityisyydelle ja turvallisuudelle sekä heikentää kansalaisten luottamusta terveydenhuoltoon. Lisäksi kyberhyökkäykset voivat lamauttaa kriittisiä palveluita, vaarantaen potilasturvallisuuden (Obaid 2022, 31).

4.1 Tietoturva

Tietoturva on yksi tietosuojan toteuttamisen keino. Sen tarkoitus on suojata tietoaineisto ja tietojärjestelmät. Tietoturva tarkoittaa muun muassa toimenpiteitä, joilla varmistetaan tiedon luottamuksellisuus ja eheys, järjestelmien käytettävyys sekä rekisteröidyn oikeuksien toteutuminen. Tällaisia keinoja ovat esimerkiksi kulunvalvonta, tilojen lukitus, asiakirjojen turvallinen säilytys ja

hävitys, tietojen salaus ja varmuuskopiointi sekä palomuurin, virustorjuntaohjelman ja varmenteiden käyttö. (Tietosuojavaltuutetun toimisto nd., Turvallisuuskomitea 2018). Tietoturvaan kohdistuvia uhkia ovat haavoittuvuudet, jotka voivat olla mitä tahansa heikkouksia, jotka mahdollistavat vahingon toteutumisen tai jota voidaan käyttää vahingon aiheuttamisessa. Haavoittuvuuksia voi olla tietojärjestelmissä, prosesseissa tai ihmisen toiminnassa. (Terveydenhuoltoalan kyberuhkia 2016, 51.)

4.2 Kyberturvatietoisuus

Kyberturvatietoisuus terveydenhuoltoalalla sisältää hoitajien kyvyt kyberuhkien tunnistamisessa ja ymmärtää niiden vaikutukset. Etätyöntekijöiden on oltava tietoisia kyberuhkista ja turvallisuuskäytännöistä. Heidän tulisi saada riittävä koulutus ja ohjeistus kyberturvallisuudesta, kuten vahvojen salasanojen käytöstä, tietojen jakamisen varovaisuudesta ja tunnuslukujen salaamisesta (Neittaanmäki ym. 2021, 139). Etäviestinnän haasteeksi on todettu tiedonkulkuun liittyvät haasteet; vaikeudet poimia olennainen tieto valtavasta informaatiotulvasta, tiedon epätasaisuus tai jopa että tieto ei kulkenut ollenkaan (Ravelin ym. 2021, 230; Ristolainen, Maijala, Eloranta 2020, 183). Tietotekniset taidot ovat vaihtelevia henkilöstön kesken (Ravelin ym. 2021, 230).

Luottamus on tärkeää etätyössä, mutta se voi myös aiheuttaa haasteita kyberturvallisuuden kannalta (Ravelin ym. 2021). Työntekijöiden on ymmärrettävä organisaation asettamat turvallisuussäännöt ja -rajoitukset sekä ymmärrettävä, miksi niitä tarvitaan. Toisaalta organisaation on myös varmistettava, että työntekijät voivat luottaa siihen, että heidän tietosuojaansa ja yksityisyyttään suojataan asianmukaisesti.

4.3 Tietoturvakäytännöt

Tietoturvakäytännöt ovat käytännön taitoja, kuten turvallisten salasanojen hallinta, tiedostojen salaus ja ohjelmistopäivitykset. Etätyöntekijät joutuvat viestimään ja jakamaan tietoja tiimin jäsenten kanssa erilaisten viestintäkanavien, kuten sähköpostin, pikaviestien tai pilvipalveluiden kautta (Ravelin ym. 2021, 229). On tärkeää, että työntekijät noudattavat tietoturvallisia viestintäkäytäntöjä, kuten salattujen viestien käyttöä ja tietojen jakamista vain asianmukaisesti valtuutettujen henkilöiden kanssa. Toisaalta etätyöntekijöiden on tiedettävä, miten raportoida epäilyttävistä ta-

pahtumista, havaituista kyberuhkista tai tietomurroista. Organisaation on varmistettava, että raportointimekanismit ovat helposti saatavilla ja että työntekijöitä kannustetaan ilmoittamaan mahdollisista tietoturvaloukkauksista välittömästi. (Wang ym. 2021, 146.)

4.4 Tietojenkalastelun tunnistaminen

Tietojenkalastelun tunnistaminen tarkoittaa kykyä havaita epäilyttävät sähköpostit ja linkit, jotka voivat olla kyberhyökkäyksen välineitä. Etätyöstä tehdyissä tutkimuksissa on tunnistettu, että etätyöntekijät saattavat olla alttiita sosiaalisen manipulaation hyökkäyksille, kuten tietojenkalastelulle (Williams ym. 2020, 2). Hyökkääjät voivat esittää työtovereita, asiakkaita tai muita luotettavia tahoja hankkiakseen arkaluonteisia tietoja tai saadakseen työntekijät suorittamaan haitallisia toimia. Työntekijöiden on oltava valppaita ja varovaisia epäilyttävien viestien, puheluiden tai pyyntöjen suhteen. Esimerkiksi, jos joku lähettää huijausviestin tai yrittää saada arkaluontoisia tietoja työntekijältä, etätyöympäristössä voi olla vaikeampaa tarkistaa viestin aitous tai tunnistaa huijaus. Sosiaalisen manipuloinnin onkin tutkittu olevan suurin uhka tietoturvalle kyberympäristössä (Salahdine, Kaabouch 2019, 2). Paljon aikaisemmin tutkittu hoitohenkilökunnan kokema kiire, kuormitus ja stressi heikentävät arviointikykyä ja vaikeuttavat tiedon omaksumista (Ravelin ym. 2021, 229).

5 Etätyö

Etätyö on työn organisointia, josta työnantaja ja –tekijä ovat tehneet erillisen sopimuksen ja jossa työntekijä työskentelee määritellyssä paikassa muualla kuin työnantajan toimitiloissa. Etätyö on määritelty työn pääasiallisen suorituspaikan ulkopuolella tehtävänä satunnaisena tai toistuvana työpäivänä, ja suorituspaikka on esimerkiksi kotona (Kovalainen, Poutanen & Arvonen 2020, 11). Tilastokeskuksen raportissa etätyö on määritelty ansiotyöksi, jota tehdään varsinaisen työpaikan ulkopuolella niin, että siitä on sovittu työnantajan kanssa (Sutela, Pärnänen, Keyriläinen 2019, 251). Etätyöhön liittyy yleensä tietotekniikan käyttö ja olennaista sille on ajasta ja paikasta riippumattomat työjärjestelyt (Tilastokeskus nd.). Työaika voi olla joko kokonaan etätyötä tai vain osittaista eli ns.hybridityömalli (Neittaanmäki ym. 2021, 34).

Digitalisaatio on lisännyt etätyön tekemistä jollain muotoa kaikilla aloilla viime vuosikymmenten aikana ja pandemiatilanne räjäytti tämän (Sutela ym. 2019, 251, 344). Terveydenhuoltoalan on aikaisemmin katsottu soveltuvan etätyöskentelyyn jäykästi ja etätyö ei ole terveydenhuollossa ollut yhtä yleistä kuin muilla toimialoilla, mutta pandemiatilanne sai niin työnantajat kuin –tekijätkin pohtimaan vaihtoehtoisia malleja (Ravelin ym. 2021, 229). Kyberturvallisuutta kartoittaessa tulee huomioida myös etätyöympäristö, joka käsittää fyysiset tilat, laitteet ja ohjelmistot, joita työssä käytetään. Etätyö edellyttää toimivaa teknologiaa, tietoturvan varmistamista sekä työnantajan ja työntekijän välistä luottamusta. Etätyöympäristön tulee olla terveellinen, turvallinen, rauhallinen ja työhön sopiva (Työturvallisuuskeskus 2023). Aikaisemmissa tutkimuksissa on todettu, että etätyöskentelyssä on todettu olevan kohonnut riski kyberturvallisuuden kannalta (Furnell – Shah 2020, 7; Williams ym. 2020, 2; Wang ym. 2021, 146).

6 Terveydenhuollon teknologiat sairaanhoitajien työssä

Lääkinnälliset laitteet ovat yhä lisääntyvissä määrin kytkeytyneinä internetiin, sairaaloiden tietoverkkoihin ja toisiin laitteisiin. Lääkinnällisten laitteiden hyväksyntäkriteereissä ei ole vielä riittävästi huomioitu kyberturvallisuusvaatimuksia ja valitettavan useat automaatiolaitteet ja -järjestelmät on toteutettu tietoturvattomasti (Terveydenhuoltoalan kyberuhkia 2016, 9). Lisäksi lääkinnällisten laitteiden käyttöikä on pitkä verrattuna käyttöjärjestelmien tuen kestoaikaan (Varri 2021). Internetiin tai toisiin laitteisiin kytkeytyneet laitteet voivat tarjota uusia ja tehokkaampia hoitomenetelmiä, sairaalat ovat kehittyneet yhä älykkäämmiksi ja niiden toiminta ei enää rajaudu vain fyysisen sairaalaympäristön sisälle. Kokonaisuudessa tuleekin huomioida kaikki erilaiset ympäristöt, joissa laitteita, sovelluksia ja osa-alueita saatetaan käyttää. Tukipalvelut ovat olennainen osa sairaalan toimintaa. Potilaan hoitoon liittyy suoraan tai välillisesti iso määrä muita toimintoja sekä tukipalveluja ja sujuva hoito edellyttää, että näiden pitää toimia myös häiriötilanteissa. Terveydenhuollon kyberympäristöön kuuluu myös tavanomaista toimistotietotekniikkaa, joka varmistaa toiminnan. Häiriöt maksuliikenteessä vaikuttavat sairaala-/terveyskeskusmaksujen laskutukseen potilailta, henkilökunnan palkkojen maksuun sekä lääke- ja hoitotarvikkeiden ostolaskutukseen. (Vuorinen 2019, 15.)

6.1 Sähköiset potilastietojärjestelmät

Sähköisissä potilastietojärjestelmissä säilytetään potilastietoja. Aikaisemmat tutkimukset ovat vahvistaneet, että potilastietojärjestelmän käytettävyys vaikuttaa suoraan siihen, kuinka järjestelmää käytetään turvallisesti tai epävarmasti. Liian monimutkaiset tai epäintuitiiviset toiminnot lisäävät virheitä ja voivat houkutella kiertämään turvallisuusprotokollia. Hyvin suunniteltu järjestelmä tukee sekä työn sujuvuutta että tietoturvaa. (Khairat, Coleman, Newlin, Rand, Ottmar, Bice, Carson 2019, 5, 8.)

6.2 Telelääketiede

Telelääketieteen termi otettiin käyttöön 1990-luvulla, jolloin se tarkoitti sekä potilaanhoitoon liittyvää toimintaa (tarkkailu, tutkiminen ja hoito) että terveydenhuollon henkilöstön ja potilaiden koulutusta teletekniikkaa hyödyntäen (Kautto, Koskela, Kulmala, Tuovinen, Reponen 2024, 1984). Euroopan yhteisöjen komissio on vuonna 2008 tiedonannossaan määritellyt telelääketieteen tarkoittavan terveyspalvelujen tarjoamista tieto- ja viestintäteknologian avulla tilanteissa, joissa terveysalan ammattilainen ja potilas (tai kaksi terveysalan ammattilaista) sijaitsevat eri paikoissa (Euroopan yhteisöjen komissio 2008). Digitaalinen terveydenhuolto ja etähoito ovat lähes syrjäyttäneet telelääketieteen termin ja käsittävät tänä päivänä mm. videoneuvottelujen ja digitaalisten välineiden käytön hoidon tarjoamisessa.

