UNIVERSITY OF
EASTERN FINLAND

Yksityisen terveydenhuollon henkilöstön tietoturva- ja tietosuojaosaaminen

Jaila Tuovinen
Pro gradu -tutkielma
Sosiaali- ja terveydenhuollon tiedonhallinta
Itä-Suomen yliopisto
Sosiaali- ja terveysjohtamisen laitos
Toukokuu 2023

ITÄ-SUOMEN YLIOPISTO, yhteiskuntatieteiden ja kauppatieteiden tiedekunta
Sosiaali- ja terveysjohtamisen laitos
Sosiaali- ja terveydenhuollon tiedonhallinta
Tuovinen, Jaila: Yksityisen terveydenhuollon henkilöstön tietoturva- ja tietosuojaosaaminen
Pro gradu -tutkielma, 70 sivua, 2 liitettä (12 sivua)
Tutkielman ohjaajat: YTM, TtM Tiina Hassinen, yliopisto-opettaja, TtM Heli Kumpulainen
Toukokuu 2023
Avainsanat: tietoturva, tietosuoja, terveydenhuoltohenkilöstö, osaaminen

Digitaalinen toimintaympäristö on muuttunut viime vuosina merkittävästi digitalisoitumisen edetessä ja digitalisaation hyödyntämisen lisääntyessä. Sen seurauksena tietoa on alettu hyödyntämään laajemmin ja toimintaympäristön muuttuessa tarvitaan myös toimia digitaalisen turvallisuuden kehittämiseksi, jolloin tietoturvan ja tietosuojan merkitys korostuu. Digitaalista turvallisuutta toteutetaan tietoturvan, tietosuojan, kyberturvallisuuden, riskienhallinnan sekä toiminnan jatkuvuuden takaamisen keinoin. Myös tietoturvahyökkäykset ovat kehittyneet ja asettavat vaatimuksia organisaatioiden tietoturvallisuudelle, mutta myös henkilöstön tietoturvaosaamiselle. Terveydenhuollon henkilöstön tietoturva- ja tietosuojaosaaminen koostuu tietoturvatietämyksestä, johon kuuluu kyky noudattaa ja hyödyntää tietoturvaperiaatteita sekä tietoturvakäytäntöjä. Tietoturvaosaamisen vahvistamisella on mahdollista välttää tietoturvariskejä.

Tämän kyselytutkimuksen tarkoituksena oli tutkia yksityisen terveydenhuollon henkilöstön tietoturva- ja tietosuojaosaamisen tasoa. Lisäksi tavoitteena oli tunnistaa henkilöstön tietoturva- ja tietosuojaosaamisen kehityskohteita osaamisen sekä koulutuksen kehittämisen tueksi. Tutkimusaineisto (n = 39) kerättiin sähköisellä kyselylomakkeella yksityisen terveydenhuollon organisaation yksiköistä. Tutkimusmenetelmänä tässä tutkimuksessa oli kvantitatiivinen tutkimus. Määrällinen aineisto analysoitiin tilastollisen kuvailun avulla ja täydentävä avoin kysymys sisällön analyysin avulla. Tutkimuksen teoreettisena viitekehyksenä käytettiin Staggersin ja hänen tutkimusryhmänsä (2002) ydinosaamisen alueita ja osaamisen tasoja.

Tutkimustulosten perusteella yksityisen terveydenhuollon henkilöstön tietoturva- ja tietosuojaosaaminen on hyvällä tasolla, mutta esille nousi myös kehityskohteita tietoturva- ja tietosuojaosaamisen vahvistamiseksi. Suurimmat kehityskohteet liittyivät turvallisiin salasanakäytäntöihin, työvälineiden henkilökohtaiseen käyttöön ja organisaation tietoturva- ja tietosuojaohjeiden sijainnin selkeyttämiseen. Lisäksi kehitystä vaatii tieto, keneen henkilöstö voi olla yhteydessä tietoturva- ja tietosuoja-asioihin liittyvissä ongelmissa. Tietoturva- ja tietosuojakoulutuksen osalta lisäkoulutukselle ei henkilöstön mielestä ole suurta tarvetta, mutta koulutuksen yhdistämistä käytännön työhön toivottiin. Tutkimuksesta saatu tieto on hyödynnettävissä organisaation tietoturva- ja tietosuojaosaamisen kehitystä ja koulutusta varten. Terveydenhuollon tietoturvaosaamisen jatkotutkimus on tärkeää sekä ajankohtaista ja aihe tarjoaa valtavasti erilaisia tutkimusmahdollisuuksia ja näkökulmia. Tämän tutkimuksen tulosten perusteella jatkotutkimuksissa voisi tutkia terveydenhuollon henkilöstön tietoturva- ja tietosuojakoulutuksen sisältöä ja arvioida sen soveltuvuutta eri ammattiryhmille.

UNIVERSITY OF EASTERN FINLAND, Faculty of Social Sciences and Business Studies
Department of Health and Social Management
Health and human services informatics
Tuovinen, Jaila: Information security and data protection competence of private healthcare personnel
Master's thesis, 70 pages, 2 appendices (12 pages)
Thesis Supervisors: MSocSc, MHSc Tiina Hassinen, University Teacher, MHSc Heli Kumpulainen
May 2023
Keywords: information security, data protection, health professionals, knowledge

The digital operating environment has significantly changed in recent years as digitalization has progressed and the utilization of digitalization has increased. As a result, information has been utilized more widely, and as the operating environment changes, actions are also needed to develop digital security, highlighting the importance of information security and data protection. Digital security is implemented through means such as information security, data protection, cybersecurity, risk management, and ensuring business continuity. Information security attacks have also evolved, imposing demands on organizations' information security but also on personnel's information security expertise. Healthcare personnel's information security and data protection skills consist of knowledge of information security, including the ability to adhere to and utilize information security principles and practices. Strengthening information security skills can help avoid security risks.

The purpose of this survey was to investigate the level of information security and data protection skills of private healthcare personnel. Additionally, the aim was to identify areas for improvement in personnel's information security expertise to support the development of organizational information security and data protection skills through training. The research material (n = 39) was collected via an electronic survey from a private healthcare organization’s units. A quantitative research method was used in this study, and the quantitative data was analyzed using statistical description and supplemented by a content analysis of an open-ended question. The theoretical framework for the research was Staggers' (2002) core competency areas and competency levels.

Based on the research results, private healthcare personnel's information security and data protection skills are at a good level, but areas for improvement were also identified to strengthen information security and data protection expertise. The most significant areas for improvement were related to secure password practices, personal use of tools, and the clarity of organizational information security and data protection guidelines. Additionally, it is necessary to clarify who personnel can contact regarding information security and data protection issues. Regarding information security and data protection training, personnel did not feel there was a significant need for additional training, but they hoped for a connection between training and practical work. The information obtained from the research can be utilized for the development and training of organizational information security and data protection skills. Further research into healthcare information security expertise is important and topical, providing a wide range of research opportunities and perspectives. Based on the results of this study, further research could investigate the content of healthcare personnel's information security and data protection training and assess its suitability for different professional groups.

Lyhenteet

IMIA	International Medical Informatics Association
STM	Sosiaali- ja terveysministeriö
TENK	Tutkimuseettinen neuvottelukunta
VM	Valtiovarainministeriö

Sisältö

Kuviot

Taulukot

1 Johdanto

Digitalisaatio, sähköinen asiointi ja palveluiden keskittäminen sekä verkottuminen ovat lisääntyneet ja Suomi on yksi maailman kärkimaista sähköisten palveluiden ja digitalisaation hyödyntämisessä (Sosiaali- ja terveysministeriö (STM) 2016, 4). Valtiovarainministeriö (VM) toteaa digitalisaation ja sähköisten palveluiden lisääntyneen käytön asettavan uusia haasteita tietoturvallisuuden hallinnalle samalla kun tietoturvahyökkäykset ovat kehittyneet. Nämä lisäävät vaatimuksia tietoturvallisuudelle, mutta myös henkilöstön tietoturva- ja tietosuojaosaamiselle. (VM 2017, 11.) Teknologian nopea kehittyminen digitaalisuuden myötä lisää myös haasteita tietoturvalliselle ja vaatimusten mukaiselle palveluiden tuotannolle (STM 2019, 13).

Digitaalinen turvallisuus on yksi yhteiskunnan perusedellytyksistä, jota toteutetaan tietoturvan, kyberturvallisuuden, tietosuojan, riskienhallinnan sekä toiminnan jatkuvuuden takaamisen keinoin (VM 2020, 9). Lainsäädäntö velvoittaa tietoturvan ja tietosuojan toteuttamista sosiaali- ja terveydenhuollossa, mutta lisäksi kyseessä on myös organisaation maine sekä uskottavuus (STM 2019, 10–13). Terveydenhuollon ammattilaisten työhön kuuluu digitaalisten palveluiden käyttö päivittäin. Palveluiden toteutuksessa hyödynnetään tieto- ja viestintäteknologiaa, joiden avulla tarvittavat asiakas- ja potilastiedot ovat saatavilla helposti ja oikeaan aikaan digitaalisesti. Tietojärjestelmien käytöllä tavoitellaan ensisijaisesti potilaiden sekä asiakkaiden hyvää, tehokasta ja laadukasta hoitoa tai palvelua, jolloin tietoturvan toteutuminen on tärkeää. (STM 2019, 13, 14.) Sen vuoksi on tärkeää kiinnittää erityisesti huomiota arkaluontoisten asiakas- ja henkilötietojen käsittelyyn ja salassapitoon, eheyteen sekä saatavuuteen yksityisyyden takaamiseksi (STM 2019, 13).

Tietoturva on tärkeä osa terveydenhuollon toimintaa sekä turvallisuutta, sillä sen avulla pyritään varmistamaan tiedon eheys, luottamuksellisuus ja saatavuus (STM 2019, 52). Lisäksi tietoturvan avulla turvataan yksityisyyttä, etuja ja oikeuksia (Andreasson, Koivisto & Ylipartanen 2016, 8). Tietoturvan yhtenä tärkeänä päämääränä on tietosuojan toteuttaminen, johon pyritään tietoturvan käytännön toimilla. Terveydenhuollon henkilöstölle salassapitovelvollisuus on tärkeä osa työtä ja siitä on säädetty laajasti terveydenhuoltoa koskevassa lainsäädännössä.

Terveydenhuollon organisaatioiden on varmistettava arkaluontoisten tietojen säilyminen turvassa ja niiden käsittely asianmukaisesti. (Valvira 2018; STM 2019, 14.) Tietoturvan vaarantuessa kyseessä on tietoturvapoikkeama, jolloin tiedon eheys, luotettavuus ja saatavuus eli tietosuoja on vaarantunut tahallisesti tai tahattomasti (VM 2017, 11). Tietoturvan toteuttamisessa huolellisuus ja hyvät tietoturvakäytännöt ovat ydinasemassa. Terveydenhuollon tietoturvallisuudessa ammattilaiset ovat merkittävin uhka, koska tietosuoja voi vaarantua tietämättömyyden tai virheen vuoksi. Sen vuoksi henkilöstön tietoturvatietämys ja tietoturvallinen käyttäytyminen ovat tärkeässä roolissa organisaation tietoturvan ja tietosuojan toteutumiselle. (Box & Pottas 2013, 1094; Lebek, Uffen, Breitner, Neumann & Hohler 2013, 2978.)

Tietoturvaosaaminen kuuluu osaksi ammattitaitoa ja sen ylläpitoa. Jokaisen organisaation henkilöstön jäsenen tulisi hallita tietoturvaperiaatteet ja osata hyödyntää niitä työssään. (STM 2019, 24.) Osaaminen tarkoittaa henkilön kykyä toteuttaa jokin tavoite, joka hänelle on määritelty. Ammatillinen osaaminen rakentuu tiedoista, taidoista, minäpystyvyydestä, asenteista sekä aiemmasta kokemuksesta. (Kangasniemi, Hipp, Häggman-Laitila, Kallio, Karki, Kinnunen, Pietilä, Saarnio, Viinamäki, Voutilainen & Waldén 2018, 12.) Tietoturvatietämyksellä tarkoitetaan dynaamista prosessia, jota riskien muuttuminen haastaa. Se määritellään tasoksi, jolla henkilöstön jäsenet ymmärtävät tietoturvan tärkeyden organisaatiossa, osana omaa vastuuta ja toimii ymmärryksen mukaisesti. (Kruger & Kearney 2006, 289, 290.) Henkilöstön tietoturvaosaaminen on jaoteltu tässä tutkielmassa kolmeen osaamisen ydinalueeseen pohjautuen Staggersin, Gassertin & Curranin (2002a) tiedonhallinnan ydinosaamisalueista. Osaamisen ydinalueita on turvalliset tietotekniikan käyttötaidot, tietoturvatiedot sekä tietoturvataidot.

Terveydenhuollon toimintaympäristön ja digitalisaation muutoksen vuoksi henkilöstön digitaalisen osaamisen kehittämiseksi tarvitaan laadukasta koulutusta (Bichel-Findlay, Koch, Mantas, Abdul, Al-Shorbaji, Ammenwerth, Baum, Borycki, Demiris, Hasman, Hersh, Hovenga, Huebner, Huesing, Kushniruk, Hwa Lee, Lehmann, Lillehaug, Marin, Marchollek, Martin-Sanchez, Merolli, Nishimwe, Saranto, Sent, Shachak, Udayasankaran, Were & Wright 2022, 2). Organisaatioiden on huolehdittava henkilöstön tarvittavista tiedoista ja taidoista sekä kunnossa olevista tietoturvakäytännöistä. Sen mahdollistamiseksi organisaation on tarjottava koulutusta

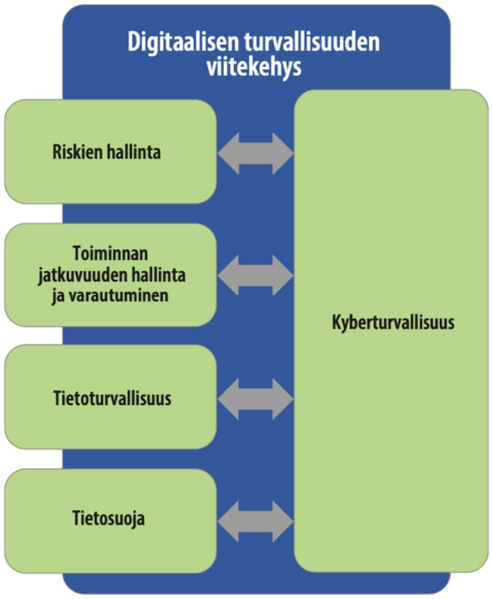
henkilöstölle tietoturvan merkityksen ymmärtämisen lisäämiseksi. Tietoturva- ja tietosuojatyöhön on kannattavaa sijoittaa, sillä henkilöstön osaamiseen sijoittaminen näiden osa-alueiden osalta tuo organisaatiolle takaisin tuottoa, tehokkuutta sekä kustannussäästöjä. (Andreasson ym. 2016, 13.) Tietoturvaan perehdyttämisen tulee alkaa heti työsuhteen alusta ja olla osana henkilöstön työuraa. Perehdytysprosessiin tulee panostaa ja huomioida, ettei tietoturva- ja tietosuoja-asiat jää vain vähäiselle huomiolle tai pelkästään itseopiskelun varaan. (Andreasson ym. 2016, 52; STM 2019, 24.) Tietoturvakoulutuksen on osoitettu lisäävän terveydenhuollon ammattilaisten tietoisuutta tietoturvasta ja lisäävän positiivista vaikutusta tietoturvallisten toiminnan viemistä käytännön työhön (EunWon & Seomun 2021, 2). Osaamisen puutteet voivat aiheuttaa ahdistusta ja epävarmuutta, jolloin työviihtyvyys heikkenee ja työteho laskee. Lisäksi tietoturva- ja tietosuojaosaamattomuus voi aiheuttaa organisaatiolle merkittävän turvallisuusuhan. (Andreasson ym. 2016, 13.)

Tämän pro gradu -tutkielman tarkoituksena on tutkia kyselytutkimuksen avulla yksityisen terveydenhuollon henkilöstön tietoturva- ja tietosuojaosaamisen tasoa. Lisäksi tavoitteena on tunnistaa yksityisen terveydenhuollon henkilöstön tietoturva- ja tietosuojaosaamisen kehityskohteita osaamisen ja organisaation koulutuksen kehittämisen tueksi. Aihe on ajankohtainen digitalisaation ja siihen liittyvien tietoturvauhkien lisääntyessä. Tässä tutkimuksessa henkilöstön tietoturva- ja tietosuojaosaamista tutkitaan pääasiassa tietoturvaosaamisen kautta, koska tietoturvan päämääränä on tietosuojan toteuttaminen tietoturvallisuuteen liittyvillä käytännön toimilla.

2 Tietoturva ja tietosuoja terveydenhuollossa

2.1 Digitaalisen toimintaympäristön muutos

Digitaalinen toimintaympäristö on muuttunut viime vuosina merkittävästi digitalisoitumisen edetessä, jonka seurauksena tietoa on alettu hyödyntämään laajemmin. Toimintaympäristön muuttuessa tarvitaan myös toimia digitaalisen turvallisuuden kehittämiseksi, jolloin tietoturvan ja tietosuojan merkitys korostuu. (VM 2020, 18, 19.) Digitaalinen turvallisuus on yksi yhteiskunnan perusedellytyksistä, jota toteutetaan tietoturvan, tietosuojan, kyberturvallisuuden, riskienhallinnan sekä toiminnan jatkuvuuden takaamisen keinoin (Kuvio 1). Digitaalisen turvallisuuden tavoitteena on suojata uhkilta ja riskeiltä, jotka kohdistuvat henkilötietoihin, tietoaineistoihin ja prosesseihin digitaalisessa toimintaympäristössä. (VM 2020, 9–11.)



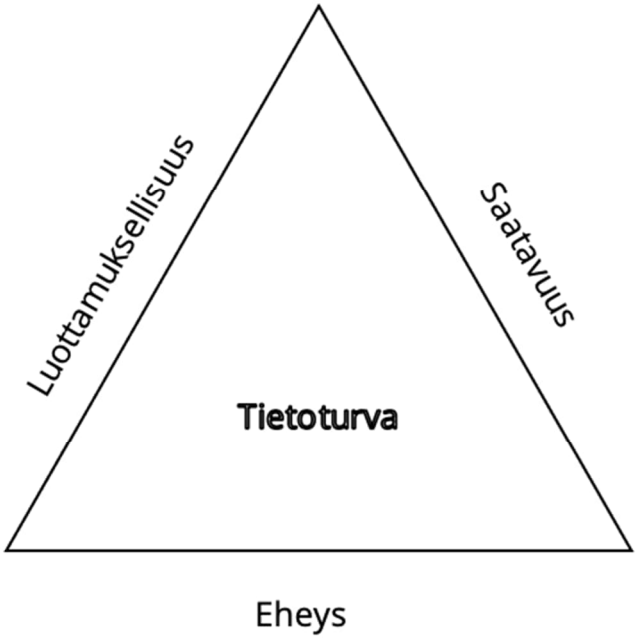
Kuvio 1. Digitaalisen turvallisuuden viitekehys (VM 2020, 16)

Riittävä tietoturva ja tietosuoja on digitalisaation välttämätön edellytys, mutta myös mahdollisuus. Digitaalinen turvallisuus voi olla merkittävä digitalisaation kilpailuetu tai epävarmuutta synnyttävä tekijä, kun sen merkitys tulee entisestään korostumaan tietojenkäsittelyn lisääntyessä. Tietoturvallisuus mahdollistaa digitalisoitumisen ja teknologian hyötyjen hyödyntämisen täysimääräisesti. (Andreasson ym. 2016, 10, 11.) Tässä tutkielmassa

käsitellään digitaalista turvallisuutta pääasiassa tietoturvan näkökulmasta, mutta myös siihen olennaisesti liittyvän tietosuojan kautta. Lisäksi tutkielmassa sivutaan myös kyberturvallisuutta osana tietoturvallisuutta.