6.3 IoT-laitteet

Iot eli internet of things-termillä tarkoitetaan esineiden internetiä. Termi tarkoittaa fyysisten laitteiden, ajoneuvojen, rakennusten ja muiden esineiden verkkoa, joissa on sisäänrakennettuja sensoreita, ohjelmistoja ja muita teknologioita, joiden avulla ne voivat kerätä ja vaihtaa dataa internetin kautta (Sanastokeskus 2009). Terveydenhuollossa tällaisia ovat esimerkiksi potilaiden etähoitoon tai -seurantaan käytettävät laitteet. Monet IoT-laitteet, kuten potilasmonitorit, infuusiopumput, EKG-laitteet tai implantit (esim. insuliinipumput) ovat alttiita hyökkäyksille, jos niissä ei ole suojausta kuten salattua tiedonsiirtoa tai käyttöoikeuksien hallintaa. Kyberturvallisuusuhat eivät koske vain tietoa, vaan voivat vaikuttaa suoraan potilaan fyysiseen turvallisuuteen, jos laitetta manipuloidaan, esim. lääkkeen annostelua säädetään.

Monissa tutkimuksissa korostetaan ongelmaa, että IoT-laitteet ovat usein käytössä vuosia ilman päivityksiä (Obaid, Salman 2022, 31). Iot-laitteiden kyberturvallisuusuhat eivät koske vain tietoa, vaan voivat vaikuttaa suoraan potilaan fyysiseen turvallisuuteen, jos laitetta manipuloidaan (esim. lääkkeen annostelua säädetään). Tutkimuksissa on mallinnettu tilanteita, joissa hyökkäys vaikuttaa hoidon laatuun tai viivästyttää diagnoosia (Obaid, Salman 2022, 29, 31). IoT-laitteiden turvallinen käyttö edellyttää hoitohenkilökunnalta kykyä tunnistaa riskejä ja käyttää järjestelmiä oikein.

7 Tietosuojaa ja kyberturvaa koskevat säädökset ja suositukset

Henkilötietolaki (523/1999) ohjaa potilastietojen käsittelyä. Sen tarkoituksena on toteuttaa yksityiselämän ja muita yksityisyyden suojaa turvaavia perusoikeuksia henkilötietoja käsiteltäessä sekä edistää hyvän tietojenkäsittelytapojen kehittämistä ja noudattamista. Lakia sovelletaan henkilötietojen automaattiseen käsittelyyn. (Finlex 1999; Lehto ym. 2019, 72.) Keväällä 2018 EU-maissa astui voimaan yleinen tietosuoja-asetus, GDPR-laki, jonka tarkoituksena on muun muassa vastata uusiin digitalisaatioon liittyviin tietosuojakysymyksiin ja -haasteisiin (Tietosuojavaltuutetun toimisto nd.).

Lainsäädäntö siis velvoittaa sosiaali- ja terveydenhuollossa asiakas- ja henkilötietojen arkaluonteisen käsittelyn suojaamiseen. Lainsäädännön lisäksi tämä liittyy myös terveydenhuollon maineeseen ja uskottavuuteen arkaluontoisten terveystietojen käsittelijänä (Vuorinen 2019, 13). Tämä edesauttaa myös asiakkaan hoidon optimaalista onnistumista sitouttamalla asiakasta omaan hoitoonsa.

7.1 Laiteturvallisuus

Lääkinnälliset laitteet ovat yhä lisääntyvissä määrin kytkeytyneinä internetiin, sairaaloiden tietoverkkoihin ja toisiin laitteisiin. Lääkinnällisten laitteiden hyväksyntäkriteereissä ei ole vielä riittävästi huomioitu kyberturvallisuusvaatimuksia ja valitettavan useat automaatiolaitteet ja -järjestelmät on toteutettu tietoturvattomasti (Terveydenhuoltoalan kyberuhkia 2016, 9). Lisäksi lääkinnällisten laitteiden käyttöikä on pitkä verrattuna käyttöjärjestelmien tuen kestoaikaan (Varri 2021). Internetiin tai toisiin laitteisiin kytkeytyneet laitteet voivat tarjota uusia ja tehokkaampia hoitomenetelmiä, sairaalat ovat kehittyneet yhä älykkäämmiksi ja niiden toiminta ei enää rajaudu

vain fyysisen sairaalaympäristön sisälle. Kokonaisuudessa tuleekin huomioida kaikki erilaiset ympäristöt, joissa laitteita, sovelluksia ja osa-alueita saatetaan käyttää. Tukipalvelut ovat olennainen osa sairaalan toimintaa. Potilaan hoitoon liittyy suoraan tai välillisesti iso määrä muita toimintoja sekä tukipalveluja ja sujuva hoito edellyttää, että näiden pitää toimia myös häiriötilanteissa. Terveydenhuollon kyberympäristöön kuuluu myös tavanomaista toimistotietotekniikkaa, joka varmistaa toiminnan. Häiriöt maksuliikenteessä vaikuttavat sairaala-/terveyskeskusmaksujen laskutukseen potilailta, henkilökunnan palkkojen maksuun sekä lääke- ja hoitotarvikkeiden ostolaskutukseen. (Vuorinen 2019, 15.) Lainsäädännön lisäksi on suosituksia ja standardeja, joista tunnetuin on ISO 27001, joka on kansainvälinen standardi tietoturvan hallinnasta. Siinä määritellään vaatimukset tietoturvan hallintajärjestelmän perustamiselle, toteuttamiselle, ylläpidolle ja jatkuvalle parantamiselle organisaation puitteissa (ISO/IEC 27001: 2022).

8 Sairaanhoitajien kyberturvataitojen osaamisen kehittäminen

Kyberturvallisuustaitojen puute voi vaikuttaa hoitohenkilökunnan työhön muun muassa siten, että tietoturvariskit lisääntyvät hoitajien käsitellessä usein arkaluonteisia potilastietoja ja muita henkilökohtaisia tietoja, kuten sosiaaliturvatunnuksia ja terveystietoja. Jos hoitajilla on heikot kyberturvallisuustaidot, he voivat altistaa nämä tiedot luvattomalle pääsylle, tietovuodoille tai tietomurroille. (Norri-Sederholm ym. 2019, 90.)

Hoitohenkilökunnan käyttäessä päivittäin tietojärjestelmiä, kuten sairaaloiden potilastietojärjestelmiä ja lääkeannostelujärjestelmiä altistuvat nämä haitallisille tietojärjestelmähyökkäyksille. Kyberhyökkääjät voivat pyrkiä hyödyntämään hoitajien heikkoja kyberturvallisuustaitoja esimerkiksi haittaohjelmien, tietojärjestelmärikosten tai verkkohyökkäysten avulla. Tällaiset hyökkäykset voivat vaarantaa potilasturvallisuuden ja häiritä hoitajien työnkulkua. (Argaw ym. 2020, 5; Norri-Sederholm ym. 2017, 91.) Aiemmin on todettu, että hoitohenkilökunnan kesken on suuria eroja ittaidoissa sekä näiden omaksumiseen vaikuttavissa asenteissa (Ravelin ym. 2021, 230).

Paheneva terveysalan henkilöstön kuormittuneisuus ja vaihtuvuus lisäävät omalta osaltaan inhimillisiä erehdyksiä (Blek ym. 2022, 359). Hoitajat voivat olla alttiita kalasteluviesteille tai muille huijauksille, jotka pyrkivät saamaan heitä paljastamaan arkaluonteisia tietoja tai avaamaan haitallisia tiedostoja. Jos hoitajat eivät tunnista näitä huijauksia tai eivät ole tietoisia niiden seurauksista, he voivat tahattomasti altistaa itsensä ja organisaationsa tietoturvariskeille (Norri-Sederholm ym.

2019, 91; Terveydenhuoltoalan kyberuhkia 2016, 7, 8). Kiire heikentää arviointikykyä, etenkin kun tiedot, taidot ja käytänteet ovat vielä omaksumisvaiheessa (He, Aliyu, Evans, Luo 2021, 3; Williams ym. 2020, 2).

Hyvien tietoturvakäytäntöjen noudattaminen on keskeistä kyberturvallisuuden kannalta. Jos hoitajat eivät ole tietoisia organisaationsa tietoturvakäytännöistä tai eivät noudata niitä, se voi johtaa tietoturvaloukkauksiin (Leksimi 2022, 2). Esimerkiksi heikot salasanat, salasanojen jakaminen tai laitteiden lukitsematta jättäminen voivat altistaa organisaation tietomurroille tai luvattomalle pääsylle (Blek ym. 2022; 345). Useamman kuin yhden henkilön käyttämät tunnukset tietojärjestelmiin ja laitteisiin ovat valitettavan yleinen käytäntö terveydenhuollossa (Terveydenhuoltoalan kyberuhkia 2016, 5). Tietoisuuden puute saattaa näkyä siten, että osa hoitajista on vähemmän tietoisia uusimmista kyberturvallisuusuhkista ja -menetelmistä. Tietoturvallisuuden jatkuvasti muuttuessa on tärkeää pysyä ajan tasalla uhkista ja suojautumiskeinoista. Heikot kyberturvallisuustaidot voivat johtaa siihen, että hoitajat eivät tunnista tai osaa reagoida uusiin uhkiin, mikä voi altistaa heidät ja organisaation tietoturvaloukkauksille. (He ym. 2021, 6; Norri-Sederholm ym. 2019, 95.) On tärkeää, että hoitajilla on riittävät kyberturvallisuustaidot ja tietoisuus, jotta he voivat suojella potilastietoja ja ylläpitää turvallista toimintaympäristöä. Tässä korostuukin työnantajan rooli.

8.1 Tietoturvapolitiikka

Tietoturvapolitiikka kattaa organisaation ohjeet ja säännöt tietoturvan edistämiseksi. Kyberturvallisuus tulisi olla sisäänrakennettuna organisaation toimintaan niin operatiivisen, oikeudellisen kuin taloudellisenkin näkökulman vuoksi. Kyberturvallisuuden hyvä taso edellyttää toimivan teknologian lisäksi myös sitä, että koko henkilöstö on perehtynyt ja sitoutunut hyviin tietoturvakäytäntöihin. (Kyberturvallisuuskeskus 2020, 22.) Monet terveydenhuoltoalan kyberturvallisuusalan osaajista ovat töissä organisaatioiden tietohallintayksiköissä. Kuitenkin suuri osa terveydenhuollon suurimmista kyberuhista liittyvät lääketieteellisiin laitteisiin, joiden hallinta ei tyypillisesti kuulu tietohallinnon tehtäviin. Organisaation osaaminen on toisin sanoen hajallaan. (Kyberturvallisuuskeskus 2020, 26.)

8.2 Tuki ja resurssit

Työnantajan tarjoamat työkalut ja koulutukset kyberturvan ylläpitämiseksi. Lukuisat eri viimevuotiset tutkimukset alleviivaavat, että organisaatioiden tulisi tarjota asianmukaista koulutusta ja tukea hoitajille digi- ja kyberturvallisuustaitojen parantamiseksi ja tietoturvakäytäntöjen noudattamiseksi (Blek ym. 2022, 355; He ym.2021, 6; Ravelin ym. 2021, 231; Kruse ym. 2017, 7). Neittaanmäki ym. (2021, 143) sekä Norri-Sederholm ym. (2019, 86) ovat mm. painottaneet, että tarvittavan kyberosaamisen hallinta on johdon vastuulla ja kaikilla organisaation työntekijöillä tulee olla riittävät tiedot kyberturvallisuudesta ja tarvittavat kyberturvallisuusosaaminen omaan tehtävään liittyen. Jotta nopeasti muuttuvaa kyberympäristöä voidaan hallita, tulee johdon tarjota ammattilaisille tarvittavat työkalut ja ajantasainen koulutus (Neittaanmäki ym. 2021, 143; Obaid ym. 2022, 35). Säännölliset koulutukset kyberuhkien tunnistamisesta ja parhaista käytännöistä sekä simulaatiot ja harjoitukset ovat tässä avainasemassa.

8.3 Kyberturvatietoisuus

Kyberturvatietoisuudessa korostuu viestinnän merkitys. Etätyöntekijöiden on oltava tietoisia kyberuhkista ja turvallisuuskäytännöistä. Heidän tulisi saada riittävä koulutus ja ohjeistus kyberturvallisuudesta, kuten vahvojen salasanojen käytöstä, tietojen jakamisen varovaisuudesta ja tunnuslukujen salaamisesta (Neittaanmäki ym. 2021, 139). Etäviestinnän haasteeksi on todettu tiedonkulkuun liittyvät haasteet; vaikeudet poimia olennainen tieto valtavasta informaatiotulvasta, tiedon epätasaisuus tai jopa että tieto ei kulkenut ollenkaan (Ravelin ym. 2021, 230; Ristolainen ym. 2020, 183). Tietotekniset taidot ovat vaihtelevia henkilöstön kesken (Ravelin ym. 2021, 230). Siinä missä hoitohenkilökunnan digitaaliset taidot saattavat olla hyvät, voi löytyä suuria puutteita kyberturvataidoista. Digitaidot ovat laajempi käsite, joka kattaa yleiset digitaalisen teknologian käyttöön liittyvät taidot, kun taas kyberturvataidot keskittyvät erityisesti tietoturvaan ja kyberuhkien torjuntaan. Molemmat taidot ovat kuitenkin tärkeitä digitaalisessa maailmassa, ja niiden kehittäminen auttaa yksilöitä toimimaan tehokkaasti ja turvallisesti digitaalisessa ympäristössä.

Kyberturvataidot (engl. cybersecurity skills) viittaavat erityisesti taitoihin ja osaamiseen, jotka liittyvät tietoturvaan ja kyberuhkien torjuntaan. Kyberturvataidot keskittyvät digitaalisten järjestelmien ja verkkojen suojaamiseen haitallisilta hyökkäyksiltä, tietomurroilta, tietovarkauksilta ja

muilta kyberrikoksilta. Kyberturvataitojen hankkiminen sisältää muun muassa tietoturvaan liittyvien peruskäsitteiden ja -tekniikoiden ymmärtämisen, tietojärjestelmien haavoittuvuuksien tunnistamisen, tietomurtojen jäljittämisen, uhkien torjumisen ja tietoturvallisten toimintatapojen omaksumisen (Aaltola, Ruoslahti, Heinonen 2022, 5).

9 Tavoite, tarkoitus ja tutkimuskysymykset

Tutkimuksen tavoitteena on selvittää, miten etätyötä tekevät hoitajat huolehtivat kyberturvallisuuden toteutumisesta työssään. Tarkoituksena on tuottaa tietoa hoitajien kyberturvallisuusosaamisesta ja tunnistamaan mahdollisia kehitystarpeita, jotta voidaan parantaa kyberturvallisuuskäytäntöjä terveydenhuollon etätyössä.

Tutkimuskysymys:

Miten etätyötä tekevien hoitohenkilöiden kyberturvataidot ja digiosaaminen ilmenevät tutkimuskirjallisuudessa?

Opinnäytetyöstä saatua tietoa voidaan hyödyntää työelämän kehittämisessä sekä erityisesti kartoittaessa koulutustarpeita. Saadun tiedon avulla voidaan myös lisätä oman toiminnan arviointia, herättää keskustelua ja siten parantaa potilasturvallisuutta sekä hoitotyön laatua.

10 Toteutus

10.1 Integratiivinen kirjallisuuskatsaus

Tutkimusmenetelmä valitaan tutkimusongelma, tutkimuskysymys ja tiedonintressi silmällä pitäen (Vilkka 2021, 68; Vilkka 2023, 19). Lisäksi tutkimusmenetelmän ja – aineiston keräämiseen vaikuttavat käytettävissä olevat resurssit (Tuomi & Sarajärvi 2018, 97; Vilkka 2021, 70). Integratiivinen kirjallisuuskatsaus on hyvä tapa tuottaa uutta tietoa jo tutkitusta aiheesta ja se auttaa kirjallisuuden tarkastelussa, kriittisessä arvioinnissa ja syntetisoinnissa (Suhonen, Axelin, Stoltin 2016). Integratiivinen kirjallisuuskatsaus on tutkimusmenetelmä, jossa yhdistetään ja analysoidaan erilaisia tutkimuksia ja aineistoja monipuolisesti. Se eroaa perinteisistä systemaattisista katsauksista siten,

että se sallii sekä määrällisten (kvantitatiivisten) että laadullisten (kvalitatiivisten) tutkimusten yhdistämisen. Tavoitteena on saada kattava ja syvällinen ymmärrys tarkasteltavasta ilmiöstä. Integratiivista kirjallisuuskatsausta kuvataan prosessiksi, josta tunnistetaan viisi eri vaihetta: tutkimusongelman nimeäminen, analysoitavan aineiston keruu, aineiston laadun arviointi, aineiston analysointi ja tulkinta sekä tulosten esittäminen (Elo, Kajula, Tohmola, Kääriäinen 2022, 217; Suhonen ym. 1982, 1984).

Integratiivinen kirjallisuuskatsaus on erityisen hyödyllinen silloin, kun halutaan muodostaa kattava ja kokonaisvaltainen käsitys ilmiöstä yhdistämällä eri tieteenalojen ja tutkimusperinteiden tuloksia Se tarjoaa laajemman kuvan tutkittavasta aiheesta mahdollistamalla erilaisten tutkimusmenetelmien ja -aineistojen yhdistämisen, se voi auttaa tunnistamaan uusia teoreettisia yhteyksiä, sitä voidaan hyödyntää useilla tieteenaloilla ja se voi auttaa löytämään alueita, joita ei ole vielä riittävästi tutkittu ja voi täten toimia pohjana uusille tutkimuksille (Elo ym. 2022. 216; Vilkka 2023, 25; Salminen 2011, 8). Koska integratiivinen kirjallisuuskatsaus ei ole yhtä tiukka menetelmällisesti, mahdollistaa se tutkimusprosessin mukauttamisen tarpeen mukaan. Parhaimmillaan se on helposti sovellettavissa käytäntöön, tuottaa monipuolista tietoa, jota voidaan hyödyntää päätöksenteossa tai kehittämisessä. (Sulosaari, Kajander-Unkuri 2016, 107-108.)

10.2 Tiedonhaku ja aineiston hallinta

Teoreettista viitekehystä laatiessa perehdyttiin aihetta koskevaan aiempaan tutkimukseen ja kirjallisuuteen. Kirjallisuushaun tulee pohjautua tutkimuskysymyksiin ja hakuprosessin tulee olla läpinäkyvä ja tuottaa mahdollisimman kattavasti kaikki ne tutkimukset, jotka voivat vastata tutkimuskysymyksiin (Elo, Kajula, Tohmola, Kääriäinen 2022, 217; Malmivaara 2008, 275). Integratiivisessa katsauksessa voidaan aineistona käyttää monipuolisesti niin vertaisarvioituja tutkimuksia kuin käytäntöjä koskevia ammatillisia materiaaleja (Vilkka 2023, 25, 33; Salminen 2011, 31). Tiedonhakustrategiaa käytiin läpi yhdessä JAMK:in kirjaston informaatikon kanssa. Koko kirjallisuuden haku- ja valintaprosessin aikana seurataan systemaattisesti mukaanotto- ja poissulkukriteereitä. Otsikkotasolla pidetään kriteerinä, että otsikosta tai tiivistelmästä tulee löytyä ”cybersecurity” ja ”nurse/health care staff” sekä ”remote work” käsitteet tai niiden synonyymit, joko suomeksi tai englanniksi. Kirjallisuushakua tehdään viidestä eri tietokannasta, CINAHL (Ebsco), Medic, Cochrane, PubMed, ProQuest sekä suomen kielellä että englanniksi. Koska sanasto ei ole aihe-

piirissä täysin vakiintunutta, käytettiin kunkin tietokannan omia sanastoja hakulausekkeen muodostamisessa, jotta löydettiin riittävästi soveltuvia artikkeleita. Hakusanat on johdettu keskeisistä käsitteistä terveydenhuollon kyberturvallisuus, digitaalinen hoitotyö, digitaaliset taidot terveydenhuollossa ja etätyö. Hakulausekkeen muodostamisessa oli tärkeää, että haku tuottaisi nimenomaan tietoa hoitajien kyberturvataidoista ja hakuehdot olisivat kaikissa tietokannoissa mahdollisimman samanlaiset. Pois rajattiin vain kyberturvallisuutta käsittelevät artikkelit ja sellaiset hakutulokset, joissa kyberturvallisuutta tarkasteltiin tietoteknisestä näkökulmasta. Koska aihe on erittäin ajankohtainen ja aiheesta tulee tietoa nopealla vauhdilla, pidettiin harkinnanvaraisena aikarajana 4 vuotta eli mukaan otettiin pääsääntöisesti vertaisarvioituja artikkeleita vuodesta 2021 lähtien. Mukaan otettiin artikkelit tai julkaisut, jotka olivat saatavilla maksuttomina Jyväskylän ammattikorkeakoulun tietokannoista ja joista oli abstrakti tai kokoteksti saatavilla.

Kirjallisuushaku toteutettiin maalis-huhtikuussa 2025. Tutkimukseen valikoitui kahdeksan tutkimusartikkelia. Systemaattisen tietokantahaussa artikkeleita valikoitui neljä ja lisäksi tutkimuksia on haettu manuaalisesti artikkeleiden lähdeluetteloiden ja esiin tulevien käsitteiden avulla Google Scholar-palvelun kautta, joista löytyi myös neljä. Niin sanottua harmaata kirjallisuutta, jota ei löydy haulla tietokannoista etsitään tutkimalla artikkeleiden lähdeluetteloja ja viitteitä (Malmivaara 2008, 273; Vilkka 2023, 33). Tutkimuksessa käytetyt tietokannat ja hakusanat löytyvät tutkimuksen liitteissä (Liite 1).

Hakulausekkeeksi muodostettiin ”cyber security*” OR ”digital attact*” OR “digital skills*” OR “cyber security breach*” OR “data breach*” OR “malware*” OR “phishing*” AND “nurse*” OR “health care staff*” OR “medical staff” OR “health care professionals*” OR “hospital staff” AND “remote work*” OR “digital healthcare*” OR “telework*” OR “telemedicine*” OR “e-health*”.