2.2 Tietoturva ja tietosuoja

Tietoturva on tärkeä osa terveydenhuollon toimintaa ja turvallisuutta. Se tarkoittaa järjestelyitä (Kuvio 2), joiden avulla pyritään varmistamaan tiedon eheys, luottamuksellisuus ja saatavuus (STM 2019, 52). Tiedon eheys tarkoittaa tiedon yhteneväisyyttä alkuperäiseen tietoon verrattuna. Luottamuksellisuus tarkoittaa tiedon turvaa siten, ettei kukaan sivullinen saa tietoa käsiinsä. Luottamuksellisuutta voidaan turvata salassapidolla. (STM 2019, 13, 14.) Saatavuus tarkoittaa tiedon käyttömahdollisuutta haluttuna aikana (STM 2019, 52). Terveydenhuollossa tietojen luottamuksellisuuden suojaaminen on erityisen tärkeää arkaluonteisten tietojen vuoksi ja yksityisyyden takaamiseksi. Turvallisuudessa korostuu myös tietojen eheys ja saatavuus, koska potilaan hoitamiseksi oikean tiedon tulee olla käytettävissä oikealla hetkellä hoitotilanteessa. (STM 2019, 13.) Terveydenhuollossa tietoturvaa voidaan tarkastella myös tiedon teknisistä, fyysisistä ja hallinnollisista näkökulmista. Fyysiseen turvallisuuteen kuuluu katastrofien ehkäisytoimenpiteet tiedon suojaamiseksi, tekniseen turvallisuuteen kuuluu tietoturvallisuus ja hallinnolliseen turvallisuuteen kuuluu turvatoimenpiteet turvallisuuden sekä luotettavuuden varmistamiseksi. (Kang & Seomun 2021, 17.)



Kuvio 2. Tietoturvan perusta (STM 2019, 52)

Tietosuoja on osa tietoturvan päämäärää ja siihen pyritään tietoturvan käytännön toimilla. Tietoturvan avulla turvataan yksityisyyttä, etuja ja oikeuksia eli turvataan tietosuojan toteutuminen. (Andreasson ym. 2016, 8.) Tietosuoja on jokaisen perusoikeus ja sen tarkoituksena on ohjata hyviä henkilötietojen käsittelykäytäntöjä, kuten milloin ja millä edellytyksillä henkilötietoja voi käsitellä. Tietosuoja on tärkeää tiedon sekä tiedon kohteen yksityisyyden turvaamiseksi, jotta jokaisen henkilötiedot ovat suojatut. (Andreasson ym. 2016, 8; Tietosuojavaltuutetun toimisto 2022.) Tietosuoja toimii rekisteröidyn ja rekisterinpitäjän välisen luottamuksen rakentajana (Andreasson ym. 2016, 8).

Terveydenhuollon henkilöstölle salassapitovelvollisuus on tärkeä osa työtä ja siitä on säädetty laajasti terveydenhuoltoa koskevassa lainsäädännössä. Salassapitovelvollisuudesta on säädetty muun muassa laissa yksityisestä terveydenhuollosta (152/1990, 12 §), laissa potilaan asemasta ja oikeuksista (785/1992, 13 §) sekä laissa terveydenhuollon ammattihenkilöistä (559/1994, 17 §). Terveydenhuollon organisaatioiden on varmistettava arkaluontoisten tietojen säilyminen turvassa ja niiden käsittely asianmukaisesti. Palveluksessa oleva henkilö ei saa luvatta ilmaista tehtävänsä vuoksi saatuja tietoja toisen henkilön terveydestä, sairaudesta, vammaisuudesta, toimenpiteistä tai muista seikoista työsuhteensa aikana eikä työsuhteensa päätyttyä. (Valvira 2018; STM 2019, 14.)

2.3 Tietoturvan toteuttaminen

Terveydenhuollon ammattilaisten työhön kuuluu päivittäin digitaalisten palveluiden, kuten potilastietojärjestelmien käyttö potilastiedon hallinnassa. Tietojärjestelmien käytöllä tavoitellaan ensisijaisesti potilaiden sekä asiakkaiden hyvää, tehokasta ja laadukasta hoitoa tai palvelua, jonka vuoksi tietoturvan toteutuminen on tärkeää. (STM 2019, 13, 14.) Tietoturvan päämääränä ja tavoitteena on turvata terveydenhuollon toimintaa, tietoliikennettä, laitteistoja ja ohjelmistoja sekä tietoaineistoja asiakirjojen turvallisella säilytyksellä, tietojen salauksella, tilojen ja laitteiden lukituksella, kulunvalvonnalla sekä virustorjuntaohjelmien, palomuurin ja varmenteiden hyödyntämisen avulla (STM 2019, 52). Yleisiä tietoturvakäytäntöjä on monimutkaisten salasanojen käyttö, saman salasanan käyttö vain yhdessä palvelussa, harkittu liitetiedostojen tai linkkien avaaminen, hyvä perehtyminen organisaation tietoturvakäytäntöihin sekä häiriötilanteiden hallinta tutustumalla etukäteen tietoturvasta vastaaviin henkilöihin (Kyberturvallisuuskeskus 2020). Tekniset toimenpiteet ovat kuitenkin riittämättömiä, jos työntekijät eivät ole tietoisia turvallisuusriskeistä (Lebek ym. 2013, 2978).

Tietoturvan toteuttamisessa huolellisuus ja hyvät tietoturvakäytännöt ovat ydinasemassa. Terveydenhuollon tietoturvallisuudessa ammattilaiset ovat merkittävin uhka, koska tietosuoja voi vaarantua tietämättömyyden tai virheen vuoksi. Sen vuoksi henkilöstön tietoturvatietämys ja tietoturvallinen käyttäytyminen ovat tärkeässä roolissa organisaation tietoturvaa ja tietosuojaa. (Box & Pottas 2013, 1094; Lebek ym. 2013, 2978.) Tietoturvatietämyksellä tarkoitetaan dynaamista prosessia, jota riskien muuttuminen haastaa. Se määritellään tasoksi, jolla henkilöstön jäsenet ymmärtävät tietoturvan tärkeyden organisaatiossa, osana omaa vastuuta ja toimii ymmärryksen mukaisesti. (Kruger & Kearney 2006, 289, 290.)

Tietoturvan vaarantuessa kyseessä on tietoturvapoikkeama, jolloin tiedon eheys, luotettavuus ja saatavuus eli tietosuoja on vaarantunut tahallisesti tai tahattomasti esimerkiksi tietovuodon, palvelunestohyökkäyksen tai puhelun salakuuntelun vuoksi (VM 2017, 11). Mahdollisia turvallisuusriskejä on muun muassa henkilöstön huonot salasanakäytännöt, tietokoneilta pois kirjautumatta jättäminen ja terveystietojen toimittaminen sähköpostitse väärälle henkilölle (Humaidi & Balakrishnan 2018, 18, 19). Terveydenhuollossa kyberuhkat ovat päivittäisiä, jonka vuoksi myös kyberturvallisuus kuuluu sosiaali- ja terveydenhuollon palveluiden

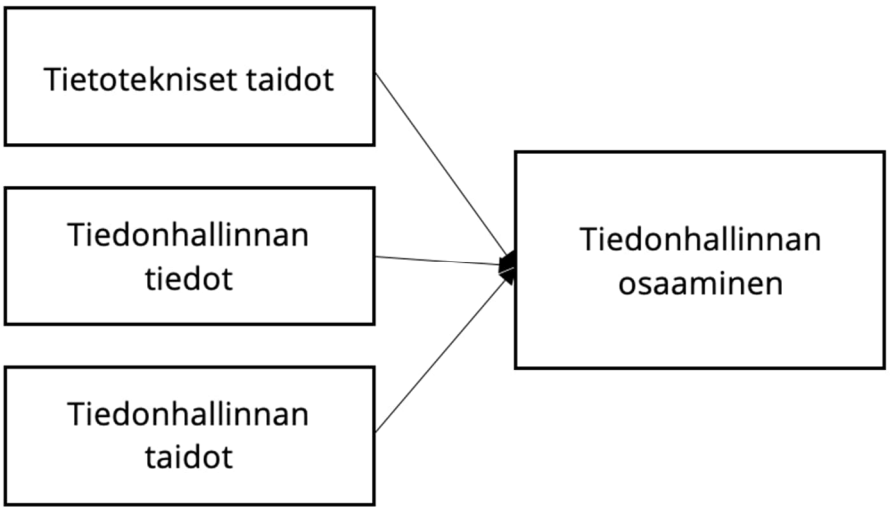
varmistamiseen sekä kokonaisturvallisuuteen osana tietoturvaa (STM 2019, 11). Kyberturvallisuus on vielä vakiintumaton suhteellisen uusi termi, jolla viitataan digitalisoitumisesta johtuviin uudenlaisiin turvallisuushaasteisiin. Sen tarkoituksena on suojata digitalisoituvaa yhteiskuntaa haitalliselta kybervaikuttamiselta ja tietoverkkotiedusteluilta sekä turvata luottamuksellisuutta tiedonkäsittelyssä. (STM 2019, 13; Liikenne- ja viestintävirasto Traficom 2020, 4; Sisäministeriö 2022.)

Terveydenhuoltoon kohdistuvat kyberuhkat liittyvät terveydenhuollossa käytettävien laitteiden ohjelmistoihin, mobiililaitteisiin, etähallittaviin laitteisiin sekä salasanoihin ja järjestelmien käyttöön (Viestintävirasto 2016, 3–7). Kyberuhkien keinoina on ollut erityisesti kiristyshaittaohjelmat, jotka salaavat hyökkäyksen kohteena olleen tietokoneen tiedostoja. Tietojen salauksen avulla hyökkääjä vaatii tietojen palauttamiseksi lunnaiden maksamista. Toinen yleinen keino on tietojenkalasteluyritys sähköpostitse terveydenhuollon organisaation henkilöstölle. Luotettavan näköisellä sähköpostiviestillä ja kirjautumissivulla pyritään saamaan sähköpostitili hyökkääjän haltuun. (STM 2019, 18, 19.) Kolmas yleinen keino on ohjelmistojen haavoittuvuuksien hyväksikäyttö, jolloin hyökkääjä voi esimerkiksi estää ohjelmiston tai järjestelmän toimimisen ja paljastaa sen kautta salassa pidettäviä tietoja (Viestintävirasto 2016, 3). Haasteena kyberturvallisuudelle on ihminen itse ja huolimattomuus tietoturvaan liittyvissä asioissa (Sederholm, Laitinen, Lehto & Kari 2019, 89).

Tehokkaassa kyberturvallisuuden toteuttamisessa keskeisessä roolissa on valpas ja koulutettu henkilöstö, jotka osaavat ja uskaltavat raportoida havaitsemistaan poikkeamista sekä uhkista (Liikenne- ja viestintävirasto Traficom 2020, 24). Lisäksi keskeinen osa kestävien tietoresurssien turvaamista on organisaation tarpeisiin räätälöidyt suojatoimenpiteet (Horne, Ahmad & Maynard 2016, 6). Kyberturvallisuuden hallinnassa tulee huomioida organisaation resursointi, järjestelmien ja palveluiden hankinta, kriittisten toimintojen ja järjestelmien toimintavarmuus sekä erityisesti henkilöstön tietoturvaosaaminen. Turvallisuuteen liittyy lisäksi vahvasti asiakas- ja henkilötietojen käsittelyn arkaluonteisuus ja niiden suojaaminen yksityisyyden turvaamiseksi. Lainsäädäntö velvoittaa tietoturvan ja tietosuojan toteuttamista sosiaali- ja terveydenhuollossa, mutta kyseessä on myös organisaation maine sekä uskottavuus. (STM 2019, 10–13.)

2.4 Tiedonhallinnan ydinosaamisen alueet viitekehyksenä

Tutkimuksen teoreettisena viitekehyksenä on käytetty Staggersin tutkimusryhmineen (2002a) laatimia tiedonhallinnan ydinosaamisalueita sekä osaamisen tasoja. Staggers tutkimusryhmineen (2002a) on tutkinut hoitotyön tiedonhallinnan osaamista ja laatinut sen perusteella kolme kattavasti kuvattua tiedonhallinnan ydinosaamisaluetta hoitotyön ammattilaisille. Nämä kolme ydinosaamisaluetta ovat tietotekniset taidot, tiedonhallinnan tiedot ja tiedonhallinnan taidot (Kuvio 3). Tietoteknisillä taidoilla tarkoitetaan tietokonelaitteistojen ja -ohjelmistojen käyttöä, tiedolla ja taidolla puolestaan osaamisen kehittämisen perustaa. Tiedonhallinnan osaamiseen kuuluu tietokonetaitojen eri osa-alueita, joita on hallinta, viestintä, datan käyttö, dokumentaatio, koulutus, seuranta, työpöytäohjelmistojen käyttö sekä järjestelmien käyttö. Lisäksi osaamiseen kuuluu tiedonhallinnan eri osa-alueita, joita on datan käyttö, vaikutusten ymmärtäminen, yksityisyys ja turvallisuus sekä järjestelmien käyttö. (Staggers ym. 2002b, 2–13.)



Kuvio 3. Tiedonhallinnan ydinosaamisen alueet (Staggers ym. 2002a)

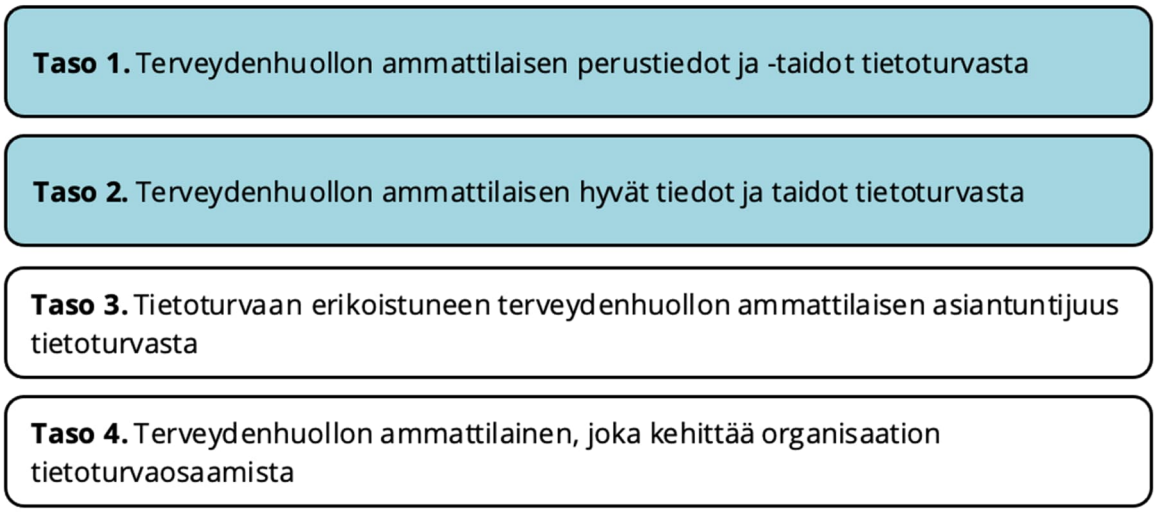
Ydinosaamisen alueet johdettiin tähän tutkimukseen sopiviksi tietoturva- ja tietosuojaosaamisen ydinalueiksi (Taulukko 1). Tietotekniikan käyttötaidoista muotoutui turvallisten tietotekniikan käyttötaitojen ydinalue, tiedonhallinnan tiedoista tietoturvatietojen ydinalue ja tiedonhallinnan taidoista tietoturvataitojen ydinalue. Tässä tutkimuksessa ydinalueita hyödynnetään henkilöstön tietoturva- ja tietosuojaosaamisen tarkasteluun. Niiden

mukaisesti tietoturva- ja tietosuojaosaaminen koostuu turvallisista tietotekniikan käyttötaidoista, tietoturvatiedoista sekä tietoturvataidoista.

Taulukko 1. Tietoturva- ja tietosuojaosaamisen ydinalueet

Staggersin ym. (2002a) tiedonhallinnan ydinosaamisen alueet		**Tietoturva- ja tietosuojaosaamisen ydinalueet**
Tietotekniikan käyttötaidot	→	Turvalliset tietotekniikan käyttötaidot
Tiedonhallinnan tiedot	→	Tietoturvatiedot
Tiedonhallinnan taidot	→	Tietoturvataidot

Ydinosaamisen alueiden lisäksi Staggers tutkimusryhmineen (2002a) on kehittänyt neljä osaamisen tasoa tiedonhallinnan osaamisen arviointia sekä kehittämistä ja koulutusta varten. Osaamisen tasot on jaettu neljään eri tasoon, joita ovat aloittelija, kokenut, tiedonhallinnan asiantuntija sekä tiedonhallinnan kehittäjä. Oletuksena ei ole, että tietyn tason hoitotyön ammattilainen olisi pätevä kaikissa kyseisen tason asioissa. (Staggers ym. 2002a, 383–390.) Taso 1 kuvailee aloittelijan osaamista, taso 2 kokeneen henkilön osaamista, taso 3 tiedonhallinnan asiantuntijan osaamista ja taso 4 tiedonhallinnan kehittäjän osaamista. Aloittelijalla on perustavanlaatuista osaamista tiedonhallinnasta ja tietotekniikan perusteista. Kokeneella henkilöllä on taito käyttää tiedonhallinnan ja tietotekniikan taitoja muun pätevyyden tukena. Asiantuntijalla on terveydenhuollon koulutuksen lisäksi myös koulutusta tiedonhallinnan tai tietojenkäsittelyn alalta ja hän kykenee tietojärjestelmien kehittämiseen. Kehittäjä kykenee johtamaan tiedonhallinnan käytäntöjä sekä kehittämään tutkimusta. Eri osaamisen alueilla on huomioitu myös tietoturvan ja tietosuojan osaaminen. (Staggers ym. 2002a, 385, 386). Tässä tutkimuksessa tarkastellaan tietoturva- ja tietosuojaosaamisen näkökulmasta osaamisen tasoja 1 ja 2 (Kuvio 4), jotka on johdettu Staggersin tutkimusryhmineen (2002a) laatimista osaamisen tasoista.



Kuvio 4. Tietoturva- ja tietosuojaosaamisen tasot (Mukaillen Staggers ym. 2002b)

Tasolla 1 tietoturvan ja tietosuojan osalta osaamisvaatimuksena on ymmärtää asiakkaan ja potilaan oikeudet sekä osata etsiä käytettävissä olevia resursseja eettisten päätösten tueksi. Tasolla 2 osaamisvaatimuksena on käsitellä tietoa eheyden periaatteiden sekä ammattietiikan ja lakivaatimusten mukaisesti. Lisäksi tasolla 2 tulee osata kuvata tapoja tiedon suojaamiseksi. (Staggers ym. 2002b, 3, 4.) Tässä tutkielmassa tasojen osaamisvaatimuksia sovelletaan siten, että tasolla 1 on henkilöstön perustiedot ja -taidot tietoturvasta ja tasolla 2 hyvät tiedot ja taidot tietoturvasta.

3 Tietoturvaosaaminen

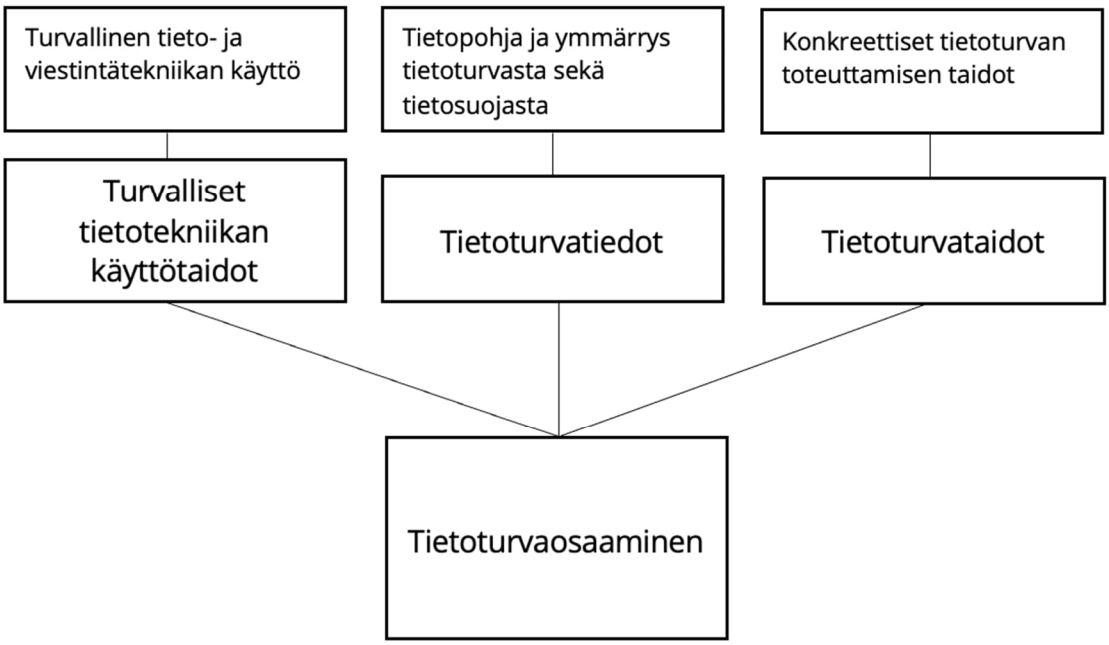
3.1 Tietoturvaosaaminen osana ammattitaitoa

Terveydenhuollon ympäristöissä tapahtuu merkittäviä muutoksia, joihin sisältyy myös digitaalisia muutoksia. Sen seurauksena terveydenhuollon tehtävissä lisääntyy henkilöstön digitaalisten taitojen osaamisen merkitys ja siten myös digitaalisten taitojen koulutuksen tärkeys. Tärkeintä on, että jokainen terveydenhuollon ammattilainen osaa käyttää tieto- ja viestintätekniikkaa turvallisesti työssään. (Bichel-Findlay ym. 2022, 2–7.) Osaaminen tarkoittaa henkilön kykyä toteuttaa jokin ennalta määritelty tavoite. Ammatillinen osaaminen rakentuu tiedoista, taidoista, minäpystyvyydestä, asenteista sekä aiemmasta kokemuksesta. (Kangasniemi ym. 2018, 12.)

Tietoturvaosaaminen on tärkeä osa terveydenhuollon toimintaa, koska terveydenhuollossa työskennellään potilaiden kanssa ympäri vuorokauden ja tuotetaan, käytetään sekä hallinnoidaan terveydenhuollon tietoja. Terveydenhuollon tehtävänä on suojella potilasta vahingoilta, joihin kuuluu myös potilastietojen yksityisyyden ja luottamuksellisuuden varmistaminen, joten terveydenhuollon ammattilaisten tulisi tunnistaa tietoturvan tärkeys sekä haluta hyödyntää tietoturvallisuutta työssään. (EunWon & Seomun 2021, 2; Kang & Seomun 2021, 16.) Tietoturvaosaaminen kuuluu osaksi ammattitaitoa ja sen ylläpitoa. Jokaisen organisaation henkilöstön jäsenen tulisi hallita tietoturvaperiaatteet ja osata hyödyntää niitä työssään (STM 2019, 24). Tietoturvaosaamiseen voi vaikuttaa pidempi työura, jolloin terveydenhuollon ammattilaiset ovat vastaanottavaisempia ja osaavampia tietoturvakoulutuksessa. Haasteena tietoturvaosaamiselle voi olla fyysiset ja ympäristöön liittyvät esteet. Lisäksi epävarmuutta tietoturvan toteutumiseen voi lisätä ennalta arvaamattomat tai kiireelliset hätätilanteet, jolloin tietoturvallinen käyttäytyminen voi jäädä terveydenhuollon ammattilaiselta huomioimatta. (EunWon & Seomun 2021, 11.)

Tietoturva- ja tietosuojaosaaminen on luokiteltu tässä tutkimuksessa kolmeen ydinalueeseen, joita on turvalliset tietotekniikan käyttötaidot, tietoturvatiedot ja tietoturvataidot (Kuvio 5). Turvallisilla tietotekniikan käyttötaidoilla tarkoitetaan tässä tutkielmassa turvallista tieto- ja

viestintätekniikan käyttöä. Turvalliseen tietotekniikan käyttöön liittyy muun muassa hyvin suojattujen salasanojen käyttö, arkaluontoisen tiedon käsittely huolellisesti ja suojatusti sekä viestien ja liitteiden turvallisuuden arviointi (Kyberturvallisuuskeskus 2020). Tietoturvatiedoilla tarkoitetaan tässä tutkimuksessa henkilöstön tietopohjaa ja ymmärrystä tietoturvasta ja tietosuojasta, jotka auttavat toteuttamaan tietoturvallista toimintaa. Tietoturvatiedot ovat tärkeä tekijä, jonka on tunnistettu vähentävän tietoturvaloukkausten riskiä organisaatiossa (Safa & Von Solms 2016, 442). Tiedolla tarkoitetaan perusteltua uskomusta ja ymmärrettyä sekä sisäistettyä informaatiota (Tieteen termipankki 2016). Ammatillisena osaamisalueena tieto vaatii alakohtaisen tietopohjan, jonka avulla on mahdollista ymmärtää, hahmottaa ja arvioida työn ilmiöitä ja näkökulmia (Kangasniemi ym. 2018, 12). Tietoturvataidoilla tarkoitetaan tässä tutkimuksessa konkreettisia henkilöstön opittuja taitoja, joiden avulla voidaan toteuttaa tietoturvallista toimintaa. Taitoa pidetään yhtenä tiedon lajina, joka on toimintaa koskevaa tietoa (Tieteen termipankki 2016). Taidoilla tarkoitetaan opittua kykyä, jota yksilön on mahdollista käyttää tehokkaasti toimintaan. Ammattilaisten osaamisessa tiedot ja taidot tukevat toisiaan. Yksilö ymmärtää tarkoituksenmukaisen toimintatavan tilanteeseen tiedon avulla ja käyttää taitoa toiminnan toteuttamiseen. (Kangasniemi ym. 2018, 12.)



Kuvio 5. Tietoturvaosaamisen ydinalueet ja sisältö

Terveydenhuollon tietoturvaosaamisesta on tehty tutkimuksia kansainvälisesti vähäisesti. Aiemmat tutkimukset ovat keskittyneet enemmän teknisten ratkaisujen kehittämiseen yksityisyyden suojaamiseksi. Lisäksi on tutkittu terveystietotekniikan käytön vaikutusta hoidon laatuun. (Appari & Johnson 2010, 297–300; Kang & Seomun 2021, 17.) Tietoturvaosaaminen on kuitenkin noussut esille eri tiedonhallinnan tutkimuksissa yhtenä tiedonhallinnan osaamisen osa-alueena. Hübner tutkimusryhmineen (2018) on nostanut tietoturvaosaamisen yhdeksi kansainvälisen terveysinformatiikan osaamissuosituskehyksen kompetenssiksi tietotekniikan ydinosaamisalueella ja International Medical Informatics Association (IMIA) on reagoinut digitalisaation ja yhteiskunnan muutoksiin laatimalla päivitetyt suositukset tiedonhallinnan koulutustarpeista, joissa huomioidaan jokaisen roolin taidoissa tietoturvaosaaminen ja siihen liittyvän koulutuksen tärkeys (Bichel-Findlay ym. 2022, 2–10).

3.2 Tietoturvaosaamisen kehittäminen

Terveydenhuollon toimintaympäristön ja digitalisaation muutoksen vuoksi henkilöstön digitaalisen osaamisen kehittämiseksi tarvitaan laadukasta koulutusta (Bichel-Findlay ym. 2022, 2). Ihmiset ovat tärkeässä roolissa digitaalisen turvallisuuden tuottajana, jonka vuoksi tietoturvallisuus on riippuvainen tietoturvallisesta käyttäytymisestä. Osaamisen puutteen vuoksi henkilöstön koulutus on kuitenkin tärkeää tietoturvaosaamisen kehittämisessä ja organisaatioiden vastuulla on pitää huolta ammattilaisten tietoturvaosaamisen tason tunnistamisesta sekä täydennyskoulutuksesta. (Rhee, Kim & Ryu 2009, 817; STM 2019, 24; VM 2020, 21.) Lisäksi organisaatioiden on huolehdittava siitä, että henkilöstöllä on tarvittavat tiedot ja taidot sekä kunnossa olevat tietoturvakäytännöt. Tämän mahdollistamiseksi organisaation on tarjottava koulutusta henkilöstölle tietoturvan merkityksen ymmärtämisen lisäämiseksi. Tietoturva- ja tietosuojatyöhön on kannattavaa sijoittaa, sillä henkilöstön osaamiseen sijoittaminen näiden osa-alueiden osalta tuo organisaatiolle takaisin tuottoa, tehokkuutta sekä kustannussäästöjä. (Andreasson ym. 2016, 13.) Tietoturvakoulutuksen on osoitettu lisäävän terveydenhuollon ammattilaisten tietoisuutta tietoturvasta ja lisäävän positiivista vaikutusta tietoturvallisten toiminnan viemistä käytännön työhön (EunWon & Seomun 2021, 2).

Tietoturvaan perehdyttämisen tulee alkaa heti työsuhteen alusta ja olla osana henkilöstön työuraa. Työuran alussa perehdytysprosessiin tulee panostaa ja huomioida, ettei tietoturva- ja

tietosuoja-asiat jää vain vähäiselle huomiolle tai pelkän itseopiskelun varaan. (Andreasson ym. 2016, 52; STM 2019, 24.) Osaamisen puutteet voivat aiheuttaa ahdistusta ja epävarmuutta, jolloin työviihtyvyys heikkenee ja työteho laskee. Lisäksi tietoturva- ja tietosuojaosaamattomuus voi aiheuttaa organisaatiolle merkittävän turvallisuusuhan. (Andreasson ym. 2016, 13.) Perehdytyksen ja koulutuksen kautta tietoturvaosaaminen tulisi saada käytäntöön ja siihen sopivia on harjoitukset, jotka keskittyvät uhka-arvioihin, riskeihin, haavoittuvuuksiin sekä muihin tunnistettuihin kehittämiskohteisiin (STM 2019, 24). Lisäksi hyödyllisiä tapoja tietoturva- ja tietosuojaosaamisen perehdyttämiseen on henkilöstölle laaditut tietoturva- ja tietosuojaoppaat, intranetin kautta jaetut sisäiset ohjeet ja määräykset, verkkokurssit, luentokoulutukset, perehdytyksen ja ohjeiden ymmärtämisen kontrollointi, tietoturva- ja tietosuojasitoumukset sekä tietosuojavastaavan säännölliset tiedotteet (Andreasson ym. 2016, 53, 54). Myös EunWon tutkimusryhmineen (2021) suosittelee terveydenhuollon organisaatioiden tietoturvakäyttäytymisen ja henkilöstön tietoturvaosaamisen vahvistamista empiiristen ohjeiden kautta.

Perehdytyksen lisäksi tietoturvakäytäntöjen ja -ohjeiden noudattamiseksi on korostettu luottamuksen merkitystä. Organisaation huolehtiessa vahvan luottamuksen säilymisestä työntekijät ovat sitoutuneita noudattamaan tietoturvakäytäntöjä ja -ohjeita tietojen suojaamiseksi. Tuolloin työntekijät kokevat luottamusta työnantajan tietoturva- ja tietosuojaohjeita ja -käytäntöjä kohtaan ja osoittavat luottamustaan noudattamalla niitä. (Humaidi & Balakrishnan 2018, 18, 19.) Luottamuksen muodostuminen edellyttää positiivista työympäristöä ja tietoturva- ja tietosuojakulttuuria. Luottamusta lisääväksi tekijäksi on tunnistettu esihenkilötason tuki, joka lisää työntekijöiden kokemaa luottamusta tietoturva- ja tietosuojaohjeita kohtaan. Lisäksi luottamusta lisääviksi tekijöiksi on tunnistettu työnantajan tarjoamat koulutukset, selkeä ja helposti saatavilla oleva tietoturva- ja tietosuojaohjeistus, avoin ja kannustava keskustelu tietoturva- ja tietosuoja-asioista. (Humaidi & Balakrishnan 2018, 23, 24.)

4 Tutkimuksen tarkoitus ja tutkimuskysymykset

Tämän tutkimuksen tarkoituksena on tutkia kyselytutkimuksen avulla yksityisen terveydenhuollon henkilöstön tietoturva- ja tietosuojaosaamista.

Tutkimuskysymykset ovat:

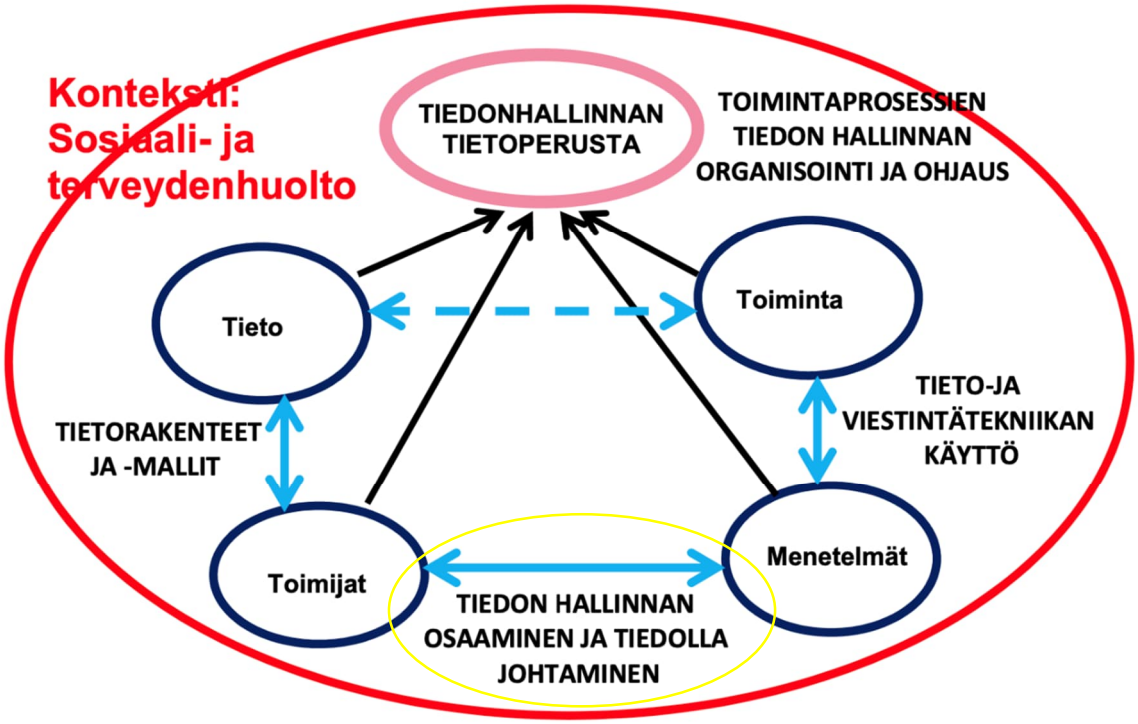
1. Mikä on henkilöstön tietoturva- ja tietosuojaosaamisen taso?
2. Mitä kehittämiskohteita on henkilöstön tietoturva- ja tietosuojaosaamisessa?

Lisäksi tutkimuksen tavoitteena on tunnistaa yksityisen terveydenhuollon henkilöstön tietoturva- ja tietosuojaosaamisen kehityskohteita osaamisen ja organisaation koulutuksen kehittämisen tueksi.

5 Tutkimuksen menetelmälliset lähtökohdat

5.1 Tutkimus osana sosiaali- ja terveydenhuollon tiedonhallinnan paradigmaa

Tiedonhallinnan paradigma on keskeinen menetelmällinen ja teoreettinen kehys sosiaali- ja terveydenhuollon tiedonhallinnan tutkimuksessa, jossa se toimii ohjaavana kokonaisuutena (Saranto & Kinnunen 2019, 210). Paradigmassa tiedonhallinnan lähestymisnäkökulmia kuvataan neljän keskeisen käsitteen eli entiteetin kautta, joita ovat toiminta, menetelmät, toimijat ja tieto (Kuvio 6). Käsitteeseen toiminta sisältyy sosiaali- ja terveydenhuoltopalvelujen suunnittelu, toteutus, käyttö ja arviointi. Käsiteellä menetelmät viitataan toiminnasta muodostuvien tietojen käsittelyn, välittämisen ja tallentamisen sosiaalisiin sekä teknisiin toimintatapoihin. Toimijat ovat palveluiden tuottajia, jotka tuottavat sosiaali- ja terveydenhuollon palveluita. Toimijat voivat olla myös niitä käyttäviä henkilöitä tai yhteisöjä. Käsiteellä tieto tarkoitetaan tiedon kuvautumista tiedon arvoketjun mukaisena hierarkkisena jatkumona, joka jalostuu datasta viisauteen. (Kuusisto-Niemi & Saranto 2009, 22.)



Kuvio 6. Sosiaali- ja terveydenhuollon tiedonhallinnan paradigma (Saranto & Kuusisto-Niemi 2012, 142)

Tämä pro gradu -tutkielma linkittyy sosiaali- ja terveydenhuollon tiedonhallinnan paradigmassa toimijat ja menetelmät osa-alueen välille tiedonhallinnan osaamisen ja tiedolla johtamisen osa-alueeseen. Kyseisen osa-alueen tutkimukset voivat liittyä esimerkiksi osaamisen kehittämiseen, henkilöstön valmiuksiin, koulutuksen suunnitteluun ja arviointiin, tiedon toisiokäyttöön, johtamiseen tai päätöksentekoon. (Saranto & Kinnunen 2019, 212.) Tässä tutkielmassa keskitytään erityisesti osaamisen arviointiin ja kehittämiseen. Mielenkiinto kohdistuu yksityisen terveydenhuollon henkilöstön tietoturva- ja tietosuojaosaamisen arviointiin sekä osaamisen kehityskohteiden tunnistamiseen, joiden perusteella voidaan arvioida tietoturva- ja tietosuojakoulutuksen kehitystarvetta.

5.2 Tutkimusympäristönä yksityinen terveydenhuolto

Yksityiset terveydenhuollon palvelut täydentävät julkisia terveydenhuollon palveluita niiden tarpeen kasvaessa väestön ikääntymisen myötä. Yksityisiä terveydenhuollon palveluita tuottaa yksityiset palveluntuottajat, eli yritykset, järjestöt ja säätiöt. Palveluntuottajat voivat myydä yksityisiä terveydenhuollon palveluita suoraan asiakkaille, kunnille tai kuntayhtymille. Yksityisen terveydenhuollon toimintaa ja palveluita ohjaa sosiaali- ja terveysministeriö sekä yksityistä terveydenhuoltoa koskevat lait ja asetukset. Sen lisäksi yksityisen terveydenhuollon valvonnassa pääasiallisessa vastuussa on aluehallintavirasto ja koordinaatiovastuussa sosiaali- ja terveysalan lupa- ja valvontavirasto Valvira. (STM 2022.)

Yksityiset sosiaali- ja terveydenhuollon palveluntuottajat tuottavat reilun neljänneksen Suomen sosiaali- ja terveyspalveluista, jotta lisääntyneeseen palveluiden tarpeeseen pystytään vastaamaan. Yleisimpiä yksityisiä terveyspalveluita on lääkärin ja hammaslääkärin vastaanottotoiminta, työterveyshuolto sekä fysioterapiapalvelut. (STM 2022.) Yksityisiä terveydenhuollon palveluita tuottaessa tulee palveluntuottajalla olla toiminnan edellyttämää henkilökuntaa ja asianmukaiset tilat sekä laitteet. Toiminnan tulee olla lääketieteellisesti asianmukaista ja siinä tulee huomioida potilasturvallisuus. (Laki yksityisestä terveydenhuollosta 152/1990.)

Tutkimuksen kohderyhmäksi valittiin mukaan yksityisen terveydenhuollon organisaation useampien yksiköiden terveydenhuollon ammattilaisia eri puolelta Suomea. Organisaation

suuri koko vaikutti kohderyhmän valintaan, jonka vuoksi kaikkia organisaation terveydenhuollon ammattilaisia ei ollut mahdollista valita mukaan. Lisäksi kohderyhmän valintaan vaikutti myös tutkimuksen kohdistuminen yksityisiin terveyspalveluihin, jolloin kohderyhmästä rajautui pois muun muassa organisaation sosiaalipalvelut. Kohderyhmän valinnassa ei huomioitu erikseen sitä, onko henkilö suorittanut organisaation järjestämän tietoturva- ja tietosuojakoulutuksen, koska se on lähtökohtaisesti pakollinen koko henkilöstölle. Organisaatio esiintyy tutkimuksessa anonyyminä.