Taulukko 1. Hakustrategia

”cyber security” OR ”digital skill*” OR ”patient data*” OR “digital attack*” OR “malware*” OR “phissing” OR “cyber security breach*” OR “data breach*” OR “kyberturva*” OR “digitaaliset taidot” OR “digitai*” OR “potilastie*” OR “tietoturva*” OR “tietomur*” OR “digihyökkäys” OR “tieto* kalastelu* OR “haittaohjelma*”
AND
”nurse*” OR ”healthcare professional*” OR ”healthcare staff*” OR “medical staff*” OR “hospital staff*” OR “hospital worker*” OR “essential worker*” OR “sairaanhoita*” OR “hoitohenkilökun*” OR “hoitohenkilöstö*” OR “terveydenhuollon ammatti*”
AND
”remote work*” OR ”digital health*” OR ”telework*” OR “telemedicine*” OR “digital tool*” OR “e-work*” OR “e-health*” OR “etätyö*” OR “etähoi*” OR ”digihoi*” OR “digitaalinen terveydenhuol*” OR “digitervey*” OR ”digiklinik*”

Hakustrategian etenemisen aikana tarkasteltiin mukaanottokriteerien täyttymistä. Jos haulla tuli mukaan tutkimuksia, jotka eivät täyttäneet mukaanottokriteereitä, se hylättiin. (Taulukko 2)

Taulukko 2. Mukaanotto- ja poissulkukriteerit

MUKAANOTTO	POISSULKU
- 1/2021 jälkeen julkaistut artikkelit - abstrakti ja kokoteksti saatavilla - artikkeli kuvailee etätyötä tekevien sairaanhoitajien kyberturvallisuustaitoja - vertaisarvioidut artikkelit	- yli 4 vuotta aikaisemmin julkaistut artikkelit - maksumuurin takana olevat - artikkeli ei ole saavutettavissa JAMK:n tietokannoista - artikkeli kuvailee terveydenhuollon kyberuhkia

Kirjallisuuskatsaukseen valittiin kahdeksan (8) artikkelia (liite 2).

10.3 Aineiston laadunarviointi

Malmivaara (2008) on esittänyt, että kirjallisuuskatsaukseen mukaan otettavien tutkimusten laadun arviointi on välttämätön osa systemaattista katsausta. Ainoastaan siten voidaan arvioida tutkimukseen sisältyvän harhan todennäköisyyttä ja päästä mahdollisimman todenmukaisiin johtopäätöksiin tutkimustuloksista. Lemetti & Ylönen (2016, 68) on artikkelissaan tiivistänyt useasta eri lähteestä, että arviointikriteerien käyttäminen on suositeltavaa tutkimusten raportoinnissa, sillä se lisää tutkimuksen luotettavuutta sekä auttaa lukijaa ymmärtämään paremmin raportoidun tutkimuksen asetelmaa, toteuttamista, analyysia ja tuloksia. Tutkimusartikkeleiden arvioinnissa huomio tulee olla pätevyydessä eli validiteetissa, kliinisessä merkittävyydessä sekä yleistettävyydessä (Booth ym. 2016, 151-155; Vilkka 2023, 93). Kaikissa lähdemateriaaleissa suositellaan vähintään kahta tutkijaa tekemään tutkimusten valintaprosessia ja laadunarviointia, mikä lisää laadunarvioinnin luotettavuutta, mutta tämä ei opinnäytetyössä ole mahdollista (Stolt ym. 2016, Vilkka 2023, Booth ym. 2016). Luotettavuuden arviointiin on olemassa useita tarkistuslistoja, tässä kirjallisuuskatsauksessa käytettiin apuna Joanna Briggs Instituutin kehittämää CASP Systematic Review Checklist- tarkistuslistaa (JBI 2014). Tätä tarkistuslistaa käytetään järjestelmällisen katsauksen metodologisen laadun arviointiin ja siihen sisältyy yhteensä yksitoista arviointikriteeriä. Tämä auttaa aloittavaa tutkijaa arvioimaan aineiston pätevyyttä, tuloksia ja merkitystä sekä sen sisällyttämistä katsaukseen (CASP, 2013). Kaikki tutkimukseen valikoituneet artikkelit olivat vertaisarvioituja, joten tutkijan tehtävä oli tarkastella kriittisesti, vastasiko artikkeli tutkimuskysymykseen.

10.4 Sisällönanalyysi

Aineisto analysoitiin induktiivisella eli aineistosta lähtevänä sisällönanalyysillä. Sisällönanalyysia voidaan käyttää tiedon tiivistämiseen ja jäsentämiseen auttamalla teemojen, mallien ja suhteiden vertailua ja tämä edistää katsauksen synteesiprosessia (Tuomi ym. 2018, 124). Sisällönanalyysi koostuu kolmesta vaiheesta, joita ovat valmistelu, organisointi ja raportointi. Aineiston järjestämisvaiheessa selvitetään tutkimuksen aihe, teoria, menetelmä, tavoite ja mahdollinen muuttuja. Toisessa vaiheessa tehdään induktiivinen analyysi eli edetään aineistosta löytyneistä ja tutkimuskysymyksen kannalta olennaisista havainnoista tuloksiin ja päätelmiin. Kolmannessa vaiheessa analyysi ja tulokset kuvataan ja havainnollistetaan kirjallisesti niin, että tämä on toistettavissa. (Elo, Kajula, Tohmola, Kääriäinen 2022, 217-218; Vilkka 2023, 87)

Sisällönanalyysi aloitetaan analyysiyksikön valinnalla, joka tässä tutkimuksessa oli tutkimustulosten esittämä löydös. Tutkimusten tulokset käytiin läpi ja tiivistettiin ydinsisältö, joista pelkistettiin olennaiset asiat. Samankaltaiset ilmaisut ryhmiteltiin yhteen ja ne muodostivat alakategorioita. Yhdistämällä alakategorioita saatiin esiin teemoja, joista tehtiin yläkategorioita. Tulosten yhteys alkuperäisaineistoon esitettiin autenttisilla lainauksilla, joka vahvistaa tutkimuksen luotettavuutta (Elo ym. 2022, 220, 223; Tuomi ym. 2018, 108-113). Näistä muodostui asenteet ja käyttäytyminen, digitaalisten taitojen merkitys, organisaation ja johdon rooli, etätyön vaikutus sekä koulutuksen ja teknologian saatavuuden vaikutus. Sisällönanalyysi esitetään tutkimuksen liitteissä (liite 3).

11 Tulokset

11.1 Asenteet ja käyttäytyminen kyberturvallisuudessa

Tutkimus korostaa, että ihmisten käyttäytymisen ymmärtäminen on keskeistä tehokkaan kyberturvallisuusstrategian kehittämisessä. Tutkimuksessa tunnistettiin neljä erilaista riskiprofiilia, jotka kuvaavat yksilöiden tietoisuutta ja suhtautumista kyberuhkiin. Nämä profiilit korostavat, että pelkkä tietoisuus kyberuhista ei aina johda turvalliseen käyttäytymiseen; yksilön asenteet ja motivaatiot vaikuttavat merkittävästi heidän toimintaansa (Przymus, Malagocka, Przybyszewaki 2024, 1441, 1442).

Tutkimus osoittaa, että terveydenhuollon ammattilaisten asenteet mHealth-teknologiaa kohtaan ovat suhteellisen alhaisia Lounais-Etiopiassa. Asenteisiin vaikuttavat merkittävästi koulutustaso, tietoisuus teknologiasta, työkokemus, ICT-infrastruktuurin saatavuus, älypuhelimen omistaminen ja tietokonekoulutus. Nämä tekijät tulisi ottaa huomioon suunniteltaessa ja toteutettaessa mHealth-teknologian käyttöönottoa resurssirajoitteisissa ympäristöissä (Walle, Butta, Kassie, Chereka, Kanfe, Dubale, Enyew, Dube, Shibabaw, Hunde, Kitil, Ferede, Wubante, Baykemagn, Demsash 2024, 7). Myös Jarva ym. 2021 tutkimuksessa on tunnistettu positiivisen asenteiden lisääntyvän, kun digitaaliset taidot kehittyvät (Jarva, Oikarinen, Andersson, Tuomikoski, Kääriäinen, Meriläinen, Mikkonen 2021, 1391).

11.2 Digitaalisten taitojen merkitys kyberturvallisuudelle

Tutkimuksissa tulee esiin, että digitaalinen terveysosaaminen on monimuotoinen kokonaisuus, joka kattaa tekniset taidot, potilaslähtöisyyden sekä kyvyn yhdistää digitaalisia ja perinteisiä hoitomenetelmiä. Tutkimus osoittaa, että digitaalinen terveysosaaminen ei rajoitu pelkästään teknisiin taitoihin, vaan se sisältää myös kyvyn arvioida digitaalisten ratkaisujen soveltuvuutta potilaan tarpeisiin ja yhdistää niitä perinteisiin hoitomenetelmiin. Ammattilaisten kokemukset ja näkemykset korostavat tarvetta jatkuvalle koulutukselle ja tuelle digitaalisten taitojen kehittämisessä (Jarva ym. 2021, 1391).

Jarva ym. 2021 tutkimuksessa tuodaan ilmi aikaisemman työkokemuksen tuoma hyöty ja varmuus käytettäessä uusia/digitaalisia työvälineitä (Jarva ym. 2021; 1387, 1389). Digitaalinen potilasohjaus koettiin edelleen haastavana mm. heikkojen internet-yhteyksien ulkoisten häiriöiden ja kyvyttömyyden käyttää kehonkieltä. Taustatekijät (ikä, sukupuoli, työkokemus, kulttuuri) ovat tunnistettu merkittäviksi tekijöiksi kaikissa tutkimuksissa.

11.3 Organisaation ja johdon rooli

Tutkimus osoittaa, että vaikka suurin osa hoitohenkilöstöstä kokee osaamisensa riittäväksi, on olemassa merkittäviä puutteita erityisesti tietoturvakäytännöissä ja toimintatavoissa. Erityistä huomiota tulisi kiinnittää koulutukseen ja ohjeistukseen, jotta voidaan varmistaa potilastietojen turvallinen käsittely ja suojata terveydenhuollon järjestelmiä kyberuhkilta. (Blek, Solankallio-Vahteri 2022, 361).

Tutkimus korostaa, että organisaatioiden on tärkeää investoida kyberturvatoimiin ja koulutukseen, erityisesti etätyön yleistyessä. Työntekijöiden kyberhygienia ei ole pelkästään yksilön vastuulla, vaan siihen vaikuttavat merkittävästi organisaation tarjoamat resurssit ja ohjeistukset. Lainsäätäjien ja viranomaisten tulisi huomioida nämä tekijät kehittäessään strategioita etätyön turvallisuuden parantamiseksi (Karayel, Aktas, Akbiyik 2024; 101). Vertailut eri toimialojen välillä osoittavat, että terveydenhuoltoalan henkilöstöllä on yksi matalimmista kyberturvallisuushygienian tasoista. Erot julkisella ja yksityisellä sektorilla ovat merkittävät (Karayel ym. 2024; 106).

Tutkimus korostaa, että kyberturvallisuus ei ole pelkästään etätyön haaste, vaan myös sen mahdollistaja. Organisaatioiden tulisi kehittää kyberturvastrategioitaan tukemaan etätyötä ja hyödyntää pandemia-aikana opittuja käytäntöjä tulevaisuuden työmuotojen suunnittelussa. (Bisham, Creese, Dutton, Esteve, Gonzalez, Goldsmith 2022, 382). Organisaation tieto- ja kyberturvallisuudesta vastuussa olevan teknisen henkilöstön ja hoitohenkilöstön välistä vuorovaikutusta on tärkeää vahvistaa ja kehittää. Tämä varmistaa, että käyttöön otettavat tietoturvaohjeet ja toimintamallit tukevat arjen hoitotyötä mahdollisimman hyvin ja ovat selkeästi perusteltuja (Blek ym. 2022, 360).