5.3 Tutkimusmenetelmät ja aineiston keruu

Tutkimusmenetelmänä tässä tutkimuksessa käytettiin kvantitatiivista eli määrällistä tutkimusta. Kvantitatiivinen tutkimus selvittää prosenttiosuuksiin sekä lukumääriin liittyviä kysymyksiä, jonka vuoksi sitä voidaan kutsua myös tilastolliseksi tutkimukseksi. Se sopii tutkimusmenetelmäksi olemassa olevien tilanteiden kartoittamiseen, mutta ei asioiden syiden selvittämiseen. Kvantitatiiviseen tutkimukseen tiedot voidaan hankkia valmiista aineistoista tai kerätä itse, kuten tässä tutkimuksessa on tehty. (Heikkilä 2014, 15.)

Tutkimusaineiston keruu toteutettiin sähköisellä standardoidulla kyselyllä, joka on yleinen aineistonkeruun menetelmä kvantitatiivisessa tutkimuksessa (Heikkilä 2014, 15). Kyselylomakkeisiin perustuva tiedonkeruu perustuu kolmeen vaiheeseen: lomakkeen rakentamiseen, tutkittavien yksiköiden valintaan ja tiedonkeruumenetelmän valintaan. Lomakkeen suunnittelussa tulee olla näkemys siitä, mitä tutkitaan ja keneltä aineisto kerätään. (Alastalo & Borg 2010.) Näiden vaiheiden perusteella tiedonkeruuta varten suunniteltiin sähköinen standardoitu kyselylomake, valittiin tutkittavat yksiköt kyselyyn sekä päätettiin tiedonkeruumenetelmäksi tutkimuskyselyyn vastaaminen verkossa sähköisen nettilinkin kautta. Kyselylomakkeen ulkonäössä ja toiminnallisuudessa pyrittiin selkeyteen ja se laadittiin Itä-Suomen yliopiston alaisella Webropol-sovelluksella. Lisäksi kyselylomakkeesta laadittiin kohtuullisen pituinen, jotta vastausaika ei ylity liian pitkäksi. Vastausajaksi arvioitiin kyselylomakkeen testauksen avulla 15–20 minuuttia. Ylipitkä kysely voi vähentää vastaushalua, jonka vuoksi vastausajan ei tulisi ylittää 15–20 minuuttia (Alastalo & Borg 2010).

Kyselyn tutkittavat yksiköt ja niihin sopivat kysymykset laadittiin hyödyntäen tutkimuksessa käytettyä Staggersin ja hänen tutkimusryhmänsä (2002a) teoreettista viitekehystä sekä tässä tutkimuksessa käsiteltyä teoriatietoa. Keskeisiksi osaamisen tutkittaviksi osa-alueiksi valikoitui tietoturva- ja tietosuojaosaamiseen liittyvät teemat: turvalliset tietotekniikan käyttötaidot, tietoturvatiedot ja tietoturvataidot, jotka on mukailtu Staggersin ja hänen tutkimusryhmänsä (2002a) hoitotyön tiedonhallinnan ydinosaamisalueista tietotekniikan käyttötaidot, tiedonhallinnan tiedot ja tiedonhallinnan taidot. Lisäksi taustatietojen ja osaamisen ydinalueiden lisäksi teemaksi valikoitui koulutuksen kehityksen näkökulmasta kysymyksiä organisaation tietoturva- ja tietosuojakoulutuksesta. Kyselyyn laadittiin 32 strukturoitua eli suljettua yhden vastauksen monivalintakysymystä ja yksi avoin kysymys. Kyselylomake koostui kuudesta osiosta: taustatiedot, koulutustausta, turvalliset tietotekniikan käyttötaidot, tietoturvatiedot, tietoturvataidot ja organisaation tietoturva- ja tietosuojakoulutus (Taulukko 2). Suljettuja kysymyksiä suosittiin niiden yksinkertaisuuden ja nopean vastausmahdollisuuden vuoksi. Lisäksi kyselyyn luotiin täydentäväksi kysymykseksi yksi koulutustoiveisiin liittyvä avoin kysymys, joka mahdollisti kohdejoukon toiveiden kuulemisen. (Heikkilä 2014, 47–49.) Kyselyllä haettiin vastauksia molempiin tutkimuksen tutkimuskysymyksiin.

Taulukko 2. Kyselylomakkeen osiot

Staggersin ym. (2002a) tiedonhallinnan ydinosaamisen alue	**Kysymysten osiot**	**Kysymykset**
	Taustatiedot	1–3
	Koulutustausta	4–8
Tietotekniikan käyttötaidot	Turvalliset tietotekniikan käyttötaidot	9–14
Tiedonhallinnan tiedot	Tietoturvatiedot	15–20
Tiedonhallinnan taidot	Tietoturvataidot	21–28
	Organisaation tietoturva- ja tietosuojakoulutus	29–33

Vastausasteikkojen laadinnassa hyödynnettiin perusperiaatteena symmetrisyyttä sekä kattavuutta. Symmetrisyydellä tarkoitetaan myönteisten ja kielteisten vaihtoehtojen yhtä suuri määrä. Kattavuudella tarkoitetaan, että asteikot vastaavat ihmisten kykyä arvioida tutkittavaa asiaa. Vaihtoehtojen täydellisyys ja toistensa poissulkevuus ovat tärkeitä, kun vastaaja saa valita vain yhden vaihtoehdon. Liiallinen vaihtoehtojen määrä johtaa tulosten näennäistarkkuuteen.

(Alastalo & Borg 2010.) Vastausasteikoksi valikoitui 5-asteinen Likertin asteikko. Vastausvaihtoehdoiksi annettiin pääsääntöisesti 1 = Täysin eri mieltä, 2 = Osittain eri mieltä, 3 = Ei samaa eikä eri mieltä, 4 = Osittain samaa mieltä ja 5 = Täysin samaa mieltä. Kysymyksissä 9 ja 29 kuitenkin vastausvaihtoehtojen sanamuodot erosivat kysymyksen luonteen vuoksi ja vaihtoehdot olivat 1 = En koskaan / 1 = Ei ollenkaan, 2 = Harvoin / 2 = Vähän, 3 = Joskus / 3 = En osaa sanoa, 4 = Usein / 4 = Jonkin verran ja 5 = Aina / 5 = Paljon.

Kyselytutkimus testattiin ennen sen virallista lähetystä kohdejoukolle ulkopuolisella testiryhmällä N = 5. Osa jäsenistä oli terveydenhuollon ammattilaisia ja osa muun alan ammattilaisia. Testaukseen valittiin tarkoituksella mukaan henkilöitä myös terveydenhuoltoalan ulkopuolelta, jotta palautetta saatiin mahdollisimman erilaisista taustoista tulevilta henkilöiltä ja kyselylomakkeesta saatiin luotua mahdollisimman selkeä ja ymmärrettävä. Testiryhmän tehtävänä oli antaa palautetta kyselyn kysymysten selkeydestä ja kysymysasettelusta sekä havainnoida vastaamiseen kuluvaa aikaa. Palautteiden jälkeen kyselytutkimuksen kysymyksenasetteluita ja sanamuotoja muokattiin selkeämmäksi. Lisäksi saatekirjettä muokattiin tiiviimmäksi ja ymmärrettävämmäksi kokonaisuudeksi. Kyselyn testauksen jälkeen vastauslinkki lähetettiin sähköpostitse kohderyhmälle helmikuussa 2023 ja vastausaikaa kyselylle annettiin alkuun kolme viikkoa. Kyselyn vastausajan päätyttyä vastauksia oli tullut 25, joten vastausaikaa päädyttiin vielä pidentämään viikolla ja muistuttamaan kohdejoukkoa kyselyyn vastaamisesta. Kyselyn lähetys ja muistutukset ulkoistettiin tietoturva- ja tietosuojasyistä organisaation sisäiselle henkilöstölle.

5.4 Aineiston analyysi

Kyselyaineistoihin perustuvien tutkimusten analyysimenetelmät riippuvat tiedon käyttötarkoituksesta. Yleisimpiä analyysimenetelmiä survey-tutkimuksissa on kuvailevat tilastolliset menetelmät. (Alastalo & Borg 2010.) Kyselytutkimuksissa kysymykset esitetään sanallisesti, mutta kyselyaineistot koostuvat kuitenkin usein mitatuista luvuista ja numeroista. Sen vuoksi niiden analysointiin soveltuu tilastolliset menetelmät (Vehkalahti 2019, 13). Tutkimusaineiston suljettujen kysymysten vastaukset analysoitiin hyödyntäen IMB SPSS-statistics 27 tilasto-ohjelmaa ja määrällisen tutkimuksen analysointimenetelmiä. Lisäksi tutkimusta täydentävä avoin kysymys analysoitiin sisällönanalyysin keinoin hyödyntäen

teemoittelua. Teemoittelu on yksi laadullisen tutkimusmenetelmän sisällönanalyysin muoto ja sen avulla aineistosta paikannetaan tutkimusongelman kannalta olennaiset teemat. Teemat tarkoittavat toistuvia asioita aineistossa. Niiden paikantamiseksi nostetaan esiin keskeisiä asiakokonaisuuksia ja tyypillisiä piirteitä tutkimusongelman kannalta. (Juhila 2023.)

Aineistonkeruu toteutettiin Itä-Suomen yliopiston alaisella Webropol-ohjelmalla, johon myös kyselyn vastaukset tallentuivat. Analysoitava aineisto vietiin suoraan Webropol-ohjelmasta Excel-taulukkolaskentaohjelmaan sekä SPSS-statistics 27 tilasto-ohjelmaan analysointia varten. Tutkimusaineiston koko (n = 39) vaikutti aineiston analyysimenetelmän valintaan, joten analysoinnissa hyödynnettiin kuvailevia tilastollisia menetelmiä. Sen avulla analysoidut tulokset ovat helposti ymmärrettäviä ilman laajoja taustatietoja (Alastalo & Borg 2010). Analyysia varten aineisto koodattiin uudelleen Likert-asteikosta kolmiasteiseen muotoon selkeämmän tilastollisen kuvailun vuoksi (Taulukko 3).

Taulukko 3. Likert-asteikon muuttujien uudelleenkoodaus

Alkuperäinen arvo	**Uusi arvo**
1 = Täysin eri mieltä	1 = Eri mieltä
2 = Osittain eri mieltä	1 = Eri mieltä
3 = Ei samaa eikä eri mieltä	2 = Ei samaa eikä eri mieltä
4 = Osittain samaa mieltä	3 = Samaa mieltä
5 = Täysin samaa mieltä	3 = Samaa mieltä

Tyypillisiä tunnuslukuja on frekvenssit eli tapausten lukumäärät, aritmeettiset keskiarvot, muut keskiluvut, prosenttiosuudet ja hajontaluvut (Alastalo & Borg 2010). Aineistosta analysoitiin keskeisiksi tunnusluvuiksi havaintojen lukumäärä (n), keskiarvo (ka), mediaani (md), moodi (mo) ja keskihajonta (SD). Lisäksi aineiston analysoinnissa hyödynnettiin ristiintaulukointia vaikutussuhteiden analysoimiseksi. Tulosten havainnollistamiseksi käytettiin taulukoita ja kuvioita, jotka ovat yleinen havainnollistamisen tapa kvantitatiivisessa tutkimuksessa (Heikkilä 2014, 15).

Tulosten analysoinnin jälkeen henkilöstön tietoturva- ja tietosuojaosaaminen luokiteltiin osaamisen tasoille 1 ja 2 ydinaluekohtaisesti. Luokittelu tehtiin vastausten keskiarvojen

perusteella hyödyntäen Krugerin ja Kearneyn (2006) mittausmenetelmän mukaisia prosenttiosuuksia 0–59 %, 60–79 % ja 80–100 % (Taulukko 4). Kyselyn vastausten suurin arvo oli 3, joten keskiarvon ollessa yli 80 % (yli 2.4) oli kyseessä tason 2 osaaminen eli hyvät tiedot ja taidot tietoturvasta. Keskiarvon ollessa 60–79 % (1.8–2.3) oli kyseessä tason 1 osaaminen eli perustiedot ja -taidot tietoturvasta. Keskiarvon ollessa alle 59 % (alle 1.8) oli kyseessä perustietoja ja -taitoja heikompi osaaminen, joka ei sijoitu osaamisen tasoille 1 tai 2.

Taulukko 4. Osaamisen luokittelu mittaustulosten perusteella

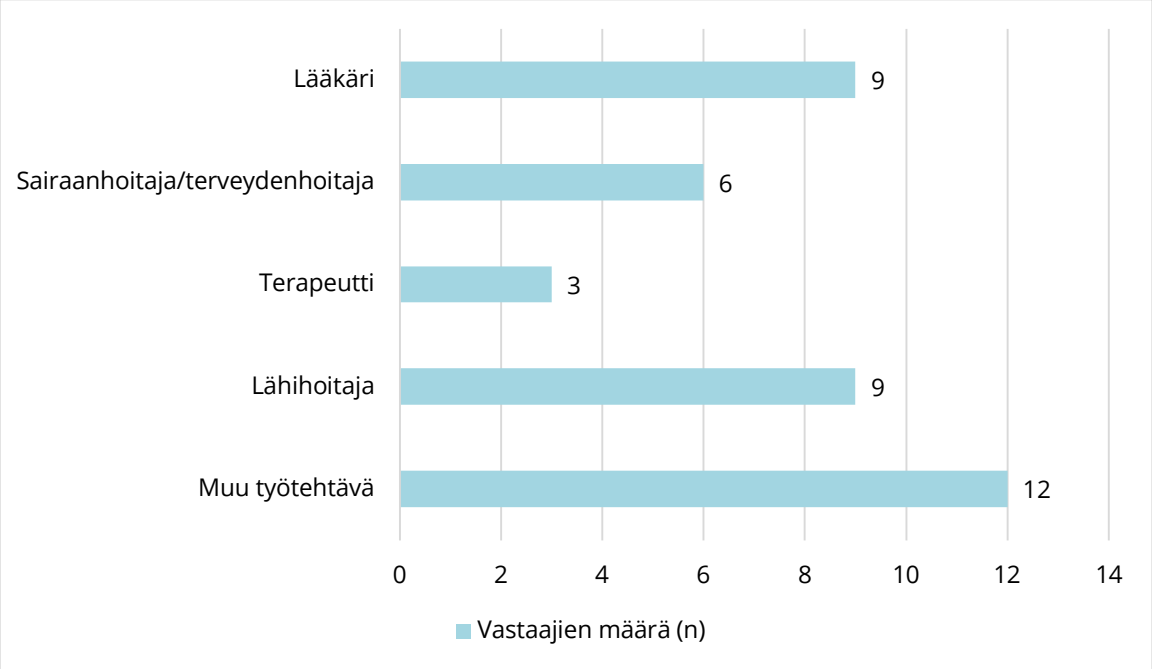
Mittaustulos	**Sijoittuminen osaamisen tasolle**	**Tietoturvaosaaminen**
80–100 %	Taso 2	Hyvät tiedot ja taidot tietoturvasta
60–79 %	Taso 1	Perustiedot ja -taidot tietoturvasta
0–59 %	Ei sijoitu osaamisen tasolle	Perustietoja ja -taitoja heikompi osaaminen

Ydinaluekohtaiset keskiarvot analysoitiin laskemalla vastausten keskiarvot yhteen ja jakamalla kysymysten määrällä. Tulokseksi saatiin keskiarvo, jonka perusteella ydinalueen osaaminen sijoitettiin oikealle osaamisen tasolle. Tulosten luokittelussa huomioitiin myös päinvastaiset kysymykset, joiden paras arvo on 1 ja huonoin 3. Tuolloin keskiarvo muutettiin käänteiseksi.

6 Tulokset

6.1 Vastaajien taustatiedot

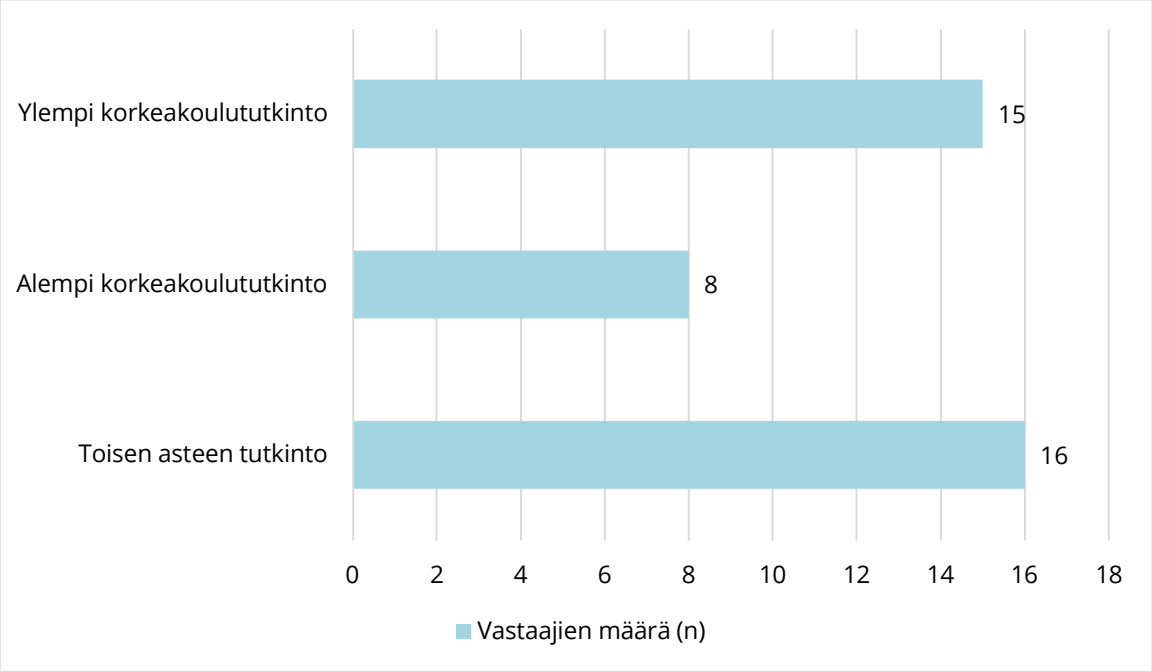
Tutkimuskyselyyn vastasi 39 henkilöä. Kaikki vastaajat eivät kuitenkaan vastanneet jokaiseen kysymykseen, vaan osaan kysymyksistä vastasi 38 henkilöä. Suurin osa vastaajista, 31 % (n = 12) työskentelee organisaatiossa muussa työtehtävässä (Kuvio 7). Kyseiseen ryhmään sisältyy yksiköiden johtajat, esihenkilöt ja muut yksikön työntekijät, joiden työtehtävä ei ole mikään muista vastausvaihtoehtojen työtehtävistä. Toisiksi eniten vastaajista oli lääkäreitä 23 % (n = 9) ja lähihoitajia 23 % (n = 9). Sairaanhoitajien/terveydenhoitajien osuus vastaajista oli 15 % (n = 6) ja terapeuttien osuus oli 8 % (n = 3).



Kuvio 7. Kyselyyn vastanneiden työtehtävä organisaatiossa (n)

Suurin osa, 72 % (n = 28) kyselyyn vastanneista työskenteli organisaatiossa vakituisessa työsuhteessa. Lisäksi 23 % (n = 9) työskenteli organisaatiossa ammatinharjoittajana ja 5 % (n = 2) määräaikaisessa työsuhteessa. Työuran pituus tutkimuksen kohteena olevassa yksityisen terveydenhuollon organisaatiossa painottui 0–5 vuoteen 51 % (n = 20) ja 5–10 vuoteen 23 % (n = 9). Lisäksi 10–15 vuoden työuria oli 10 % (n = 4) vastaajista ja 15–20 vuoden sekä yli 20-vuoden työuria oli molempia 8 % (n = 3) vastaajista.

Tutkimuskyselyn toisena taustatietojen osa-alueena oli koulutustausta, johon sisältyi kysymyksiä ammatillisesta koulutuksesta, tietoturva ja tietosuojakoulutuksesta sekä ammatillisessa koulutuksessa että organisaation koulutuksessa. Vastaajista suurimman osan, 41 % (n = 16) ammatillinen koulutus oli toisen asteen tutkinto (Kuvio 8). Toisiksi suurin 38 % (n = 15) koulutustausta oli ylempi korkeakoulututkinto. Lisäksi vastaajista 21 % (n = 8) ammatillinen koulutus oli alempi korkeakoulututkinto.



Kuvio 8. Kyselyyn vastanneiden ammatillinen koulutustausta (n)

Ammatilliseen koulutukseen on sisältynyt tietoturvaan ja tietosuojaan liittyviä opintoja 67 % (n = 26) vastanneista jonkin verran, 15 % (n = 6) vastanneista vähän ja 8 % (n = 3) vastanneista paljon. Ammatillisiin opintoihin ei ole sisältynyt ollenkaan tietoturvaan ja tietosuojaan liittyviä opintoja 8 % (n = 3) vastanneista ja 2 % (n = 1) vastanneista ei osaa sanoa kuinka paljon niitä on sisältynyt opintoihin.

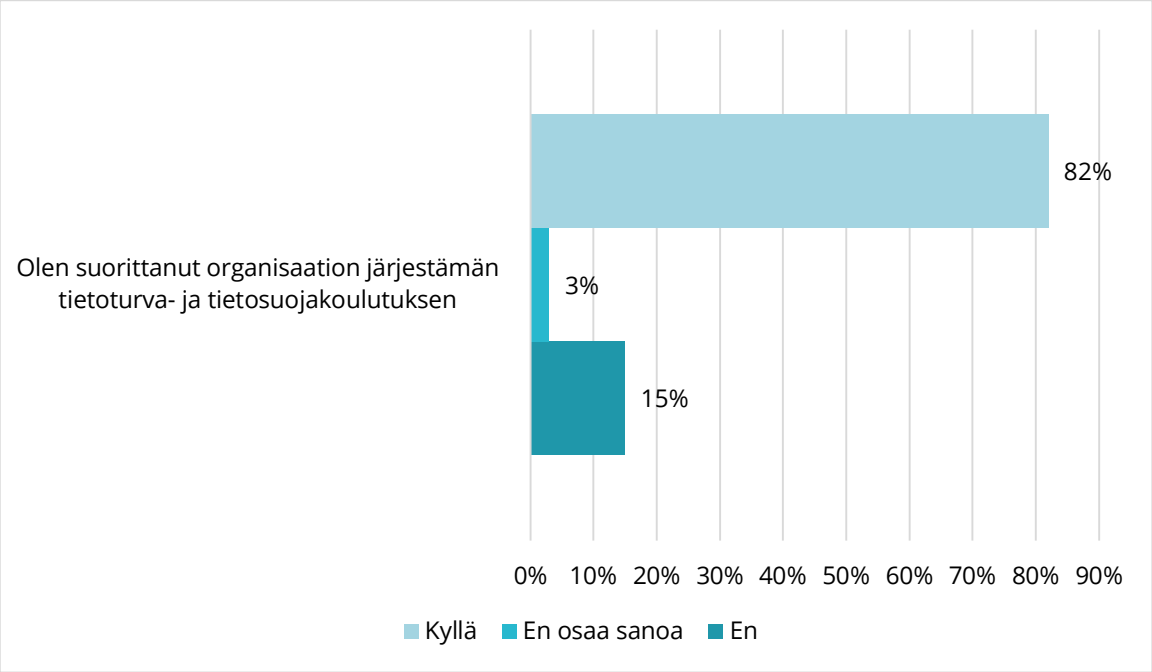
Ammatilliseen koulutukseen sisältyneiden tietoturva- ja tietosuojaopintojen määrän jakautumista eri koulutuksiin tarkastellaan taulukossa 5. Ylemmän ja alemman korkeakoulututkinnon sekä toisen asteen tutkinnon koulutuksiin on vastaajien mukaan sisältynyt tietoturva- ja tietosuojaopintoja. Alemman korkeakoulun tutkinnon suorittaneista 87.5 %, toisen asteen tutkinnon suorittaneista 75 % ja ylemmän korkeakoulun tutkinnon suorittaneista 66.5 % arvioi tietoturva- ja tietosuojaopintoja olleen ammatillisessa

koulutuksessa jonkin verran tai paljon. Sen sijaan ylemmän korkeakoulututkinnon suorittaneista 33.5 %, toisen asteen tutkinnon suorittaneista 19 % ja alemman korkeakoulututkinnon suorittaneista 12.5 % arvioi, ettei opintoja ole sisältynyt koulutukseen ollenkaan tai niitä on sisältynyt vähän. Eniten tietoturva- ja tietosuojaopintoja on sisältynyt vastaajien arvion mukaan alempaan korkeakoulututkintoon ja vähiten tai ei ollenkaan ylempään korkeakoulututkintoon.

Taulukko 5. Ammatilliseen koulutukseen sisältyvien tietoturva- ja tietosuojaopintojen määrän jakautuminen eri koulutuksissa (%)

Koulutustausta	Ei ollenkaan	Vähän	En osaa sanoa	Jonkin verran	Paljon
Ylempi korkeakoulututkinto	6.5	27	0	60	6.5
Alempi korkeakoulututkinto	12.5	0	0	87.5	0
Toisen asteen tutkinto	6	13	6	62	13

Organisaation järjestämän pakollisen tietoturva- ja tietosuojakoulutuksen on suorittanut 82 % (n = 32) eli suurin osa vastaajista (Kuvio 9). Koulutusta ei ole suorittanut ollenkaan 15 % (n = 6) vastaajista ja 3 % (n = 1) ei osaa sanoa onko suorittanut koulutusta. Organisaation tietoturva- ja tietosuojakoulutuksen suorittamatta jättäneistä 50 % (n = 3) vastasi kysymykseen koulutuksen suorittamatta jättämisen syystä. Vastaajista 67 % (n = 2) on sitä mieltä, että koulutuksen suorittamatta jättämisen syynä on muu syy ja 33 % (n = 1) ei ole ollut tietoinen koulutuksesta.

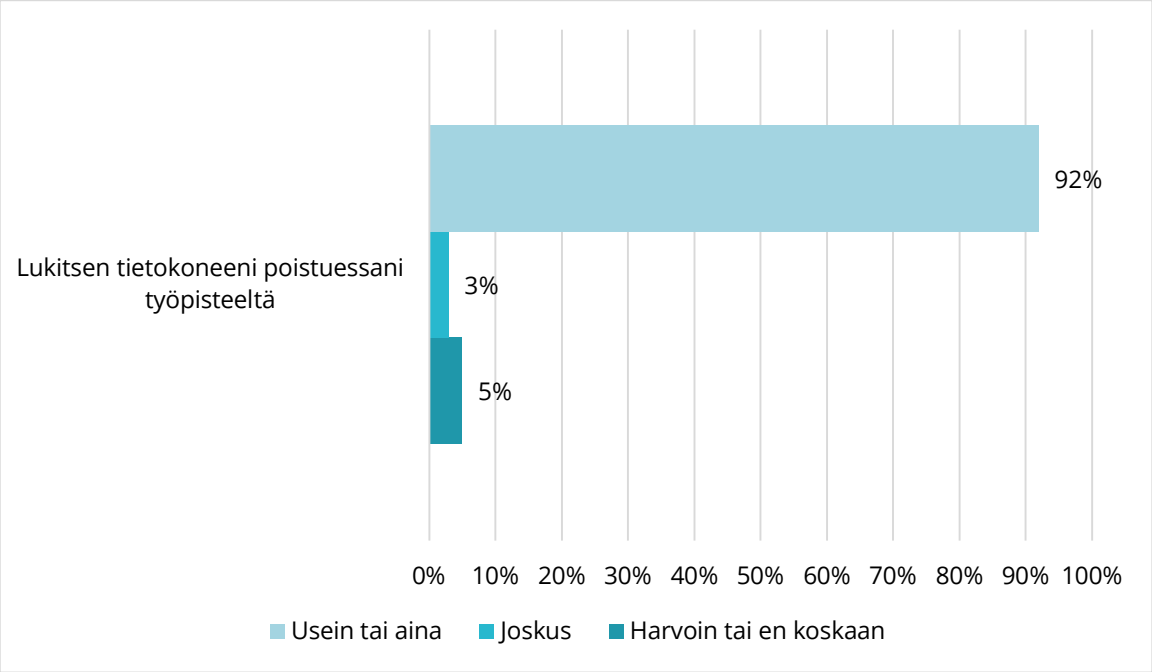


Kuvio 9. Organisaation järjestämän tietoturva- ja tietosuojakoulutuksen suorittaneet vastaajat (%)

Organisaation järjestämien koulutusten lisäksi ulkopuolisia tietoturva- ja tietosuoja koulutuksia on vastaajista 54 % (n = 21) eli suurin osa suorittanut jonkin verran. Vähän ulkopuolisia tietoturva- ja tietosuojakoulutuksia on suorittanut 23 % (n = 9) vastaajista ja 20 % (n = 8) ei ole suorittanut ollenkaan. Vastaajista 3 % (n = 1) ei osaa sanoa, onko suorittanut ulkopuolisia koulutuksia aiheesta.

6.2 Turvallisten tietotekniikan käyttötaitojen osaaminen

Turvallisia tietotekniikan käyttötaitoja osana tietoturva- ja tietosuojaosaamista tarkastellaan työvälineisiin, salasanoihin ja sähköpostin liitetiedostoihin liittyvien kysymysten avulla. Vastaajista 60 % (n = 23) lukitsee tietokoneen aina poistuessaan työpisteeltään ja 32 % (n = 12) lukitsee usein (Kuvio 10). Yksi vastaaja (3 %) lukitsee taas joskus ja kaksi vastaajaa (5 %) ei koskaan.



Kuvio 10. Tietokoneen lukitsevat vastaajat (%)

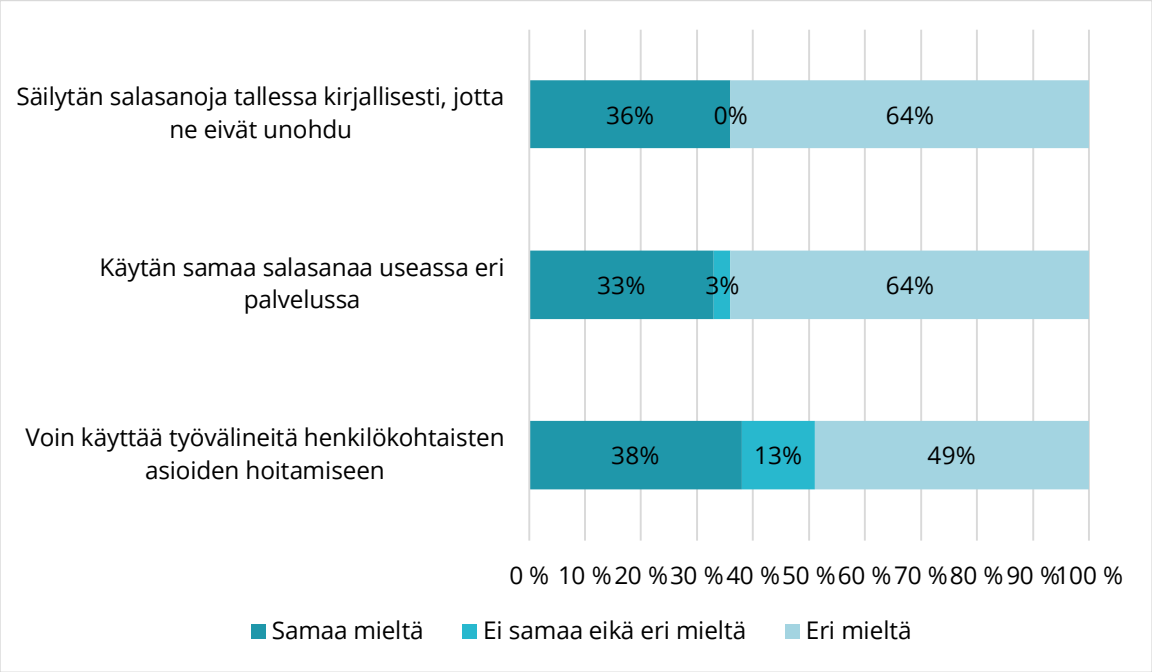
Turvallisten tietotekniikan käyttötaitojen osaamisessa (Taulukko 6) esiintyi korkein keskiarvo 2.9 kysymyksessä ”Käytän työssäni vain organisaation määrittämiä työvälineitä” keskihajonnalla 0.3. Toiseksi suurin keskiarvo esiintyi kysymyksessä ”Voin käyttää työvälineitä henkilökohtaisten asioiden hoitamiseen” keskiarvolla 1.9 ja keskihajonnalla 0.9. Tietoturvaan olennaisesti liittyvien käytännön toimien osalta salasanaan liittyvät kysymykset ”Käytän samaa salasanaa useassa eri palvelussa” ja ”Säilytän salasanoja tallessa, jotta ne eivät unohdu” saivat molemmat keskiarvon 1.7. Salasanoihin liittyvät keskihajonnat olivat väliltä 0.9–1.0. Alhaisin keskiarvo 1.0 esiintyi kysymyksessä ”Voin ladata huoletta tuntemattoman lähettäjän sähköpostin liitetiedoston” keskihajonnalla 0.2.

Taulukko 6. Turvallisten tietotekniikan käyttötaitojen osaaminen n (%)

Kysymys	n	ka	md	mo	SD	Eri mieltä	Ei samaa eikä eri mieltä	Samaa mieltä
10. Käytän työssäni vain organisaation määrittämiä työvälineitä	39	2.9	3	3	0.3	1 (3)	0 (0)	38 (97)
11. Voin käyttää työvälineitä henkilökohtaisten asioiden hoitamiseen	39	1.9	2	1	0.9	19 (49)	5 (13)	15 (38)
12. Käytän samaa salasanaa useassa eri palvelussa	39	1.7	1	1	0.9	25 (64)	1 (3)	13 (33)
13. Säilytän salasanoja tallessa kirjallisesti, jotta ne eivät unohdu	39	1.7	1	1	1.0	25 (64)	0 (0)	14 (36)
14. Voin ladata huoletta tuntemattoman lähettäjän sähköpostin liitetiedoston	39	1.0	1	1	0.2	38 (97)	1 (3)	0 (0)

1 = Eri mieltä, 2 = Ei samaa eikä eri mieltä, 3 = Samaa mieltä

Lähes kaikki 97 % (n = 38) vastaajista käyttää työssään vain organisaation määrittämiä työvälineitä ja ovat samaa mieltä siitä, ettei tuntemattoman lähettäjän sähköpostiviestin liitetiedostoa voi ladata huoletta. Eniten eroavaisuuksia vastauksissa on salasanoihin liittyvissä kysymyksissä ja työvälineiden käytössä henkilökohtaisten asioiden hoitamiseen (Kuvio 11). Salasanojen osalta 64 % (n = 25) vastaajista ei käytä samaa salasanaa useassa eri palvelussa, eikä säilytä salasanoja tallessa kirjallisesti. Vastaajista puolestaan 33 % (n = 13) käyttää samaa salasanaa ja 36 % (n = 14) säilyttää salasanoja tallessa kirjallisesti, jotta ne eivät unohdu. Vastaajista 49 % (n = 19) ei käytä työvälineitä henkilökohtaisten asioiden hoitamiseen ja 38 % (n = 15) puolestaan käyttää.



Kuvio 11. Turvallisten tietotekniikan käyttötaitojen kehityskohteet

Turvallisten tietotekniikan käyttötaitojen ydinalueen kysymysten (10–14) vastausten keskiarvo oli 2.52 (Taulukko 7). Käänteisten kysymysten (11–14) osalta keskiarvot käännettiin vastaamaan asteikkoa, jossa arvo 3 on suurin mahdollinen arvo. Keskiarvon ollessa 80–100 % eli yli 2.4 on kyseessä tason 2 osaaminen. Tasolla 2 henkilöstöllä on hyvät tiedot ja taidot tietoturvasta.

Taulukko 7. Turvallisten tietotekniikan käyttötaitojen osaamisen taso

Kysymys	**Ydinalueen vastausten keskiarvo**	**Sijoittuminen osaamisen tasolle**
10. 11. 12. 13. 14.	2.9 1.9 -> 2.1 1.7 -> 2.3 1.7 -> 2.3 1.0 -> 3.0	
	= 2.52	**Taso 2**

Vastausten perusteella turvallisten tietotekniikan käyttötaitojen ydinalueen osaaminen on hyvällä tasolla. Vahvin osaaminen oli liitetiedostojen turvallisuuden huomioimisessa sekä työvälineiden käyttämisessä työtehtäviin. Vahva osaaminen oli myös työpisteen turvallisuuden huomioimisessa lukitsemalla tietokone työpisteeltä poistuessa. Suurimmat kehityskohteet olivat salasanoihin liittyvät käytännöt sekä työvälineiden käyttö henkilökohtaisten asioiden hoitamiseen.

6.3 Tietoturvatietojen osaaminen

Tietoturvatietojen osaamista tarkastellaan tietoturvan ja tietosuojan käsitteiden ymmärtämisen, oman osaamisen arvioinnin sekä tietämyksen kautta (Taulukko 8). Kysymyksessä ”Tiedän mitä tietoturva tarkoittaa” esiintyi korkein keskiarvo 3.0 keskihajonnalla 0.2. Toisiksi korkein keskiarvo 2.9 esiintyi kysymyksessä ”Tiedän mitä tietosuoja tarkoittaa” keskihajonnalla 0.2 ja kysymyksessä ”Minulla on mielestäni riittävä tietoturva- ja tietosuojaosaaminen” keskihajonnalla 0.4. Kysymyksen ”Tiedän miten toimia tilanteissa, joissa tietoturva tai tietosuoja on vaarantunut” keskiarvo oli 2.7 ja keskihajonta 0.6. Heikoin keskiarvo 2.6 keskihajonnalla 0.8 esiintyi kysymyksessä ”Tiedän keneltä voin kysyä apua tietoturva- ja tietosuoja-asioissa” ja kysymyksessä ”Tiedän mistä löydän organisaation kirjalliset tietoturva- ja tietosuojaohjeet”.

Taulukko 8. Tietoturvatietojen osaaminen n (%)

Kysymys	n	ka	md	mo	SD	Eri mieltä	Ei samaa eikä eri mieltä	Samaa mieltä
15. Tiedän mitä tietoturva tarkoittaa	39	3.0	3	3	0.2	0 (0)	1 (3)	38 (97)
16. Tiedän mitä tietosuoja tarkoittaa	39	2.9	3	3	0.2	0 (0)	2 (5)	37 (95)
17. Minulla on mielestäni riittävä tietoturva- ja tietosuojaosaaminen	38	2.9	3	3	0.4	1 (3)	2 (5)	35 (92)
18. Tiedän keneltä voin kysyä apua tietoturva- ja tietosuoja-asioissa	38	2.6	3	3	0.8	6 (16)	2 (5)	30 (79)
19. Tiedän miten toimia tilanteissa, joissa tietoturva tai tietosuoja on vaarantunut	38	2.7	3	3	0.6	4 (11)	2 (5)	32 (84)
20. Tiedän mistä löydän organisaation kirjalliset tietoturva- ja tietosuojaohjeet	39	2.6	3	3	0.8	6 (15)	3 (8)	30 (77)

1 = Eri mieltä, 2 = Ei samaa eikä eri mieltä, 3 = Samaa mieltä

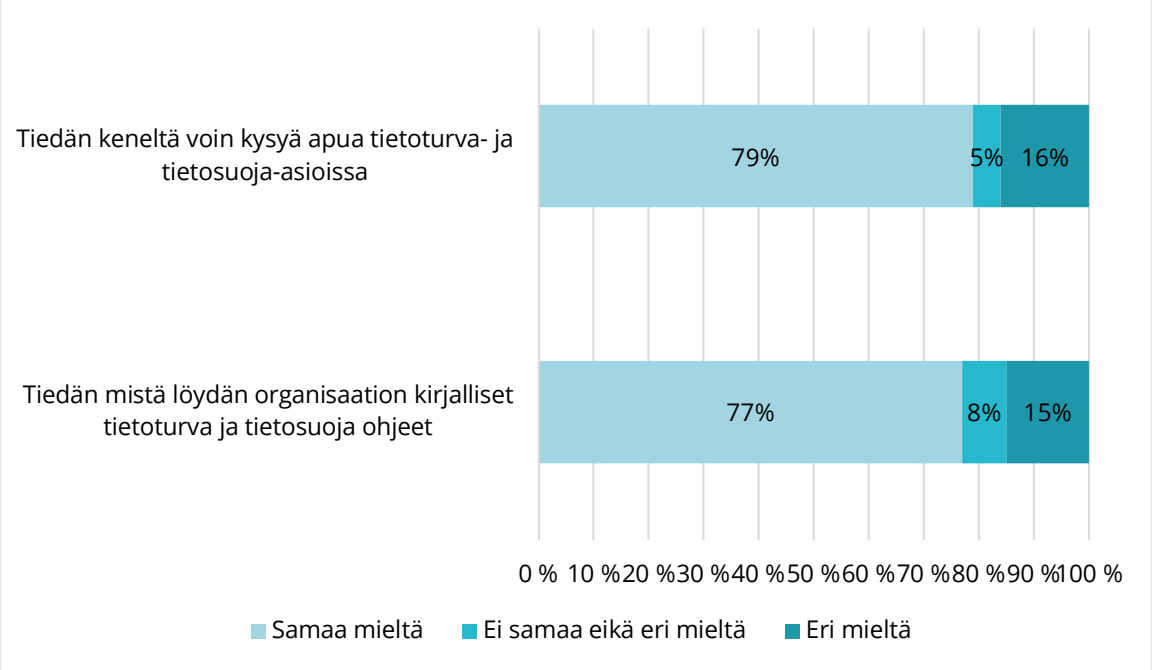
Lähes kaikki vastaajat 97 % (n = 38) tietävät mitä tietoturva tarkoittaa ja 95 % (n = 37) tietävät mitä tietosuoja tarkoittaa. Lisäksi 92 % (n = 35) arvioi oman tietoturva- ja tietosuojaosaamisensa riittäväksi. Tämän kysymyksen ollessa yksi keskeisimmistä tutkimuksen kannalta, tarkastellaan osaamisen kokemuksen jakautumista eri työtehtäviin tarkemmin (Taulukko 9). Oman tietoturva- ja tietosuojaosaamisen koki riittäväksi kaikki kyselyyn vastanneet lääkärit ja muussa

työtehtävässä työskentelevät henkilöt. Heikoimmaksi puolestaan oman osaamisensa arvioi terapeuttina työskentelevät henkilöt.