11.4 Etätyön vaikutus turvallisuuskäytäntöihin

Tutkimuksessa on todettu, että kyberturvallisuus ei heikennä tehokasta työskentelyä kotona (Bisham ym. 2022, 382). Tutkimuksen tulokset osoittavat, että etätyö voi lisätä työntekijöiden kyberturvatietoisuutta ja turvallisuustoimenpiteiden toteuttamista. Etätyön on positiivisesti yhteydessä kyberturvatietoisuuteen ja turvallisuustoimenpiteiden toteuttamiseen siten, että kyberturvapolitiikan noudattaminen vahvistaa etätyön vaikutusta kyberturvatietoisuuteen ja kasvava kyberturvatietoisuus johtaa todennäköisemmin turvallisuustoimenpiteiden toteuttamiseen. Tutkimus korostaa, että etätyö voi edistää kyberturvallisuutta lisäämällä työntekijöiden tietoisuutta ja vastuullisuutta. Organisaatioiden tulisi tukea tätä kehitystä tarjoamalla selkeää kyberturvapolitiikkaa ja koulutusta. (Nwankpa, Datta, 2023, 8, 11; Bisham ym. 2022, 383).

12 Pohdinta

12.1 Tulosten tarkastelu

Etätyötä tekevien sairaanhoitajien kyberturvataidoista on toistaiseksi vähän suoraa tutkimusta, mutta aihetta sivuavia selvityksiä on tehty erityisesti hoitohenkilöstön yleisestä kyberturvallisuusosaamisesta. Olemassa olevat selvitykset viittaavat siihen, että kyberturvallisuusosaamisessa on puutteita ja että etätyötä tekevien hoitohenkilöstön tieto- ja kyberturvataidot muodostuvat monen tekijän yhteisvaikutuksesta. Etätyön lisääntyessä on tärkeää kehittää koulutusta ja ohjeistusta, jotka tukevat turvallista työskentelyä myös etäympäristöissä. Kyberturvallisuustaidot eivät riipu pelkästään tietoisuudesta vaan myös asenteista ja organisaatiokulttuurista. Toimialakohtaiset erot ovat merkittäviä. Tutkimukset osoittavat, että terveydenhuoltoalalla kyberturvallisuushygienian taso on heikompi verrattuna esimerkiksi puolustus-, IT- ja rahoitusaloihin. Tämä korostaa terveydenhuollon toimialan erityistarvetta kohdistaa resursseja ja huomiota henkilöstön kyberturvallisuustaitojen parantamiseen.

Kyberturvataidot eivät ole pelkästään tekninen kysymys, vaan liittyvät vahvasti asenteisiin, osaamiseen ja organisaation tukeen. Kyberturvallisuustietoisuus ja käytännön toiminta eivät aina kohtaa. Vaikka hoitohenkilöstöllä voi olla hyvä tietoisuus kyberturvallisuusriskeistä, tieto ei automaattisesti johda turvallisiin toimintatapoihin. Tämä korostaa tarvetta yhdistää tietoisuus konkreettisiin taitoihin ja käytännön harjoitteluun. Digiosaaminen on keskeinen edellytys turvalliselle työskentelylle. Vahvat digitaidot tukevat paitsi teknologian sujuvaa hyödyntämistä myös turvallisten toimintatapojen omaksumista. Puutteellinen digiosaaminen voi altistaa virheille, mikä lisää kyberriskejä. Erityisesti teknologian nopea kehitys edellyttää jatkuvaa osaamisen päivittämistä.

Etätyö tuo mukanaan uusia riskejä, joihin ei aina ole varauduttu koulutuksen tai ohjeistuksen kautta. Etätyö lisää tietoturvahaavoittuvaisuuksia. Etätyöympäristössä fyysisen valvonnan ja teknisen tuen puute altistaa työntekijät uusille riskeille. Kotiverkkojen suojaus ja omien laitteiden käyttö tuovat lisähaasteita, joita ei aina ole huomioitu organisaatioiden tietoturvastrategioissa. Organisaation rooli on ratkaiseva kyberturvallisuuden tukemisessa. Toisin kuin aiemmissa tutkimuksissa, etätyö saattaa vaikuttaa myös myönteisesti tutkittavien kyberturvataitoihin. Tämä olisi tärkeää tiedostaa koulutuksia suunniteltaessa.

Organisaation tuki ja kyberturvallisuuskulttuuri voivat mahdollistaa tai estää turvalliset käytännöt. Organisaatiot eivät aina panosta riittävästi säännölliseen testaamiseen, päivittämiseen ja varmuuskopiointiin. Myös koulutuksen ja tietoisuuden lisäämisen osalta on puutteita. Erityisen tärkeää on kehittää johdon ja teknisen tuen sekä hoitohenkilöstön välistä vuoropuhelua, jotta tietoturvaohjeet tukevat käytännön työtä ja ovat helposti ymmärrettäviä. Teknologian saatavuus on myös ratkaiseva tekijä digitaalisen terveyden kehittämisessä.

Koulutuksen rooli on keskeinen – se vaikuttaa sekä osaamiseen että asenteisiin. Koulutus ja osaamisvaatimukset kaipaavat systemaattista kehittämistä. Tieto- ja kyberturvallisuusosaamisen kehittäminen tulisi integroida tiiviimmin osaksi hoitotyön koulutuspolkuja ja työelämän jatkuvaa oppimista. Terveysalan opetussuunnitelmat tarvitsevat päivitystä, jotta ne vastaavat paremmin digitaalisen terveyden ja kyberturvallisuuden vaatimuksiin (Blek ym. 2022, 360.)

12.2 Tutkimuksen eettisyys ja luotettavuus

Tässä integroivassa kirjallisuuskatsauksessa luotettavuutta on pyritty vahvistamaan avoimella ja systemaattisella aineistonhaulla. Hakuprosessi, tietokannat, hakusanat ja valintakriteerit on pyritty kuvaamaan mahdollisimman selkeästi. Työskennellessä on noudatettu Tutkimuseettisen neuvottelukunnan ohjetta (2012). Tiedonhaussa on ollut asiantuntijana kirjaston informaatikko, mikä on lisännyt luotettavuutta (Niela-Vilen, Hamari 2016, 26). Lähteiden valinnassa on painotettu tieteellistä laatua ja ajankohtaisuutta ja analyysi on toteutettu sisällönanalyysin keinoin.

Katsauksen teoreettinen viitekehys on ohjannut aineiston tulkintaa ja auttanut jäsentämään ilmiötä syvällisemmin. Läpinäkyvyyttä on vahvistettu tekemällä muistiinpanoja joka vaiheessa ja palaamalla niihin (Vilkka 2023, 80). Tutkimuksen lähdemateriaali valittiin tieteellisin perustein; ne olivat ajantasaisia ja kuvattiin, millä kriteereillä lähteet valittiin ja suljettiin pois. Luotettavuutta vahvistavana tekijänä on CASP-tarkistuslista. Sisällön analyysi valittiin aineiston analyysitavaksi, jotta tulokset olisivat mahdollisimman läpinäkyvät, selkeät ja perustellut. Cronin ja Georgen mukaan (2022, 186) integratiivinen kirjallisuuskatsaus soveltuu erityisen hyvin, jos tutkittava ilmiö on monimutkainen ja siihen liittyvä tutkimustieto on hajanaista, kuten tässä esim. kyberturva ja hoitotyö etätyössä.

Lähteiden metodologista laatua ja relevanssia arvioitiin kriittisesti. Hakuprosessin avoimuuden varmistamiseksi hakustrategia, käytetyt tietokannat, hakusanat ja rajaukset pyrittiin kuvaamaan mahdollisimman tarkasti, jotta tutkimus on mahdollista toistaa (Lemetti, Ylönen 2016, 75). Johtuen resursseista lähteiden analysointi on tehty itsenäisesti yhden aloittelevan tutkijan voimin ja mukaan otettu suomen- sekä englanninkielisiä, Jyväskylän ammattikorkeakoulun tunnuksilla saavutettavissa olevaa materiaalia, nämä huomioitu tutkimuksen luotettavuutta heikentävinä tekijöinä. (Salminen 2011, 33). Kirjallisuuskatsauksen toteutukseen vaikuttavat olennaisesti käytettävissä oleva aika ja tutkijoiden määrä, sillä ne ohjaavat prosessin etenemistä, tehtyjä valintoja sekä tiedonhaun kattavuutta ja tarkkuutta (Elo ym. 2022, 223). Ajan rajallisuus heijastuu erityisesti systemaattiseen tiedonhakuun, analyysivaiheeseen ja laadunarviointiin, jotka voivat jäädä pinnallisemmiksi. Tämän vuoksi katsauksen läpinäkyvyyden varmistamiseksi on tärkeää, että tutkija tuo esiin, mitä hän on ehtinyt toteuttaa annetussa aikarajassa ja missä määrin se on voinut vaikuttaa lopputulokseen (Vilkka 2023, 104).

Tutkija on huomioinut joka vaiheessa objektiivisuuden ja kriittisyyden tunnistaen omat ennakko-oletuksensa ja pysynyt mahdollisimman puolueettomana. Tämä sisältää myös kriittisen tarkastelun lähteiden laadusta, metodologisista rajoituksista ja mahdollisista julkaisuharhaa muodostavista tekijöistä (Vilkka 2023, 94, 99). Integroiva lähestymistapa on mahdollistanut monipuolisen kuvan muodostamisen ilmiöstä ja tarjoaa arvokasta pohjaa jatkotutkimukselle sekä käytännön kehittämistyölle. Sen avulla voidaan tunnistaa, mihin asioihin tutkimuksella ei vielä ole vastattu aiheessa ja sen tieteellisessä keskustelussa (Cronin ym. 2023, 168; Vilkka 2023, 25).

Eettisesti katsaus perustuu aiemmin julkaistuihin tutkimuksiin ja katsauksessa käytetyt aineistot ovat julkisesti saatavilla olevia, joten tutkimuslupaa ei tarvittu. Tutkimuksen toteuttamisessa on noudatettu vastuullisuutta; kaikki lähteet on esitetty asianmukaisesti, aineiston ja tutkimustulosten raportointi on rehellistä, avointa ja puolueetonta (Tuomi ym. 2018, 150). Tulkinnassa on huomioitu tutkijan rooli ja kontekstien vaikutus tutkimusten yleistettävyyteen. Tarkoituksena on ollut tuottaa luotettavaa ja kunnioittavaa tietoa ilmiöstä ilman yleistämistä tai leimaamista virheellisesti (Tutkimuseettinen Neuvottelukunta TENK 2023).

12.3 Johtopäätökset ja jatkotutkimuskysymykset

Tutkimus osoittaa, että vain pieni osa julkisen ja yksityisen sektorin organisaatioista on ryhtynyt hitaasti riittäviin toimiin testatakseen, analysoidakseen, skannatakseen, päivittääkseen, ylläpitääkseen ja varmuuskopioidakseen tietoverkkoja, laitteistoa, ohjelmistoja, viestintävälineitä ja tallennuslaitteita säännöllisesti. Lisäksi ne eivät ole olleet riittäviä työntekijöidensä kyberturvallisuushygienian parantamiseen liittyvässä koulutuksessa ja tietoisuuden lisäämisessä. Tämän vuoksi organisaatiot kohtaavat usein tietoturvaloukkauksia, koska ne eivät pysty ottamaan, suunnittelemaan ja rahoittamaan kyberturvallisuustoimia etätyöskentelyn tueksi. (Bisham ym. 2022,377.)

Tutkimus korostaa tarvetta räätälöidylle koulutukselle ja tuelle eri tasoisen informatiikkaosaamisen omaaville hoitajille. Tämä voi parantaa tietojärjestelmien hyödyntämistä ja edistää hoidon laatua (Kaihlanen, Elovainio, Virtanen, Kinnunen, Vehko, Saranto, Heponiemi 2023, 4027, 4030). Ammattiin valmistuvien sekä työssä olevien hoitohenkilöstön tieto- ja kyberturvallisuusosaamista tulee kehittää jatkuvasti. Osaamisen kehittämisen ja ylläpidon tulisi perustua selkeästi määriteltyihin osaamisvaatimuksiin. On myös tärkeää, että terveysalan opetussuunnitelmat päivitetään ottaen huomioon tieto- ja kyberturvallisuusosaamisen tarpeet (Blek ym. 2022).