Taulukko 9. Riittävän tietoturva- ja tietosuojaosaamisen kokemus eri työtehtävissä

Työtehtävä	Eri mieltä	Ei samaa eikä eri mieltä	Samaa mieltä
Lääkäri	0	0	100
Sairaanhoitaja/terveydenhoitaja	0	17	83
Terapeutti	33	0	67
Lähihoitaja	0	11	89
Muu	0	0	100

Eniten eroavaisuuksia tietoturvatietojen ydinalueessa on tietämyksessä, missä organisaation kirjalliset tietoturva ja tietosuojaohjeet sijaitsevat sekä siinä, miten toimia tietoturvan tai tietosuojan vaarantuessa. Vastaajista 15 % (n = 6) ei tiedä, mistä organisaation kirjalliset tietoturva- ja tietosuojaohjeet löytyvät ja 11 % (n = 4) ei tiedä, miten toimia tietoturvan tai tietosuojan vaarantuessa (Kuvio 12).



Kuvio 12. Tietoturvatietojen kehityskohteet

Tietoturvatietojen ydinalueen kysymysten (15–20) vastausten keskiarvo oli 2.78 (Taulukko 10). Keskiarvon ollessa 80–100 % eli yli 2.4 on kyseessä tason 2 osaaminen. Vastausten perusteella henkilöstöllä on hyvät tiedot ja taidot tietoturvasta tietoturvatietojen ydinalueessa.

Taulukko 10. Tietoturvatietojen osaamisen taso

Kysymys	Ydinalueen vastausten keskiarvo	Sijoittuminen osaamisen tasolle
15. 16. 17. 18. 19. 20.	3.0 2.9 2.9 2.6 2.7 2.6	
	= 2.78	**Taso 2**

Tietoturvatietojen osaamisen ydinalueessa osaaminen on hyvällä tasolla. Vahvin osaaminen oli tietoturvan ja tietosuojan ymmärtämisessä sekä riittävässä tietoturva- ja tietosuojaosaamisessa. Suurimmiksi kehityskohteiksi tietoturvatietojen osaamisen alueella nousi organisaation kirjallisten tietoturva ja tietosuojaohjeiden sijainnin selkeyttäminen sekä tiedon lisääminen siitä, keneltä voi kysyä apua tietoturva- ja tietosuoja-asioissa.

6.4 Tietoturvataitojen osaaminen

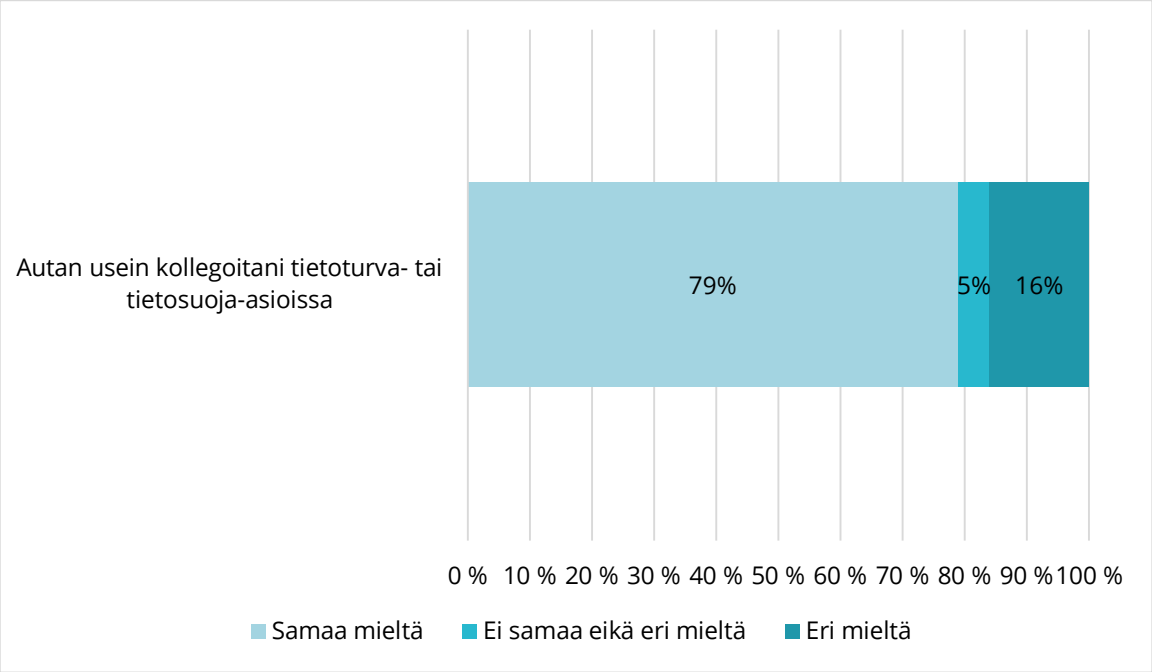
Tietoturvataitojen osaamista tarkastellaan tietoturvan huomioimisen, vastuun, ohjeiden noudattamisen, auttamisen, salaamisen ja salassapidon sekä tietoturvauhan kohtaamisen kautta (Taulukko 11). Korkein keskiarvo 3.0 esiintyi kysymyksessä ”Huomioin tietoturvan ja tietosuojan toteutumisen työssäni” keskihajonnalla 0.0 ja ”Noudatan työssäni organisaation tietoturvakäytäntöjä ja ohjeita” keskihajonnalla 0.2. Toisiksi suurin keskiarvo 2.9 esiintyi kysymyksissä ”Olen osaltani vastuussa organisaation tietoturvasta” ja ”Osaan käyttää salattua sähköpostia ja turvapostia ja tiedän, milloin niitä tulee käyttää”. Molemmissa keskihajonta oli 0.3. Enemmän hajontaa vastauksissa oli keskihajonnalla 0.8 kysymyksissä ”Autan usein kollegoitani tietoturva- tai tietosuoja-asioissa” keskiarvolla 2.6 sekä ”Olen kohdannut työssäni tietoturvauhan” keskiarvolla 2.3. Alhaisimmat keskiarvot esiintyivät käänteisissä kysymyksissä ”Salassapitovelvollisuuteni päättyy työsuhteen päätyttyä” keskiarvolla 1.0 ja keskihajonnalla 0.0 sekä ”Salassapitovelvollisuuteni päättyy työsuhteeni päättyessä” keskiarvolla 1.1 ja keskihajonnalla 0.4.

Taulukko 11. Tietoturvataitojen osaaminen n (%)

Kysymys	n	ka	md	mo	SD	Eri mieltä	Ei samaa eikä eri mieltä	Samaa mieltä
21. Huomioin tietoturvan ja tietosuojan toteutumisen työssäni	39	3.0	3	3	0.0	0 (0)	0 (0)	39 (100)
22. Olen osaltani vastuussa organisaation tietoturvasta	39	2.9	3	3	0.3	1 (3)	0 (0)	38 (97)
23. Noudatan työssäni organisaation tietoturvakäytäntöjä ja ohjeita	39	3.0	3	3	0.2	0 (0)	1 (3)	38 (97)
24. Autan usein kollegoitani tietoturva- tai tietosuoja-asioissa	38	2.6	3	3	0.8	6 (16)	2 (5)	30 (79)
25. Osaan käyttää salattua sähköpostia ja turvapostia, ja tiedän milloin niitä tulee käyttää	39	2.9	3	3	0.3	1 (3)	0 (0)	38 (97)
26. Salassapitovelvollisuuteni koskee vain potilastietoja	39	1.1	1	1	0.4	37 (95)	0 (0)	2 (5)
27. Salassapitovelvollisuuteni päättyy työsuhteeni päättyessä	38	1.0	1	1	0.0	38 (100)	0 (0)	0 (0)

1 = Eri mieltä, 2 = Ei samaa eikä eri mieltä, 3 = Samaa mieltä

Kaikki vastaajat huomioivat työssään tietoturvan ja tietosuojan toteutumisen ja ymmärtävät salassapitovelvollisuuden jatkuvan myös työsuhteen päätyttyä. Lähes kaikki (97 %, n = 38) vastaajista ymmärtävät vastuunsa organisaation tietoturvallisuudessa, noudattavat organisaation tietoturvakäytäntöjä ja ohjeita ja osaavat viestiä tietoturvallisesti salatun sähköpostin avulla. Lisäksi suurin osa 95 % (n = 37) vastaajista ymmärtää salassapidon koskevan muitakin tietoja kuin potilastietoja. Vastaajista 79 % (n = 30) auttaa usein kollegoitaan tietoturva- tai tietosuoja-asioissa (Kuvio 13). Tietoturvauhan on kohdannut työssään yli puolet, 51 % (n = 20) vastaajista.



Kuvio 13. Tietoturvataitojen kehityskohde (%)

Tietoturvataitojen ydinalueen kysymysten (21–27) vastausten keskiarvo oli 2.9 (Taulukko 12). Käänteisten kysymysten (26–27) osalta keskiarvot käännettiin vastaamaan asteikkoa, jossa arvo 3 on suurin mahdollinen arvo. Keskiarvon ollessa 80–100 % eli yli 2.4 on kyseessä tason 2 osaaminen. Tasolla 2 henkilöstöllä on hyvät tiedot ja taidot tietoturvasta.

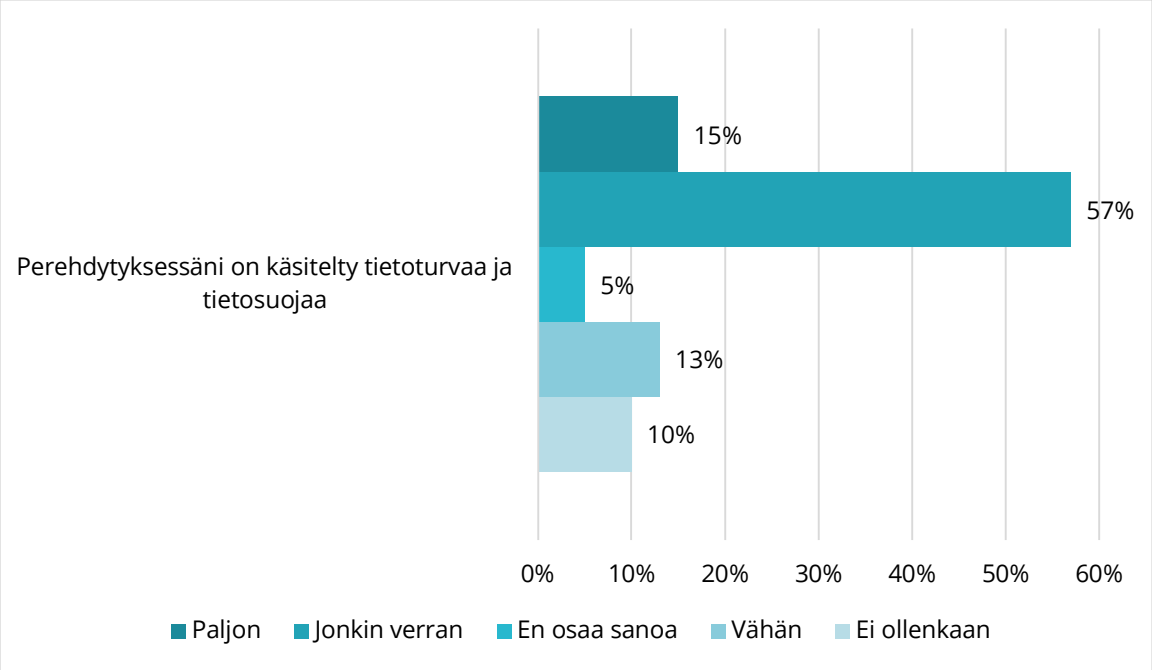
Taulukko 12. Tietoturvataitojen osaamisen taso

Kysymys	**Ydinalueen vastausten keskiarvo**	**Sijoittuminen osaamisen tasolle**
21. 22. 23. 24. 25. 26. 27.	3.0 2.9 3.0 2.6 2.9 1.1 -> 2.9 1.0 -> 3.0	
	= 2.9	**Taso 2**

Tietoturvataitojen osaamisen tulosten perusteella vastaajien tietoturvataitojen osaaminen on erittäin hyvällä tasolla. Vahvin osaaminen esiintyi tietoturvan ja tietosuoja huomioimisessa työssä, vastuussa, tietoturva- ja tietosuojaohjeiden käytäntöjen ja ohjeiden noudattamisessa sekä salassapitoon liittyvissä kysymyksissä. Yksi kehityskohde nousi kuitenkin esille, joka oli kollegoiden apuna toimiminen tietoturva- ja tietosuoja-asioissa.

6.5 Organisaation tietoturva- ja tietosuojakoulutus osana osaamista

Organisaation tietoturva- ja tietosuojakoulutusta tarkastellaan osana tietoturva- ja tietosuojaosaamista perehdytyksen, koulutuksen tärkeyden ja riittävyyden sekä toiveiden kautta. Tietoturvaa ja tietosuojaa on käsitelty perehdytyksessä 15 % (n = 6) vastaajien mielestä paljon ja 57 % (n = 22) vastaajien mielestä jonkin verran (Kuvio 14). Vähän aihetta on käsitelty 13 % (n = 2) vastaajan mielestä ja 10 % (n = 4) vastaajan mielestä ei ollenkaan. Kaksi (5 %) vastaaja ei osaa sanoa, onko perehdytyksessä käsitelty tietoturvaa ja tietosuojaa.



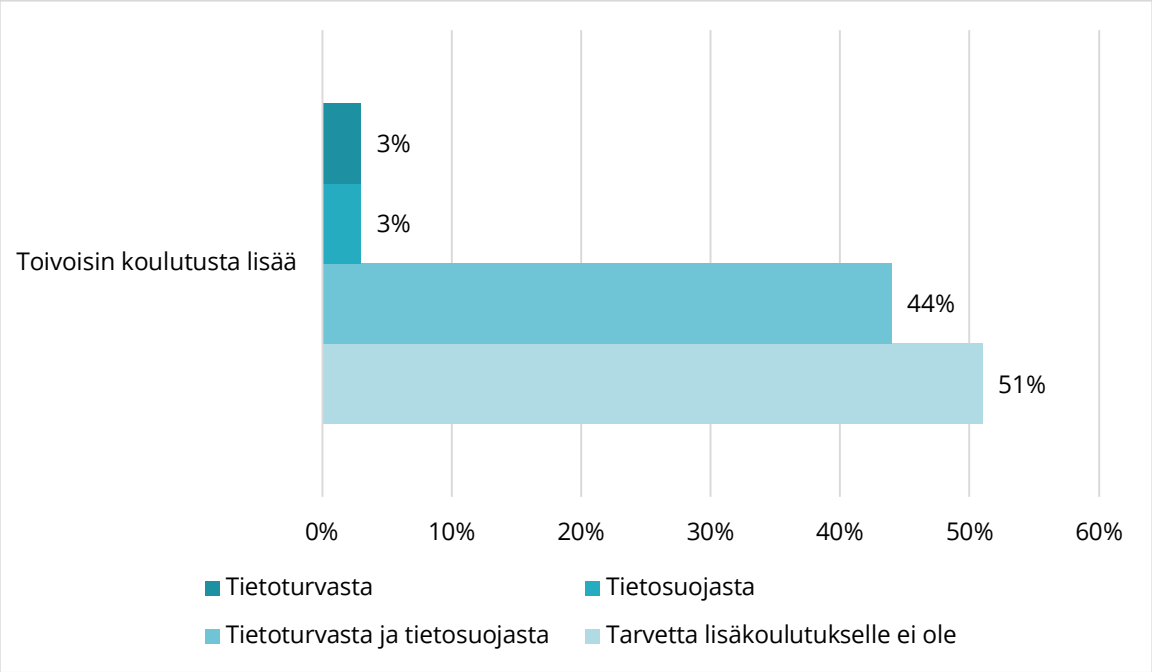
Kuvio 14. Tietoturvan ja tietosuojan käsittely osana perehdytystä (%)

Perehdytyksessä on käsitelty tietoturvaa ja tietosuojaa suurimmalla osalla vastaajista, mutta aihe on jäänyt myös käsittelemättä osan perehdytyksessä tai sitä on käsitelty vain vähän. Tietoturva- ja tietosuojakoulutuksen osalta kysymyksessä ”Koen organisaation tietoturva- ja tietosuojakoulutuksen tärkeäksi” oli keskiarvo 2.9 keskihajonnalla 0.4 ja keskiarvo 2.7 esiintyi kysymyksessä ”Organisaation järjestämä koulutus tietoturvasta ja tietosuojasta on riittävää” keskihajonnalla 0.6 (Taulukko 13).

Taulukko 13. Tietoturva- ja tietosuojakoulutuksen tärkeys ja riittävyys

Kysymys	n	ka	md	mo	SD	Eri mieltä	Ei samaa eikä eri mieltä	Samaa mieltä
Koen organisaation tietoturva- ja tietosuojakoulutuksen tärkeäksi	39	2.9	3	3	0.4	1 (2.5)	1 (2.5)	37 (95)
Organisaation järjestämä koulutus tietoturvasta ja tietosuojasta on riittävää	39	2.7	3	3	0.6	3 (7)	5 (13)	31 (80)

Kokemus organisaation järjestämästä tietoturva- ja tietosuojakoulutuksesta on tulosten perusteella positiivinen. Organisaation järjestämän tietoturva- ja tietosuojakoulutuksen kokee vastaajista lähes kaikki 95 % (n = 37) tärkeäksi ja 80 % (n = 31) mielestä koulutus on riittävää. Kolmen (7 %) vastaajan mielestä koulutus ei ole riittävää. Lisäkoulutuksen tarvetta ei suurimman osan vastaajista 51 % (n = 20) mielestä ole. Vastaajista 44 % (n = 17) toivoisi lisäkoulutusta tietoturvasta ja tietosuojasta ja 3 % (n = 1) puolestaan toivoisi lisäkoulutusta tietoturvasta ja 3 % (n =1) toivoisi tietosuojasta (Kuvio 15).



Kuvio 15. Vastaajien toiveita tietoturva- ja tietosuojaan liittyvästä lisäkoulutuksesta (%)

Tarkempia toiveita organisaation tietoturva ja tietosuojakoulutukselle selvitettiin kysymyksen ”Minkälaista koulutusta toivoisit tietoturvasta ja/tai tietosuojasta?” avulla. Vastauksissa (N = 8)

esiintyi erityisesti toive koulutusten järjestämisestä tai asian tuomisesta esille säännöllisesti käytännön tasolla ja konkretian avulla (Taulukko 14). Kahden vastauksen toiveet sijoittuivat turvallisten tietotekniikan käyttötaitojen ydinalueeseen, yksi vastauksista tietoturvatietojen ydinalueeseen ja kaksi vastauksista tietoturvataitojen ydinalueeseen. Kahdessa vastauksessa ei esitetty toiveita, vaan todettiin koulutusta jo olevan, eikä aika riittäisi lisäkoulutuksen suorittamiseen. Lisäksi yhdessä vastauksessa todettiin kaiken koulutuksen olevan tarpeellista.