Tietoisuus, osaaminen, koulutus ja organisaation tuki muodostavat yhdessä turvallisen toimintaympäristön. Etätyön lisääntyessä on välttämätöntä päivittää käytännöt, ohjeistukset ja osaamisvaatimukset vastaamaan uusia uhkakuvia. Etätyötä tekevien hoitohenkilöstön kyberturvallisuusosaaminen edellyttää sekä teknistä taitoa että tietoisuuden ja käytännön toiminnan vahvistamista. Digiosaamisen puutteet ja etätyön erityiset haavoittuvuudet korostavat tarvetta jatkuvalle koulutukselle ja selkeille toimintamalleille. Organisaation tuki, kuten johdon ja teknisen henkilöstön välinen vuoropuhelu sekä tietoturvakäytäntöjen käytännönläheisyys, ovat keskeisiä turvallisen arjen varmistamisessa. Terveysalan opetussuunnitelmien ja työelämän osaamisvaatimusten ajantasaistaminen on välttämätöntä, jotta kyberturvallisuusosaaminen kehittyy vastaamaan muuttuvia digitaalisia riskejä. Lisäksi terveydenhuoltoala tarvitsee erityishuomiota, koska sen kyberturvallisuushygienian taso on todettu heikommaksi verrattuna muihin toimialoihin.

Tämän katsauksen tarkoitukseksi muodostui tunnistaa ja yhdistää aiempaa tutkimustietoa, luoden uutta kokonaisvaltaista ymmärrystä etätyötä tekevien sairaanhoitajien kyberturvataidoista – ai-

heesta, joka on monitieteinen ja hajanaisesti tutkittu (Cronin ym. 2023, 186). Tutkimuksen yhteydessä todettiin selkeä lisätutkimuksen tarve. Etätyötä tekevien hoitohenkilöstön kyberturvallisuusosaaminen edellyttää sekä teknistä taitoa että tietoisuuden ja käytännön toiminnan vahvistamista. Digiosaamisen puutteet ja etätyön erityiset haavoittuvuudet korostavat tarvetta jatkuvalle koulutukselle ja selkeille, käytännönläheisille toimintamalleille. Organisaation tuki ja johdon sekä teknisen henkilöstön välinen vuorovaikutus ovat keskeisiä turvallisen työskentelyn varmistamisessa. Terveysalan opetussuunnitelmien ja työelämän osaamisvaatimusten päivittäminen on välttämätöntä, jotta kyberturvallisuusosaaminen vastaisi muuttuvia digitaalisia riskejä. Koska tutkimustietoa erityisesti hoitohenkilöstön kyberturvataidoista etätyöolosuhteissa on vielä niukasti, tarvitaan jatkossa lisää tutkimusta, joka selvittää tehokkaita koulutusmuotoja ja organisaatiokäytäntöjä kyberturvallisuuden parantamiseksi. Etätyötä tekevien sairaanhoitajien näkökulman saaminen kuuluviin on tärkeää, jotta koulutuksen ja organisaatioiden kehittäminen olisi mahdollisimman tehokasta, johdonmukaista ja kestävän kehityksen mukaista.

Lähteet

Aaltola, K. – Ruoslahti, H. – Heinonen, J. 2022. Desired cybersecurity skills and skills acquisition methods in the organizations. Jyväskylän yliopisto. European Conference on Cyber Warfare and Security. Viitattu 29.8.2023. https://jyx.jyu.fi/bitstream/handle/123456789/81832/Aalto-laym.pdf?sequence=1&isAllowed=y

Ahonen, O. – Kinnunen, U-M. – Kouri, P. – Liljamo, P. – Saranto, K. 2016. Sähköisten terveyspalvelujen strategia hoitotyöhön – nyt on sen implementoinnin aika. Finnish Journal of eHealth and eWelfare 2016; 8(4), 231-233. viitattu 12.6.2023. file:///C:/Users/LEHTOPA4/Downloads/60200-Article%20Text-64022-1-10-20161209.pdf

Alder, S. 2024. Healthcare Data Breaches Due to Phishing. Lähetetty 6.1.2024. HIPAA Journal. Viitattu 25.2.2025. https://www.hipaajournal.com/healthcare-data-breaches-due-to-phishing/

Argaw, S.T. – Troncoso-Pastoriza, J.R. – Lacey, D. – Florin, M-V. – Calcavecchia, F. – Anderson, D. – Burleson, W. – Vogel, J-M. – O`Leary, C. – Eshaya-Chauvin, B. – Flahault, A. 2020. Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. BMC Medical Informatics and Decision Making (2020) 20:146. Viitattu 2.6.2023. file:///C:/Users/LEHTOPA4/Downloads/s12911-020-01161-7%20(2).pdf

Bispham, M. – Creese, S. – Dutton, W.H. – Esteve-Gonzalez, P. – Goldsmith, M. 2021. An Exploratory Study of Cybersecurity in Working from Home: Problem or Enabler? Journal of Information Policy (2022) 12: 353–386. viitattu 1.4.2025. https://scholarlypublishingcollective.org/psup/information-policy/article/doi/10.5325/jinfopoli.12.2022.0010/320386/An-Exploratory-Study-of-Cybersecurity-in-Working

Blek, T. -Solankallio-Vahteri, T. 2022. Terveydenhuollon hoitohenkilöstön tieto- ja kyberturvallisuusosaaminen. Finnish Journal of eHealth and eWelfare 2022;14(4). 115829-Article Text-262609-1-10-20221223.pdf

Booth, A. – Sutton, A. – Clowes, M. – Martyn-St James, M. 2016. Systematic Approaches to a Successful Literature Review. Second edition. Lontoo: Sage. Viitattu 18.2.2025. https://www.researchgate.net/profile/Andrew-Booth-2/publication/235930866_Systematic_Approaches_to_a_Successful_Literature_Review/links/5da06c7f45851553ff8705fa/Systematic-Approaches-to-a-Successful-Literature-Review.pdf

Critical Appraisal Skills Program (CASP) 2018. CASP-tarkistuslistat. Viitattu 26.3.2025. https://casp-uk.net/casp-checklists/CASP-Systematic-Review-checklist_2022.pdf

Cronin, M.A. – George, E. 2023. The Why and How of the Integrative Review. Organizational Research Methods, Vol. 26(1), 168-192. Viitattu 13.4.2025.

Elo, S. – Kajula, O. – Tohmola, A. – Kääriäinen, M. 2022. Laadullisen sisällönanalyysin vaiheet ja eteneminen. Hoitotiede 2022, 34 (4), 215-225. viitattu 28.2.2025. https://journal.fi/hoitotiede/article/view/128987/78028

Euroopan yhteisöjen komissio 2008. Komission tiedonanto Euroopan parlamentille, neuvostolle, Euroopan talous- ja sosiaalikomitealle ja alueiden komitealle potilaita, terveydenhuoltojärjestelmiä ja yhteiskuntaa hyödyttävästä telelääketieteestä. Julkaistu 4.11.2008. Viitattu 20.2.2025. https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX%3A52008DC0689

Finlex nd. Henkilötietolaki. Viitattu 22.8.2023. https://finlex.fi/fi/laki/ajantasa/kumotut/1999/19990523

Furnell, S. – Shah, JN 2020. Home working and cyber security – an outbreak of unpreparedness? Computer Fraud & Security 2020 (8): 6-12. Viitattu 19.5.2023. Home working and cyber security â€“ an outbreak of unpreparedness? (sciencedirectassets.com)

Giansanti, D. 2020. Cybersecurity and the Digital-Health: The Challenge of This Millenium. Healthcare. viitattu 1.2.2022 file:///C:/Users/LEHTOPA4/Downloads/Cybersecurity_and_the_Digital-Health_The_Challenge.pdf

He, Y. – Aliyu, A. – Evans, M. – Luo, C. 2021. Health Care Cybersecurity Challenges and Solution Under the Climate of COVID-19: Scoping Review. Journal of Medical Internet Research 23(4). viitattu 12.5.2023. https://jmir.org/2021/4/e21747

Heinonen T. – Lindfors, P. - Nygård, C-H. 2022. Etäkotihoitotyön sisältö ja kuormittavuus sekä mahdollisuudet työurien pidentäjänä. Gerontologia. 36(2), s. 128-142. Artikkelit. Viitattu 9.1.2025. https://cris.tuni.fi/ws/portalfiles/portal/65910430/109921_Artikkelin_teksti_238537_1_10_20220608.pdf

Herukka, A. – Tuohimaa, T. – Kiviniemi, L. – Koivunen, K. 2021. Terveydenhuollon ammattilaiset sähköisten palveluiden käyttäjinä ja kehittäjinä. ePooki 13/2021. Oulun ammattikorkeakoulun tutkimus ja kehitystyön julkaisut issn 1798-2022. Viitattu 28.8.2023. https://www.oamk.fi/epooki/2021/terveydenhuollon-ammattilaiset-sahkoisten-palveluiden-kayttajina-ja-kehittajina/

Heponiemi, T. – Jormanainen, V. – Leemann, L. – Manderbacka, K. – Aalto, A-M. – Hyppönen, H. 2020. Digital Divide in Perceived Benefits of Online Health Care and Social Welfare Services: National Cross-Sectional Survey Study. Journal of Medical Internet Research 2020; 22(7): e17616. Viitattu 3.6.2023. https://www.jmir.org/2020/7/e17616/PDF

ISO (the International Organization for Standardization). viitattu 7.1.2025. https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-3:v1:en

Jarva, E. – Oikarinen, A. – Andersson, J. – Tuomikoski, A-M. – Kääriäinen, M. – Meriläinen, M. – Mikkonen, K. 2022. Healthcare professionals' perceptions of digital health competence: A qualitative descriptive study. Nursing Open 2022;9:1379-1393. Viitattu 2.4.2024. https://onlinelibrary.wiley.com/doi/epdf/10.1002/nop2.1184

JYVSECTEC 2021. Kyberhäiriöiden hallinta. Käsikirja terveydenhuollon toimijoille. JYVSECTED by Jamk. https://jyvsectec.fi/wp-content/uploads/2020/12/kyberhairioiden-hallinta-kasikirja-terveydenhuollon-toimijoille.pdf

Kaihlanen, A-M. - Gluschkoff, K. – Laukka, E. – Heponiemi, T. 2021. The information system stress, informatics competence and well-being of newly graduated and experienced nurses: a cross-sectional study. BCM Health Services Research 21(1), 1-8. Viitattu 1.10.2022. https://pubmed.ncbi.nlm.nih.gov/34654427/

Kaihlanen, A-M. – Elovainio, M. – Virtanen, L. – Kinnunen, U-M. – Vehko, T. – Saranto, K. – Heponiemi, T. 2023. Nursing informatics competence profiles and perceptions of health information system usefulness among registered nurses: A latent profile analysis. Journal of Advanced Nursing 2023; 79: 4022-4033. Viitattu 1.4.2025. https://onlinelibrary.wiley.com/doi/epdf/10.1111/jan.15718

Karayel, T. - Aktaş, B. - Akbıyı, A. 2024. Human factors in remote work: examining cyber hygiene practices. Information and Computer Security Vol. 33 No. 1, pp. 96-116. Viitattu 3.4.2025. https://www-emerald-com.ezproxy.jamk.fi:2443/insight/content/doi/10.1108/ics-11-2023-0215/full/pdf?title=human-factors-in-remote-work-examining-cyber-hygiene-practices

Kautto M. - Koskela T. - Kulmala P.- Tuovinen, T. - Reponen, J. 2024. Digi- ja etälääketieteen osaaminen – tietoa, taitoa ja soveltavaa osaamista. Duodecim Teema 2024;140:1984–9. Viitattu 20.2.2025. https://www.duodecimlehti.fi/xmedia/duo/duo18552.pdf

Khairat, S. – Coleman, C. – Newlin, T. – Rand, V. – Ottmar, P. – Bice, T. – Carson, S.S. 2019. A mixed-methods evaluation framework for electronic health records usability studies. Journal of Biomedical Informatics, Volume 94, June 2019, 103175. Viitattu 10.5.2025. https://doi.org/10.1016/j.jbi.2019.103175

Kovalainen, A. – Poutanen, S. – Arvonen, J. 2021. Covid-19, luottamus ja digitalisaatio. Tutkimus etätyöstä ja sen järjestymisestä Suomessa keväällä ja syksyllä 2020. Tutkimusraportti. Turun yliopisto. Turun työtieteiden keskus TCLS, Johtamisen ja yrittäjyyden laitos, Turun kauppakorkeakoulu, Turun yliopisto. Viitattu 19.9.2022. Tutkimusraportti2021. Covid-19, luottamus ja digitalisaatio. Tutkimus etätyöstä ja sen järjestymisestä Suomessa keväällä ja syksyllä 2020.pdf (utu.fi)

Kruse, S.C. – Frederick, B. – Jacobson, T. – Monticone, K. 2017. Cybersecurity in Healthcare: A systematic review of modern threats and trends. Technology and Healthcare 25(2017) 1-10. Viitattu 3.1.2025. https://journals.sagepub.com/doi/epdf/10.3233/THC-161263

Kyberturvallisuuskeskus 2020. Kyberturvallisuus ja yrityksen hallituksen vastuu. Kyberturvallisuuskeskuksen julkaisu. Julkaistu 4.2.2020. Viitattu 1.5.2025. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/T_KyberHV_digiAUK_220120.pdf

Lehto, M. – Pöyhönen, J. – Lehto, M. 2019. Kyberturvallisuus sosiaali- ja terveydenhuollossa. Loppuraportti vol. 2. Jyväskylän yliopisto. Viitattu 10.9.2022. Kyberturvallisuus sosiaali- ja terveydenhuollossa (jyu.fi)

Leksimi, S.A. 2022. Growing Concern on Healthcare Cyberattacks & Need for Cybersecurity. Viitattu 13.9.2022. https://www.researchgate.net/profile/Aarcha-Sunil-Lekshmi/publication/357753537_Growing_Concern_on_Healthcare_Cyberattacks_Need_for_Cybersecurity/links/61ded0425c0a257a6fe33ac8/Growing-Concern-on-Healthcare-Cyberattacks-Need-for-Cybersecurity.pdf

Lemetti, T. – Ylönen, M. 2016. Kirjallisuuskatsaukseen valittujen tutkimusartikkeleiden arviointi. Julkaisussa Kirjallisuuskatsaus hoitotieteessä. Toim. Stolt, M., Axelin, A., Suhonen, R. Turun Yliopisto. Hoitotieteen laitoksen julkaisuja, A: 73/2016, 23-34.

Malmivaara, A. 2008. Järjestelmällinen kirjallisuuskatsaus vaikuttavuudesta – Apuväline terveyden- ja sosiaalihuollon ammattilaisille, tutkijoille ja päättäjille. Sosiaalilääketieteellinen aikakauslehti 2008: 54, 273-278. Viitattu 21.3.2025. https://journal.fi/sla/article/view/1252/2401

Neittaanmäki, P. – Lehto, M. – Savonen, M. 2021. Yhteiskunnan digimurros. Jyväskylän yliopisto. Viitattu 14.9.2022. https://jyx.jyu.fi/bitstream/handle/123456789/75328/Yhteiskunnan%20digimurros.pdf?sequence=1&isAllowed=y

Niela-Vilen, H. – Hamari, L. 2016. Kirjallisuuskatsauksen vaiheet. Julkaisussa Kirjallisuuskatsaus hoitotieteessä. Toim. Stolt, M., Axelin A., Suhonen, R. Turun Yliopisto. Hoitotieteen laitoksen julkaisuja, A:73/2016, 23-34.

Norri-Sederholm, T. – Laitinen, T. – Lehto, M. – Kari, M.J. 2019. Terveydenhuolto ja kyberuhkat. FinJeHeW 2019;11(1-2), 86-99. 74183-Article Text-252233-1-10-20221024.pdf

Nwankpa, J.K. – Datta, P.M. 2023. Remote vigilance: The roles of cyber awareness and cybersecurity policies among remote workers. Computers & Security, volume 130. Viitattu 2.4.2025. https://doi.org/10.1016/j.cose.2023.103266

Obaid, O.I. – Salman, S.A-B. 2022. Security and Privacy in IoT-based Healthcare Systems: A Review. Mesopotamian journal of Computer Science, Vol. (2022), 2022, pp 29-40. viitattu 8.5.2025. https://www.researchgate.net/publication/369913866_Security_and_Privacy_in_IoT-based_Healthcare_Systems_A_Review

Przymus, Z. – Malagocka, K. – Przybyszewski, K. 2024. The human factor in cybersecurity: from risk profiles to resilience. Procedia Computer Science, Volume 246, 2024, 1437-1445. Viitattu 3.4.2025. https://doi.org/10.1016/j.procs.2024.09.587

Potilaille annettavat terveydenhuollon etäpalvelut. Valvira, Sosiaali- ja terveysalan lupa- ja valvontavirasto. Päivitetty 8.2.2022. Viitattu 1.6.2023. Potilaille annettavat terveydenhuollon etäpalvelut - Valvira

Ravelin, A. – Laukka, E. – Heponiemi, T. – Kaihlanen, A. – Kanste, O. 2021. Perusterveydenhuollon johtajien kokemuksia koronaviruspandemian vaikutuksista digitaaliseen työkulttuuriin ja sen johtamiseen. Sosiaalilääketieteellinen aikakauslehti 2021: 58: 220-234. Viitattu 1.6.2023. 103248-Kirjoitus (sisältäen ydinasiat,tiivistelmät & asiasanat)-208120-1-10-20210923.pdf

Richardson, S. – Lawrence, K. – Schoenthaler, A.M. – Mann, D. 2022. A framework for digital health equity. Digital Medicine. Viitattu 28.8.2023. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9387425/

Ristolainen, M. – Maijala, R. – Eloranta, S. Viestintä osana etäjohtamista terveydenhuollossa. FinJeHew 2020;12(3): 179-186. viitattu 3.6.2023. 95051-Article Text-252388-1-10-20221025.pdf

Salahdine, F. – Kaabouch, N. 2019. Social Engineering Attacks: A Survey. Future Internet 2019, 11, 89.Viitattu 12.6.2023. www.mdpi.com/journal/futureinternet

Salminen, A. 2011. Mikä kirjallisuuskatsaus? Johdatus kirjallisuuskatsauksen tyyppeihin ja hallintotieteellisiin sovelluksiin. Vaasan Yliopiston julkaisuja. Opetusjulkaisuja 62. Julkisjohtaminen 4. Vaasa 2011.

Suhonen, R. – Axelin, A. – Stolt, M. 2016. Erilaiset kirjallisuuskatsaukset. Julkaisussa Kirjallisuuskatsaus hoitotieteessä. Toim. M. Stolt & A. Axelin & R. Suhonen. Turku: Turun Yliopisto, 7-22. Hoitotieteen laitoksen julkaisuja, tutkimuksia ja raportteja 73/2016.

Sulosaari, V – Kajander-Unkuri, S. 2016. Integroitu kirjallisuuskatsaus. Julkaisussa Kirjallisuuskatsaus hoitotieteessä. Toim. M. Stolt & A. Axelin & R. Suhonen. Turku: Turun Yliopisto, 107-115. Hoitotieteen laitoksen julkaisuja, tutkimuksia ja raportteja 73/2016.

Sutela, H. – Pärnänen, A. – Keyriläinen, M. 2019. Digiajan työelämä. Työolotutkimuksen tuloksia 1977-2018. Tilastokeskus. Viitattu 25.9.2022. https://www.stat.fi/tup/julkaisut/tiedostot/julkaisuluettelo/ytym_1977-2018_2019_21473_net.pdf

Terveydenhuoltoalan kyberuhkia. Viestintävirasto, Kyberturvallisuuskeskus. 2016. Viitattu 26.5.2022. Terveydenhuoltoalan_kyberuhkia.pdf (kyberturvallisuuskeskus.fi)

Terveyden- ja hyvinvoinnin laitos. 2021. Terveydenhuollon etäasioinnin trendit vuosien 2013–2020 Avohilmon aineistossa. Tutkimuksesta tiiviisti 13/2021. Viitattu 23.9.2022. https://www.julkari.fi/bitstream/handle/10024/141162/URN_ISBN_978-952-343-639-8.pdf?sequence=1&isAllowed=y

Tietosuojavaltuutetun toimisto nd. EU:n tietosuoja-asetus. Viitattu 29.8.2023. https://tietosuoja.fi/gdpr

Tietosuojavaltuutetun toimisto nd. Mitä tietosuoja on? Viitattu 8.1.2025. https://tietosuoja.fi/tietosuoja

Tilastokeskus nd. Tietoa tilastoista. Käsitteet. viitattu 4.8.2023. https://www.stat.fi/meta/kas/index.html?E

Traficom, Liikenne ja viestintävirasto, Kyberturvallisuuskeskus. Haittaohjelmatartunnat ovat yhä yleisempiä. Päivitetty 12.7.2023. Viitattu 26.2.2025. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/haittaohjelmatartunnat-ovat-yha-yleisempia

Turvallisuuskomitea 2018. Kyberturvallisuuden sanasto. Viitattu 12.9.2022. https://turvallisuuskomitea.fi/wp-content/uploads/2018/06/Kyberturvallisuuden-sanasto.pdf

Tutkimuseettinen neuvottelukunta TENK 2023. Hyvä tieteellinen käytäntö HTK. Viitattu 30.4.2025. https://tenk.fi/fi/tiedevilppi/hyva-tieteellinen-kaytanto-htk

Tuomi, J. – Sarajärvi, A. 2018. Laadullinen tutkimus ja sisällönanalyysi. Helsinki: Kustannusosakeyhtiö Tammi.

Työturvallisuuskeskus 2023. Etätyössä turvallisesti. Digijulkaisu. viitattu 1.5.2025. https://ttk.fi/julkaisu/etatyossa-turvallisesti/

Valvira 2022. Potilaille annettavat terveydenhuollon etäpalvelut. Päivitetty 8.2.2022. Viitattu 10.6.2023. https://www.valvira.fi/terveydenhuolto/yksityisen_terveydenhuollon_luvat/potilaille-annettavat-terveydenhuollon-etapalvelut

Varri, A. 2021. Terveydenhuollon ohjelmistojen tietoturva kuntoon uudella standardi ISO 81001-5-1. Artikkeli Sosiaali- ja terveydenhuollon tietojenkäsittely-yhdistys ry:n sivuilla. Viitattu 29.11.2023. https://stty.org/uusi-iso-81001-5-1/

Vilkka, H. 2021. Tutki ja kehitä. 5.päivitetty painos. Jyväskylä; PS-kustannus.