Taulukko 14. Vastaajien koulutustoiveet tietoturva- ja tietosuojakoulutukselle

Osaamisen ydinalue	Koulutuksen sisältö	Koulutuksen järjestämistapa
Turvalliset tietotekniikan käyttötaidot (n = 2)	Sähköpostin käyttö turvallisesti Potilasasiakirjojen toimitus turvallisesti Kirjaaminen ja oikea-aikaiset käyntikuittaukset Kirjaamiskäytännöt	Käytännön tasolla konkreettisesti
Tietoturvatiedot (n = 1)	Lyhyet tietoiskut tietoturvasta ja tietosuojasta	Nostoja eri kanavissa Kurssit ja koulutukset
Tietoturvataidot (n = 2)	Käytännön työhön ja arkeen liittyvät tietoturva- ja tietosuojakäytännöt Asiakastilanteissa tietoturvan ja tietosuojan huomioiminen	Arjen työskentelyyn jalkautettuna

Vastauksissa tuotiin esille myös toiveita koulutuksen sisällöstä ja järjestämisestä. Toiveena koulutuksen sisällölle oli muun muassa turvallinen sähköpostin käyttö ja potilasasiakirjojen toimitus sekä kirjaamisen ja käyntikuittausten käytännöt ja niiden merkitys osana tietoturvaa. Lisäksi toiveena oli tietoiskut tietoturvasta ja tietosuojasta sekä niiden käytännöt ja huomioiminen asiakastilanteissa. Koulutuksen järjestämistavan osalta toivottiin jalkauttamista arjen työskentelyyn käytännön tasolle.

7 Pohdinta ja päätelmät

7.1 Tutkimuksen eettisyys ja luotettavuus

Tutkimuksessa noudatettiin Tutkimuseettisen neuvottelukunnan (TENK) mukaista hyvää tieteellistä käytäntöä ja tutkimuksen eettisiä sääntöjä. Perusperiaatteita hyvälle tieteelliselle käytännölle on arvostus, rehellisyys, vastuunkanto ja luotettavuus. Arvostuksella tarkoitetaan arvostusta tieteellisen toiminnan osapuolia, yhteiskuntaa ja ympäristöä kohtaan. Rehellisyydellä tarkoitetaan tieteellisen toiminnan suunnittelua, toteutusta, arviointia ja raportointia avoimesti, oikeudenmukaisesti, puolueettomasti ja salaamatta yksityiskohtia. Vastuunkannolla tarkoitetaan vastuun kantamista koko tieteellisen toiminnan elinkaaren ajan. Luotettavuudella tarkoitetaan tieteellisen toiminnan laadun varmistaminen suunnittelussa, menetelmissä, voimavaroissa ja analyyseissä. (TENK 2023, 12.) Eettisten periaatteiden mukaisesti tutkimuksessa tulee kunnioittaa tutkittavien oikeuksia ja välttää aiheuttamasta haittaa tutkittavina oleville yhteisöille, ihmisille tai muille tutkimuskohteille. Kunnioitettavia oikeuksia on muun muassa tutkittavien ihmisarvo ja yksityisyys. (Vuori 2023.) Kun tieteellinen tutkimus on suoritettu hyvän tieteellisen käytännön perusperiaatteiden (2023) mukaisesti, on se silloin myös eettisesti hyväksyttävä ja tulokset uskottavia. Tässä tutkimuksessa on noudatettu kyseisiä perusperiaatteita koko tutkimuksen ajan. Tutkimuksessa noudatettiin rehellisyyttä läpi tutkimusprosessin suunnittelemalla tutkimuksen toteutus tutkimussuunnitelma avulla, tuoden esiin rehelliset tutkimuksen tavoitteet, informoimalla tutkimukseen osallistuneita tutkimuksen tarkoituksesta ja analysoimalla tulokset sekä raportoimalla ne rehellisesti salaamatta yksityiskohtia.

Tutkimuksessa on pyritty luotettavuuteen noudattamalla tarkkuutta ja huolellisuutta tutkimustyössä, aineiston keruussa ja analysoinnissa sekä tulosten esittämisessä. Tutkimusaineistoa ja tutkimustuloksia käsiteltiin luottamuksellisesti ja huolehtien ettei tutkimuksesta voida tunnistaa yksittäistä vastaajaa tai tämän henkilöllisyyttä. Tunnistamattomuus ja nimettömyys ovat lähtökohtia aineistojen esittämisessä tutkimusjulkaisuissa, ja tutkijan vastuulla on huolehtia tutkittavien yksityisyyden suojasta. Tunnisteellisuuteen kuuluu keskeisenä asiana anonymisointi eli tunnisteiden muuttaminen tai

poistaminen. (Kuula 2011, 139–142). Tämä tutkimus toteutettiin anonyymillä kyselytutkimuksella (liite 2) organisaation henkilöstölle, joten erillistä tarvetta tunnisteiden poistamiselle ei ollut. Kyselylomakkeeseen laadittiin strukturoituja kysymyksiä ja yksi avoin kysymys siten, että vastauksista ei voida tunnistaa yksittäisen vastaajan henkilöllisyyttä. Kysely lähetettiin organisaation sisäisen henkilön välityksellä kohderyhmälle, eikä tutkijalla ollut suoraa yhteyttä tutkittaviin. Tutkimusaineiston keruu toteutettiin Itä-Suomen yliopiston alaisella Webropol-sovelluksella, joka on suojattu salasanalla. Aineistoon oli koko tutkimusprosessin ajan pääsy vain tutkijalla ja sitä käsitteli vain tutkimuksen tekijä. Aineistoa säilytettiin Itä-Suomen yliopiston alaisessa salasanasuojatussa Microsoftin OneDrive-pilvipalvelussa, jonka käyttöoikeus oli vain tutkijalla. Aineistoa käsiteltiin tutkimuksen aikana Itä-Suomen yliopiston alaisella lisenssillä SPSS- statistics 27 tilasto-ohjelmalla ja Excel laskentataulukko-ohjelmalla. Alkuperäinen aineisto hävitetään 2 vuoden päästä tutkimuksen valmistumisen jälkeen. Tutkimustulokset raportoitiin siten, ettei niistä ole mahdollista tunnistaa yksittäistä henkilöä. Kvantitatiivisissa tutkimuksissa tuloksia ei raportoida yksilöiden, joten tunnistusriskiä ei tavallisesti ole (Kuula 2011, 142).

Arvostusta on osoitettu tutkimuksen kohderyhmää kohtaan kohteliaalla viestinnällä tutkimukseen osallistumisesta ja kiitoksilla vastauksista. Lisäksi arvostusta on osoitettu muita tutkijoita kohtaan viittaamalla heidän tutkimuksiinsa asianmukaisesti lähteillä. Vastuunkantoa on osoitettu ottamalla vastuuta tutkimuksen luotettavuudesta, eettisyydestä ja asianmukaisesta suorituksesta. Tutkimukselle haettiin organisaatiolta tutkimuslupa ja aineisto kerättiin sekä käsiteltiin vastuullisesti huolehtien tutkimukseen osallistuneiden anonyymiydestä ja haittojen välttämisestä. Tutkimuksen kohteena ei ollut ihmiseen kohdistuva tai lääketieteellinen tutkimus, joten tarvetta eettisen toimikunnan lausunnolle ei ollut (Vastuullinen tiede 2020).

Kyselytutkimuksen luotettavuutta voidaan tarkastella reliabiliteetin ja validiteetin avulla. Validiteetti tarkoittaa mittarin hyvyyttä eli pätevyyttä mitata sitä, mitä mittarilla on tarkoituksena mitata. Epäpätevyyttä voi aiheuttaa esimerkiksi mittauksen ajankohta tai epäonnistunut otanta. Mittarin validiteetti on tärkeää kokonaisvaliditeetin vuoksi. tarkoittaa tulosten tarkkuutta. Tutkimustulokset eivät saa olla sattumanvaraisia. Siitä voidaan erottaa stabiliteetti ja konsistenssi. Stabiliteetilla tarkoitetaan mittarin pysyvyyttä ajassa, jolloin

satunnaisvirheet eivät vaikuta mittariin. Konsistenssilla tarkoitetaan mittarin yhtenäisyyttä eli kun useammista väittämistä koostuva mittari jaetaan kahteen joukkoon väittämiä, mittaa molemmat joukot samaa asiaa ja näiden välinen korrelaatiokerroin saa suuren arvon. (Tietoarkisto 2022a; Heikkilä 2014, 28.)

Tämän kyselytutkimuksen mittarina käytettiin itse kehitettyä kyselylomaketta, jota käytettiin aineiston keruuseen. Validiteettiin pyrittiin kiinnittämään huomiota kyselylomakkeen suunnittelussa ja laadinnassa. Kyselylomakkeen suunnittelussa huomioitiin teoriatietoa ja tutkimuksessa hyödynnettävää Staggersin ja hänen tutkimusryhmänsä (2002a) osaamisen ydinalueiden viitekehystä. Kyselylomakkeen sisältöä käytiin läpi organisaation yhteyshenkilön kanssa ja testattiin ulkopuolisella testiryhmällä (N = 5). Testauksen jälkeen kyselylomakkeen kysymyksiä selkeytettiin. Saateviestissä informoitiin selkeästi tutkimukseen osallistumisen vapaaehtoisuudesta, anonyymiydestä, tutkimuksen tarkoituksesta ja sen tekijästä sekä aineiston käsittelystä ja raportoinnista. Lisäksi tutkimukseen osallistuneilla oli pääsy näkemään tutkimusta varten laadittu tietosuojaseloste. Kyselylomakkeessa kysymyksenasettelun tarkkuustasolla on merkitystä mittaustarkkuuden kannalta. Kysymyksillä tulisi pääsääntöisesti kysyä kaikkea kohtuullisen tarkasti, mutta kysymysten ja vastausten liiallinen spesifisyys voi myös vaikuttaa mittaustarkkuuteen. (Tietoarkisto 2022b.) Tässä tutkimuksessa käytettiin pääasiassa strukturoituja kysymyksiä, mutta mukana oli myös yksi avoin kysymys.

Tutkimuskysely kohtasi vastaajakadon eikä siihen saatu tavoiteltua määrää vastauksia. Vähäistä vastausten määrää pyrittiin välttämään hyvällä suunnittelulla sekä muistutuksilla ja vastausajan jatkamisella. Vastaajakatoa saattoi aiheuttaa työn kiireellisyys ja tutkittavan aiheen arkaluonteisuus. Tutkimukselle ei saatu tarkkaa vastausprosenttia, koska kysely lähti vastaajille organisaation sisäisten henkilöiden kautta. Tutkija sai kuitenkin tiedon, että kysely lähti noin 150 henkilölle. Vastausprosentti on silloin noin 26 %. Tutkimuksen alhaisen vastausprosentin vuoksi tuloksia tulee tarkastella tiedostaen, ettei niiden pohjalta voi tehdä yleistyksiä. Tuloksia voidaan kuitenkin pitää suuntaa antavina.

7.2 Tulosten tarkastelu

Tämän tutkimuksen tarkoituksena oli tutkia yksityisen terveydenhuollon henkilöstön tietoturva- ja tietosuojaosaamisen tasoa. Lisäksi tavoitteena oli tunnistaa yksityisen terveydenhuollon henkilöstön tietoturva- ja tietosuojaosaamisen kehityskohteita osaamisen ja organisaation koulutuksen kehittämisen tueksi. Tutkimustulokset osoittivat, että kyselyyn vastanneiden tietoturva- ja tietosuojaosaaminen oli vahvalla tasolla. Henkilöstö huomioi työssään tietoturvan ja tietosuojan toteutumisen sekä ymmärtää oman vastuunsa osana sitä. Lisäksi tietoturvan ja tietosuojan merkitys ymmärretään ja työssä noudatetaan organisaation tietoturva- ja tietosuojaohjeita sekä käytäntöjä. Vahvasta osaamisen tasosta huolimatta osaamisen ydinalueissa esiintyi myös kehityskohteita.

Ensimmäisen tutkimuskysymyksen avulla tutkittiin henkilöstön tietoturva- ja tietosuojaosaamisen tasoa. Ihminen itse on tunnistettu tietoturvallisuuden ja tietosuojan suurimmaksi riskiksi. Sen vuoksi tärkeänä lähtökohtana henkilöstön osaamisessa on, että jokainen terveydenhuollon ammattilainen osaa käyttää tieto- ja viestintätekniikkaa turvallisesti työssään. (Sederholm ym. 2019, 89; Bichel-Findlay ym. 2022, 2–7.) Tätä tutkittiin turvallisten tietotekniikan käyttötaitojen ydinalueessa kartoittamalla taitoja, joilla olisi mahdollista välttää turvallisuusriskejä. Tutkimuksissa esille tulleita turvallisuusriskejä on huonot salasanakäytännöt, työpisteiltä pois kirjautumatta jättäminen sekä terveystietojen toimittaminen sähköpostitse ilman suojausta (Humaidi & Balakrishnan 2018, 18–19). Turvallisuusriskejä voidaan välttää hyvillä tietoturvakäytännöillä, joita on monimutkaisten salasanojen käyttö, saman salasanan käyttö vain yhdessä palvelussa sekä harkittu liitetiedostojen tai linkkien avaaminen (Kyberturvallisuuskeskus 2020). Tämän kyselytutkimuksen tulosten mukaan osaaminen tällä ydinalueella oli heikointa muihin ydinalueisiin verrattuna, mutta kuitenkin hyvällä tasolla sijoittuen osaamisen tasolle 2. Henkilöstö muistaa pääsääntöisesti lukita työpisteen poistuessaan siitä, ei lataa tuntemattoman lähettäjän liitetiedostoja harkitsematta ja käyttää työssään vain organisaation määrittämiä työvälineitä.

Toinen keskeinen korostunut asia tietoturvallisuuden ja tietosuojan toteuttamisessa on koulutettu ja valpas henkilöstö, kenen ammattitaitoon kuuluu tietoturvatietoisuus (Box &

Pottas 2013, 1094; Lebek ym. 2013, 2978). Jokaisen organisaation henkilöstön jäsenen tulisi hallita tietoturvaperiaatteet ja osata hyödyntää niitä työssään. (STM 2019, 24) Tätä tutkittiin tietoturvatietojen ydinalueessa. Tämän kyselytutkimuksen tulosten mukaan henkilöstön osaaminen tällä ydinalueella oli hyvällä tasolla sijoittuen osaamisen tasolle 2. Tietoturvan ja tietosuojan merkitys ymmärretään ja oma tietoturva- ja tietosuojaosaaminen arvioidaan riittävän hyväksi. Tietoturva käsitteenä ymmärretään hieman tietosuojaa paremmin. Osana tietoturvatietämystä on tärkeää, että henkilöstö ymmärtää tietoturvan merkityksen organisaatiossa (Kruger & Kearney 2006, 289, 290). Työtehtäväkohtaisesti oman osaamisen arvioi parhaaksi lääkärit sekä muussa työtehtävässä työskentelevät ja heikoimmaksi terapeutit.

Kolmas keskeinen asia osana tietoturva- ja tietosuojaosaamista on tietoturvakäytäntöjen toteuttaminen. Terveydenhuollon ammattilaisten tulee tunnistaa tietoturvan tärkeys sekä hyödyntää tietoturvallisuutta työssään (EunWon & Seomun 2021, 2; Kang & Seomun 2021, 16.) Tätä tutkittiin tietoturvataitojen ydinalueessa, jonka osaaminen oli myös hyvin vahvalla tasolla. Tämän kyselytutkimuksen tulosten mukaan osaaminen tällä ydinalueella oli erittäin hyvällä tasolla sijoittuen osaamisen tasolle 2. Kaikki vastaajat huomioivat tietoturvan ja tietosuojan toteutumisen työssään. Lisäksi suurin osa ymmärtää olevansa vastuussa organisaation tietoturvasta ja noudattaa työssään organisaation tietoturvakäytäntöjä ja -ohjeita. Tietoturvakäytäntöihin kuuluu hyvä perehtyminen organisaation tietoturvakäytäntöihin (Kyberturvallisuuskeskus 2020). Myös vastuu salassapitovelvollisuudesta ymmärretään ja tiedostetaan sen jatkuvan myös työsuhteen päätyttyä. Henkilöstön tulee huomioida salassapitovelvollisuus työsuhteensa aikana sekä työsuhteensa päätyttyä (STM 2019, 14; Valvira 2018).

Tutkimuksen tulosten perusteella tämän tutkimuksen kohteena olevan yksityisen terveydenhuollon henkilöstön tietoturva- ja tietosuojaosaaminen on kokonaisuudessaan hyvällä tasolla sijoittuen jokaisen ydinalueen osalta osaamisen tasolle 2. Osaaminen jakautui eri ydinalueilla siten, että paras osaaminen on tietoturvataitojen osaamisessa, toiseksi paras on tietoturvatietojen osaaminen ja kolmanneksi paras on turvallisten tietotekniikan käyttötaitojen osaaminen.

Toisen tutkimuskysymyksen avulla selvitettiin mitä kehittämiskohteita henkilöstön tietoturva- ja tietosuojaosaamisessa on. Osaamisen ollessa hyvällä tasolla, ei henkilöstön osaamisen ydinalueissa havaittu suuria kriittisiä puutteita tämän tutkimuksen osalta. Positiivisten tulosten joukossa oli kuitenkin keskinkertaisempia tuloksia, jotka kaipaavat kehitystä tietoturva- ja tietosuojaosaamisen varmistamiseksi. Suurimpana kehityskohteena nousi esille tietoturvariskien kannalta keskeiset salasanakäytännöt. Kolmasosa vastaajista käyttää samaa salasanaa useassa eri palvelussa ja säilyttää salasanoja tallessa kirjallisesti, jotta ne eivät unohdu. Tutkimuksissa korostuneena turvallisuusriskinä on esiintynyt huonot salasanakäytännöt (Humaidi & Balakrishnan 2018, 18–19). Turvallisuusriskejä voidaan välttää hyvillä tietoturvakäytännöillä, joita on muun muassa monimutkaisten salasanojen käyttö sekä saman salasanan käyttö vain yhdessä palvelussa (Kyberturvallisuuskeskus 2020).

Toinen keskeinen kehityskohde oli tietoturva- ja tietosuojakäytäntöihin liittyvien ohjeiden sijainnin tietämättömyys sekä tietämättömyys, keneltä aiheesta voi kysyä apua. Lähes kolmanneksella vastaajista ei ollut tietoa näiden osalta. Puutteellisista tiedoista huolimatta 97 % vastaajista on vastannut noudattavansa työssään organisaation tietoturva- ja tietosuojakäytäntöjä sekä -ohjeita. Tämän perusteella käytännöt ja ohjeet vaikuttaisivat olevan henkilöstön tiedossa ilman ohjeiden sijainnin tietämistä tai vaihtoehtoisesti kysymykseen on vastattu ilman tarkempaa tietoa siitä, mitä nämä käytännöt ja ohjeet ovat. On kuitenkin tärkeää, että jokaisella henkilöstön jäsenellä olisi tiedossa organisaation tietoturva- ja tietosuojaohjeiden sijainti, koska henkilöstön osaamista on mahdollista parantaa kirjallisten ohjeiden avulla ja lisäksi ne lisäävät luottamusta organisaatiota kohtaan. (Andreasson ym. 2016, 53, 54; Humaidi & Balakrishnan 2018, 23–24). On myös tärkeää, että jokainen henkilöstöstä tietää, keneltä tietoturva- ja tietosuoja-asioista voi kysyä apua. Tietoturvakäytäntöihin kuuluu häiriötilanteiden hallinta tutustumalla etukäteen tietoturvasta vastaaviin henkilöihin ja tietoturvapoikkeamien ehkäisemiseksi on tärkeää osata ja uskaltaa raportoida havaitsemistaan poikkeamista sekä uhkista (Kyberturvallisuuskeskus 2020; Liikenne- ja viestintävirasto Traficom 2020, 24). Kehityskohteeksi nousi myös tietoturva- ja tietosuojaosaamisessa kollegoiden auttaminen, joka on myös tärkeää tietoturva- ja tietosuojatietoisuuden lisäämiseksi.