Vilkka, H. 2023. Kirjallisuuskatsaus metodina, opinnäytetyön osana ja tekstilajina. Tallinna; Printon.

Vuorinen, S. (toim.) 2019. Kyberturvallisuus Ohje sosiaali- ja terveydenhuollon toimijoille. Sosiaali- ja terveysministeriön julkaisuja 2019:14. Viitattu 13.9.2022. Kyberturvallisuus Ohje sosiaali- ja terveydenhuollon toimijoille (valtioneuvosto.fi)

Wang, L. – Alexander, C-A. 2021. Cyber security during the COVID-19 pandemic. AIMS Electronics and Electrical Engineering, 5(2): 146-157. Viitattu 30.5.2023. file:///C:/Users/LEHTOPA4/Downloads/10.3934_electreng.2021008.pdf

Williams, C-M – Charturvedi, R. – Chakravarthy, K. 2020. Cybersecurity risks at pandemic. Journal of Medical Internet Research. viitattu 10.5.2023. https://www.jmir.org/2020/9/e23692/PDF

Walle, A.D. – Butta, F.W. – Kassie, S.Y. – Chereka, A.A. – Kanfe, S.G. – Dubale, A.T. -Enyew, E.B. – Dube, G.N. – Shibabaw, A.A. – Hunde, M.K. – Kitil, G.W. – Ferede, T.A. – Wubante, S.M. – Baykemagn, N.D. – Demsash, A.W. 2024. Healthcare Professionals' Attitude to Using Mobile Health Technology and Its Associated Factors in a Resource-Limited Country – An Implication for Digital Health Impelementers: A Cross Sectional Study. BioMed Research International, Volume 2024, article ID 1631379. Viitattu 1.4.2025. https://onlinelibrary.wiley.com/doi/epdf/10.1155/2024/1631376

YLE Uutiset 31.8.2023. Keskusrikospoliisi sai valmiiksi psykoterapiakeskus Vastaamon jättimäisen tietomuroon ja kiristysvyyhdin tutkinnan – epäilty kiistää yhä teot. Päivitetty 31.8.2023. Viitattu 1.9.2023. https://yle.fi/a/74-20047643

Liite 1

Tiedonhaku

TIETOKANTA	HAKULAUSEKE	RAJAUKSET -> HAKUTULOKSET	MUKAAN VALIKOIDUT
CINALH EBSCOHOST	nurse* OR nurses OR "nursing staff" OR "healthcare professional*" OR "registered nurse*" OR "health care worker*" OR "medical staff*" OR "hospital staff*" OR "hospital worker*" OR "essential worker*" AND "remote work*" OR "virtual work*" OR telework* OR "work from home*" OR "flexible work*" OR "hybrid work*" OR "e-work*" OR "e-health*" OR Telemedicine* OR "digital tool*" OR "digital health*" AND MH "Data Security+" OR MH "Computer Literacy" OR "digital skill*" OR "patient data*" OR digital attack* OR malware* OR phissing	English language Peer Reviewed Abstract Available 01/01/2021-05/31/2025 finnish English Proximity Apply aquivalent subjects > käytössä explode + **TULOKSET= 11** (poissulku “opiskelijat”, ei yleistettävä/poikkeava ympäristö, potilaan/asiakkaan näkökulma, sairaanhoitajan roolin kuvaukset, kokemukset etä-/digitaalisesta hoidon toteutuksesta, kokemukset käyttöönotosta, kaksoiskappaleet)	**2**
PUBMED	"Computer Security"[Mesh]) OR "Digital Health"[Mesh]) OR "Telemedicine"[Mesh] AND "Nurses"[Mesh]) OR "Registered nurses" AND "Remote Consultation"[Mesh] OR	Filters: Abstract Free full text English from 2021/1/1-2025/5/31 Sort by: Most recent **TULOKSET= 86**	**1**

	"Teleworking"[Mesh] OR "Digital Health"[Mesh]	(poissulkukriteerit ks.edellä)	
SCIENCE DIRECT	nurse "remote work" cybersecurity	Filters: year 2021-2025 **TULOKSET=24** (poissulkukriteerit ks.edellä)	**1**
PROQUEST	(“computer secu-rity”) AND (“nurses”) AND (“telework”)	Filters: Full text Peer reviewed Custom Date Range: from 2021-01-01 to 2025-05-31 (poissulkukriteerit ks.edellä) **TULOKSET: 3**	**0**

Liite 2

Opinnäytetyöhön valitut artikkelit ja tutkimukset

Nro	Tekijät / vuosi	Otsikko	Tavoitteet ja keskeiset tulokset
1.	Karayel, T. – Aktas, B. – Akbiyik, A. 2024	Human factors in remote work: examining cyber hygiene practices	- tutkittiin kyberhygieniakäytäntöjä etätyössä olevien henkilöiden keskuudessa, mukaan lukien terveydenhuoltoala - julkisen ja yksityisen sektorin merkittävä ero - kulttuurierot maiden välillä - etätyön tekijöiden kyberhygieniatutkimuksen puuttuminen - terveydenhuoltoalan alhainen taso kyberhygieniatasossa
2.	Jarva, E. – Oikarinen, A. – Andersson, J. – Tuomikoski, A-M. – Kääriäinen, M. – Meriläinen, M. – Mikkonen, K. 2021	Healthcare professionals`perceptions of digital health competence: A qualitative descriptive study	- kuvailla terveydenhuollon ammattilaisten käsityksiä digitaalisesta terveyden hoitamisesta - digitaalisten taitojen ja hoitotyön perinteisten kompetenssien (tiedot, taidot, asenteet ja arvot) yhdistelyä - tutkimus tehty ennen COVID 19-pandemiaa
3.	Nwankpa, J.K. – Datta, M.P. 2023	Remote vigilance: The roles of cyber awareness and cybersecurity policies among remote workers	- tarkastellaan kuinka etätyö vaikuttaa kyberturvatietoisuuteen - etätyötä tekevät työntekijät suhtautuvat positiivisesti kyberturvatietoisuuteen - etätyön tekijöiden sitoutuminen kyberturvakäytänteisiin - kontekstin sovellettavuus; terveydenhuoltoala yhdistetty muihin palvelualoihin
4.	Kaihlanen, A-M. – Elovainio, M. – Virtanen, L. – Kinnunen, U-M. – Vehko, T. – Saranto, K. – Heponiemi, T. 2023	Nursing informatics competence profiles and perceptions of health information system usefulness among registered nurses: A latent profile analysis	- tunnistaa sairaanhoitajien erilaisia kompetensseja ja niihin vaikuttavia tekijöitä digitaalisessa työympäristössä - digitaalisten taitojen ja tietosuojataitojen ristiriita - digitaalisen työkokemuksen ja digitaitojen ristiriita

5.	Bisham, M. – Creese, S. – Dutton W.D. – Esteve-Gonzalez, P. – Goldsmith M. 2021	An Exploratory study of cybersecurity in working from home: Problem or enabler?	- tunnistaa ja kuvailee etätyön riskejä kyberturvallisuuden näkökulmasta - COVID 19:n vaikutus - käsittelee yleisesti etätyötä; kontekstin sovellettavuus?
6.	Blek, T. – Solankallio-Vahteri, T. 2022	Terveydenhuollon hoitohenkilöstön tieto- ja kyberturvallisuusosaaminen.	- kuvaa hoitohenkilöstön tieto- ja kyberturvallisuusosaamista heidän itsensä arvioimana - todetaan osaamisen kehitystarve
7.	Przymus, Z. – Malagocka, K. – Przybyszewaki, K. 2024	The human factor in cybersecurity: from risk profiles to resilience	- tunnistaa kyberturvallisuuskäyttäytymisen malleja etätyöntekijöiden keskuudessa - korostaa eri työntekijä- ja alakohtaisia eroja omaksua tietoa ja uusia toimintatapoja - välinpitämättömyys ja asennoituminen huomattavan suuri ongelma
8.	Walle, A.D. – Butta, F.W. – Kassie, S.Y. – Chereka, A.A. – Kanfe, S.G. – Dubale, A.T. – Enyew, E.B. – Dube, G.W. – Shibabaw, A.A. – Hunde, M.K. – Kitil, G.W. – Ferede, T.A. – Wubante, S.M. – Baykemagn, N.D. – Demsash, A.W. 2024	Healthcare Professionals`Attitude to Using Mobile Health Technology and Its Associated Factors in a Resource-Limited Country – An Implication for Digital Health Implementers: A Cross Sectional Study	- kontekstin yhdistettävyys? - taustatekijöiden merkitys asenteisiin (sukupuoli, koulutus, kulttuuri)

Liite 3

Sisällönanalyysin rakenne

Etätyötä tekevien hoitajien kyberturvataidot ja digiosaaminen:

1. Yläkategoria: Asenteet ja käyttäytyminen kyberturvallisuudessa		
Alakategoria	***Pelkistetyt ilmaisut***	***Esimerkkilainaus***
Tietoisuuden ja toiminnan ristiriita	Tiedostetaan riskejä, mutta toiminta ei ole silti turvallista	*"Tietoisuus kybervaaroista ei takaa turvallista käyttäytymistä"*
Riskinotto / välinpitämättömyys	Oletetaan ettei olla kohde	*"Moni ei pidä itseään mahdollisena kohteena, vaikka tietäisi riskeistä"*
2. Yläkategoria: Digitaalisten taitojen merkitys		
Alakategoria	***Pelkistetyt ilmaisut***	***Esimerkkilainaus***
Digiosaamisen puute	Ei ole varmuutta teknologian käytöstä	*"Terveydenhuollon henkilöstö koki tarvitsevansa lisää tukea digitaalisten työkalujen käyttöön"*
Teknologiavarmuus parantaa asennetta	Itsevarmuus lisää teknologian käyttöä	*"Parempi osaaminen lisäsi mHealth-tekniikan käyttöä"*
3. Yläkategoria: Etätyön erityispiirteet kyberturvallisuudessa		

Alakategoria	**Pelkistetyt ilmaisut**	**Esimerkkilainaus**
Digiosaamisen puute	Ei ole varmuutta teknologian käytöstä	*"Terveydenhuollon henkilöstö koki tarvitsevansa lisää tukea digitaalisten työkalujen käyttöön"*
Teknologiavarmuus parantaa asennetta	Itsevarmuus lisää teknologian käyttöä	*"Parempi osaaminen lisäsi mHealth-tekniikan käyttöä"*
4. Yläkategoria: Organisaation ja johdon rooli		
Alakategoria	***Pelkistetyt ilmaisut***	***Esimerkkilainaus***
Puutteellinen koulutus	Ei ole annettu selkeitä ohjeita tai koulutusta	*"Tietoturvakoulutusta ei ole kohdistettu hoitohenkilöstölle riittävästi"*
Johdon tuen puute	Organisaation kulttuuri ei tue turvallisuutta	*"Kyberturvallisuuden nähdään olevan teknologiaosaston vastuulla, ei hoitotyön"*
5. Yläkategoria: Koulutus ja kehittämistarpeet		
Alakategoria	***Pelkistetyt ilmaisut***	***Esimerkkilainaus***
Koulutuksen vaikuttavuus	Koulutus parantaa käytäntöjä ja asenteita	*"Koulutus vaikutti positiivisesti digitaalisiin taitoihin ja tietoturvatietoisuuteen"*

Tarve jatkuvalle oppimiselle	Teknologiat muuttuvat nopeasti	"*Hoitajien tulee päivittää osaamistaan jatkuvasti pysyäkseen mukana digitaalisessa muutoksessa*"