Laadukas koulutus on tunnistettu keskeiseksi tekijäksi tietoturva- ja tietosuojaosaamisen kehittämisessä. Sen on osoitettu lisäävän terveydenhuollon ammattilaisten tietoisuutta

tietoturvasta ja tietosuojasta sekä lisäävän positiivista vaikutusta tietoturvallisten toiminnan viemiselle käytännön työhön. (Bichel-Findlay ym. 2022, 10; EunWon & Seomun 2021, 11; STM 2019, 24; Andreasson ym. 2016, 52.) Organisaation järjestämän pakollisen tietoturva- ja tietosuojakoulutuksen on suorittanut vastaajista suurin osa, mutta kuitenkin 15 % on jättänyt sen suorittamatta tietämättömyyden tai muun syyn vuoksi. Koulutuksen tärkeäksi kuitenkin koki suurin osa vastaajista. Lisäksi suurin osa oli sitä mieltä, että koulutus on riittävää nykyisellään. Tärkeänä kehityskohteena tietoturva- ja tietosuojaosaamisen kehittämiseksi on ydinalueiden kehityskohteiden lisäksi se, että varmistetaan jokaisen organisaation henkilöstön jäsenen osalta koulutuksen suorittaminen. Koulutuksen kehityksen osalta toiveena oli enemmän koulutuksen säännöllisyys, kuin tarve varsinaiselle lisäkoulutukselle aiheesta.

7.3 Päätelmät ja jatkotutkimusaiheet

Tietoturva- ja tietosuojariskien kasvaessa digitalisaation myötä, on tämän tutkimuksen aihe tärkeä ja ajankohtainen sosiaali- ja terveydenhuollon tietoturvallisuuden sekä tiedonhallinnan kannalta. Tietoturva ja tietosuoja on tärkeä osa tiedonhallinnan osaamista, jonka vuoksi myös aiheen tärkeys korostuu. Terveydenhuollon organisaatioiden tulee varmistaa arkaluontoisten asiakas- ja potilastietojen tietosuojan toteutuminen tietoturvallisilla toimilla entistä paremmin uhkien lisääntyessä. Henkilöstö on tärkeässä roolissa tietoturvan ja tietosuojan toteuttamista, jonka vuoksi organisaation on tärkeää panostaa tietoturva- ja tietosuojaosaamisen kehittämiseen ohjeiden ja käytäntöjen sekä koulutuksen avulla.

Teoreettisen viitekehyksen hyödyntäminen tietoturva- ja tietosuojaosaamisen ydinalueiden ja osaamistasojen määrittämisessä oli hyödyllistä. Osaamisen tarkastelu ydinalueiden kautta oli aiheeseen sopiva ja huomioi osaamisen eri ulottuvuudet. Ydinalueiden ja osaamisen tasojen avulla oli mahdollista arvioida millä henkilöstön tietoturva- ja tietosuojaosaamisen ydinalueilla osaaminen on hyvällä tasolla ja puolestaan myös sitä, missä on kehitettävää.

Tämän tutkimuksen tuloksista voidaan päätellä henkilöstön tietoturva- ja tietosuojaosaamisen olevan hyvällä tasolla, mutta huomata myös, että silti osaamisessa voi olla puutteita, joista voi olla haittaa tietoturvan toteuttamisen ja organisaation turvallisuuden kannalta. Tietoturvariskejä piilee terveydenhuollon ympäristössä paljon, jolloin henkilöstön tulee olla

jatkuvasti valppaana ja huomioida tietoturvan toteuttaminen myös kiireellisissä tilanteissa. Yksityisen terveydenhuollon henkilöstön tietoturva- ja tietosuojaosaaminen pohjautuu tietoihin ja taitoihin sekä tietoturvakäyttäytymiseen käytännön työssä. Tietoturvariskien pienentämiseksi henkilöstön osaamista tulisi kehittää säännöllisesti. Tietoturva- ja tietosuojaosaamiseen voidaan vaikuttaa koulutuksilla, ohjeilla ja käytännöillä sekä säännöllisillä aiheen esille nostoilla. Koulutuksessa on huomioitava kohderyhmä, ajankäyttö ja käytännönläheisyys. Tärkeää on myös se, että organisaation jokainen työntekijä on tietoinen koulutuksista ja niiden suorittamiseen on riittävä ajallinen resurssi.

Aiempaa tutkimusta yksityisen sosiaali- ja terveydenhuollon henkilöstön tietoturva- ja tietosuojaosaamisesta on tehty vähäisesti. Tietoturva- ja tietosuojaosaaminen on tärkeää organisaatioiden turvallisuuden vuoksi, sillä useissa tutkimuksissa on noussut esille ihmisen olevan pahin uhka tietoturvallisuudelle. Henkilöstön tietoturva- ja tietosuojaosaamisen avulla organisaatio voi parantaa tietoturvallisuuden tasoa ja luoda tehokkaampia tietoturvakäytäntöjä, joiden avulla suojella arkaluontoisia tietoja ja suojautua tietoturvaloukkauksilta.

Tämän tutkimuksen osalta tutkimustulokset jäivät vähäisiksi, jonka vuoksi koko organisaation tietoturva- ja tietosuojaosaamisen ei voida olettaa olevan hyvällä tasolla vain tämän tutkimuksen tulosten perusteella. Sen vuoksi yksityisen terveydenhuollon tietoturva- ja tietosuojaosaamisen tutkiminen olisi jatkossakin tärkeää. Aiheen tutkimista varten tässä tutkimuksessa käytetty kyselylomake ja viitekehys olisivat jatkossakin soveltuvia. Jatkotutkimuksen osalta tarpeellista voisi olla toistaa kysely uudelleen pyrkien suurempaan vastaajamäärään. Kyselylomakkeen luovuttamisesta organisaation jatkokäyttöön on keskusteltu alustavasti, joten jatkotutkimus voisi olla mahdollista.

Toinen mahdollinen jatkotutkimuksen aihe voisi olla terveydenhuollon henkilöstön tietoturva- ja tietosuojakoulutuksen sisällön tutkiminen ja sen soveltuvuuden arviointi eri ammattiryhmille. Tässä tutkimuksessa nousi esille toiveena koulutuksen kohdistaminen käytäntöön, joten olisi tarpeellista tutkia eri ammattiryhmien osaamistason lisäksi osaamisvaatimuksia, jotka voivat poiketa työtehtäväkohtaisesti. Näkökulmana voisi olla osaamistason ja osaamisvaatimusten arviointi eri ammattiryhmien osalta, kuten mikä on

osaamisen lähtötaso ja mitä eri ammattiryhmien työssä on kriittisintä osata tietoturvan ja tietosuojan osalta. Näin olisi mahdollista kehittää kohdennettua koulutusta ammattiryhmille sopivaksi.

Lähteet

Alastalo Marja & Borg Sami 2010. Numerolukutaito. Kvantitatiivisen tutkimuksen verkkokäsikirja. Yhteiskuntatieteellinen tietoarkisto, Tampere. Saatavissa: https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/kvanti/numerolukutaito/numerolukutaito_tiedonkeruu/ (Viitattu 10.11.2022)

Andreasson Ari, Koivisto Juha & Ylipartanen Arto 2016. Tietosuojakäsikirja johdolle. Tietosanoma, Helsinki.

Appari Ajit & Johnson Eric 2010. Information security and privacy in healthcare: current state of research. Internet and enterprise management 6(4), 279–314. Saatavissa: https://mba.tuck.dartmouth.edu/pages/faculty/eric.johnson/pdfs/AJIJIEM.pdf (Viitattu 18.11.2022)

Bichel-Findlay Jen, Koch Sabine, Mantas John, Abdul Shabbir, Al-Shorbaji Najeeb, Ammenwerth Elske, Baum Analia, Borycki Elizabeth, Demiris George, Hasman Arie, Hersh William, Hovenga Evelyn, Huebner Ursula, Huesing Elaine, Kushniruk Andre, Hwa Lee Kye, Lehmann Christoph, Lillehaug Svein-Ivar, Marin Heimar, Marschollek Michael, Martin-Sanchez Fernando, Merolli Mark, Nishimwe Aurore, Saranto Kaija, Sent Danielle, Shachak Aviv, Udayasankaran Jai, Were Martin & Wright Graham 2022. Recommendations of the International Medical Informatics Association (IMIA) on Education in Biomedical and Health Informatics: Second Revision. International Journal of Medical Informatics 170, 104908. Saatavissa: https://doi.org/10.1016/j.ijmedinf.2022.104908 (Viitattu 4.12.2022)

Box Debra & Pottas Dalenca 2013. Improving Information Security Behaviour in the Healthcare Context. Procedia Technology 9, 1093–1103. Saatavissa: https://doi.org/10.1016/j.protcy.2013.12.122 (Viitattu 4.4.2023)

EunWon Lee & Seomun GyeongAe 2021. Structural Model of the Healthcare Information Security Behavior of Nurses Applying Protection Motivation Theory. International Journal of Environmental Research and Public Health 18(4), 2084. Saatavissa: https://doi.org/10.3390/ijerph18042084 (Viitattu 19.11.2022)

Heikkilä Tarja 2014. Tilastollinen tutkimus. Edita Publishing Oy, Helsinki.

Horne Craig, Ahmad Atif & Maynard Sean 2016. A Theory on Information Security. Proceedings of the Australasian Conference on Information Systems, Australia. Saatavissa: https://ro.uow.edu.au/cgi/viewcontent.cgi?article=1066&context=acis2016 (Viitattu 5.2.2023)

Humaidi Norshima & Balakrishnan Vimala 2018. Indirect effect of management support on users´ compliance behaviour towards information security policies. Health information management journal. 47(1), 17–27. Saatavissa: https://doi.org/10.1177/1833358317700255 (Viitattu 31.3.2023)

Hübner Ursula, Shaw Toria, Thye Johannes, Egbert Nicole, de Fatima Marin Heimar, Chang Polun, O´Connor Siobhán, Day Karen, Honey Michelle, Blake Rachelle, Hovenga Evelyn, Skiba Diane & Ball Marion 2018. Technology Informatics Guiding Education Reform – TIGER*. National Library of Medicine 57(01), 30–42. Saatavissa: https://doi.org/10.3414/me17-01-0155 (Viitattu 22.11.2023)

Juhila Kirsi 2023. Teemoittelu. Laadullisen tutkimuksen verkkokäsikirja. Saatavissa: https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/kvali/analyysitavan-valinta-ja-yleiset-analyysitavat/teemoittelu/ (Viitattu 7.4.2023)

Kangasniemi Mari, Hipp Kirsi, Häggman-Laitila Arja, Kallio Hanna, Karki Suyen, Kinnunen Pirjo, Pietilä Anna-Maija, Saarnio Reetta, Viinamäki Leena, Voutilainen Ari & Waldén Anne 2018. Optimoitu sote-ammattilaisten koulutus- ja osaamisuudistus. Valtioneuvoston selvitys- ja tutkimustoimikunnan julkaisusarja 39/2018. Valtioneuvoston selvitys- ja tukitoiminta. Saatavissa: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/160883/39-2018-Optimoitu%20sote-osaaminen.pdf?sequence=1&isAllowed=y (Viitattu 6.4.2023)

Kang Jiwon & Seomun GyeongAe 2021. Information Security in Nursing: A Concept Analysis. Advances in Nursing Science 44(1), 16–30. Saatavissa: https://doi.org/10.1097/ans.0000000000000330 (Viitattu 18.11.2022)

Kruger & Kearney 2006. A prototype for assessing information security awareness. Computers & Security 25(4), 289–296. Saatavissa: https://doi-org.ezproxy.uef.fi:2443/10.1016/j.cose.2006.02.008 (Viitattu 10.4.2023)

Kuula Arja 2011. Tutkimusetiikka: aineistojen hankinta, käyttö ja säilytys. Vastapaino, Tampere.

Kuusisto-Niemi Sirpa & Saranto Kaija 2009. Sosiaali- ja terveydenhuollon tiedonhallinta – Paradigma tieteenalan perustana. Finnish Journal of EHealths and EWelfare 1(1), 19–23. Saatavissa: https://journal.fi/finjehew/article/view/41405 (Viitattu 20.9.2022)

Kyberturvallisuuskeskus 2020. Näin pidät huolta tietoturvasta kotona ja työpaikalla. Saatavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-pidat-huolta-tietoturvasta-kotona-ja-tyopaikalla (Viitattu 25.1.2023)

Laki potilaan asemasta ja oikeuksista 785/1992.

Laki terveydenhuollon ammattihenkilöistä 559/1994.

Laki yksityisestä terveydenhuollosta 152/1990.

Lebek Benedikt, Uffen Jörg, Breitner Michael, Neumann Markus & Hohler Bernd 2013. Employees` Information Security Awareness and Behavior: A Literature Rewiew. Hawaii International Conference on System Sciences 46, 2978–2987. Saatavissa: https://doi-org.ezproxy.uef.fi:2443/10.1109/HICSS.2013.192 (Viitattu 1.3.2023)

Liikenne- ja viestintävirasto Traficom 2020. Kyberturvallisuus ja yrityksen hallituksen vastuu. Traficomin julkaisuja 2/2020. Saatavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/T_KyberHV_digiAUK_220120.pdf (Viitattu 25.1.2023)

Rhee Hyeun-Suk, Kim Cheongtag & Ryu Young 2009. Self-efficacy in information security: Its influence on end users´ information security practice behavior. Computers & Security 28(8), 816–826. Saatavissa: https://doi.org/10.1016/j.cose.2009.05.008 (Viitattu 15.4.2023)

Safa Nader & Von Solms Rossouw 2016. An Information security knowledge sharing model in organizations. Computers in Human Behavior 57, 442–451. Saatavissa: https://doi-org.ezproxy.uef.fi:2443/10.1016/j.chb.2015.12.037 (Viitattu 6.4.2023)

Saranto Kaija & Kinnunen Ulla-Mari 2019. Sosiaali- ja terveydenhuollon tiedonhallinnan tutkimuskohteet Itä-Suomen yliopistossa – paradigman todentuminen tietohallinnon maisteri- ja tohtorikoulutuksessa. Finnish Journal of eHealth and eWelfare 11(3), 210–219. Saatavissa: https://doi.org/10.23996/fjhw.77593 (Viitattu 23.9.2022)

Saranto Kaija & Kuusisto-Niemi Sirpa 2012. Tiedonhallinnan koulutusohjelma arvioitavana – kokemuksia kansainvälisestä akkreditoinnista. Finnish Journal of eHealth and eWelfare 4(2), 140–144. Saatavissa: https://journal.fi/finjehew/article/view/6558 (Viitattu 10.9.2022)

Sederholm Teija, Laitinen Tiina, Lehto Martti & Kari Martti 2019. Terveydenhuolto ja kyberuhkat. Finnish Journal of eHealth and eWelfare 11(1–2), 86–99. Saatavissa: https://doi.org/10.23996/fjhw.74183 (Viitattu 22.11.2023)

Sisäministeriö 2022. Kyberturvallisuus osana kansallista turvallisuutta. Saatavissa: https://intermin.fi/kansallinen-turvallisuus/kyberturvallisuus (Viitattu 15.11.2022)

Staggers Nancy, Gassert Carole & Curran Christine 2002a. A Delphi Study to Determine Informatics Competencies for Nurses at Four Levels of Practice. Nursing Research 51(6), 383–390. Saatavissa: https://oce-ovid-com.ezproxy.uef.fi:2443/article/00006199-200211000-00006/HTML (Viitattu 18.11.2022)

Staggers Nancy, Gassert Carole & Curran Christine 2002b. Results of a Delphi Study to Determine Informatics Competencies for Nurses at Four Levels of Practice. Saatavissa: https://nursing-informatics.com/niassess/NIcompetencies_Staggers.pdf (Viitattu 18.11.2022)

STM 2016. Digitalisaatio terveyden ja hyvinvoinnin tukena. Sosiaali- ja terveysministeriön digitalisaatiolinjaukset 2025. Sosiaali- ja terveysministeriön julkaisuja 2016:5, Sosiaali- ja terveysministeriö, Helsinki. Saatavissa: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/75526/JUL2016-5-hallinnonalan-ditalisaation-linjaukset-2025_vanh.pdf?sequence=4&isAllowed=y (Viitattu 15.9.2022)

STM 2022. Yksityiset sosiaali- ja terveyspalvelut. Sosiaali- ja terveysministeriö. Saatavissa: https://stm.fi/yksityiset-sotepalvelut (Viitattu 10.11.2022)

STM 2019. Kyberturvallisuus. Ohje sosiaali- ja terveydenhuollon toimijoille. Sosiaali- ja terveysministeriön julkaisuja 2019:14. Sosiaali- ja terveysministeriö, Helsinki. Saatavissa: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/161683/J14_Kyberturvallisuus_WEB.pdf?sequence=1&isAllowed=y (Viitattu 23.9.2022)

TENK 2023. Hyvä tieteellinen käytäntö ja sen loukkausepäilyjen käsitteleminen Suomessa. Tutkimuseettisen neuvottelukunnan julkaisuja 2/2023, Helsinki. Saatavissa: https://tenk.fi/sites/default/files/2023-03/HTK-ohje_2023.pdf (Viitattu 8.4.2023)

Tieteen termipankki 2016. Filosofia: Tieto. Saatavissa: https://tieteentermipankki.fi/wiki/Filosofia:tieto (Viitattu 10.4.2023)

Tietoarkisto 2022a. Mittaaminen: Mittarin luotettavuus. Saatavissa: https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/kvanti/mittaaminen/luotettavuus/ (Viitattu 20.11.2022)

Tietoarkisto 2022b. Kyselylomakkeen laatiminen. Saatavissa: https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/kvanti/kyselylomake/laatiminen/ (Viitattu 20.11.2022)

Tietosuojavaltuutetun toimisto 2022. Tietosuoja. Saatavissa: https://tietosuoja.fi/tietosuoja (Viitattu 3.12.2022)

Valtiovarainministeriö 2020. Julkisen hallinnon digitaalinen turvallisuus. Valtiovarainministeriön julkaisuja 2020:23. Saatavissa: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/162169/VM_2020_23.pdf?sequence=2&isAllowed=y

Valtiovarainministeriö 2017. Tietoturvapoikkeamatilanteiden hallinta. Valtion tieto- ja kyberturvallisuuden johtoryhmä. Julkisen hallinnon ICT. Valtionvarainministeriön julkaisuja 8/2017, Helsinki. Saatavissa: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/79258/VM_8_2017.pdf?sequence=6&isAllowed=y (Viitattu 24.9.2022)

Valvira 2018. Salassapito- ja vaitiolovelvollisuus. Saatavissa: https://www.valvira.fi/terveydenhuolto/hyva-ammatinharjoittaminen/salassapito/salassapito-_ja_vaitiolovelvollisuus (Viitattu 11.11.2022)

Vastuullinen tiede 2020. Milloin tutkimus tarvitsee eettisen ennakkoarvioinnin? Vastuullinen tiede -toimitus. Saatavissa: https://vastuullinentiede.fi/fi/tutkimuksen-suunnittelu/milloin-tutkimus-tarvitsee-eettisen-ennakkoarvioinnin (Viitattu 12.9.2022)

Vehkalahti Kimmo 2019. Kyselytutkimuksen mittarit ja menetelmät. Helsingin yliopisto. Saatavissa: https://helda.helsinki.fi/bitstream/handle/10138/305021/Kyselytutkimuksen-mittarit-ja-menetelmat-2019-Vehkalahti.pdf (Viitattu 20.11.2022)

Viestintävirasto, kyberturvallisuuskeskus 2016. Terveydenhuoltoalan kyberuhkia. Saatavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Terveydenhuoltoalan_kyberuhkia.pdf (Viitattu 10.12.2022)

Vuori Jaana 2023. Tutkimusetiikka ihmistieteissä. Laadullisen tutkimuksen verkkokäsikirja. Yhteiskuntatieteellinen tietoarkisto, Tampere. Saatavissa: https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/kvali/tutkimusetiikka/tutkimusetiikka-ihmistieteissa/ (Viitattu 8.4.2023)

Liite 1. Saatekirje

Saatekirje

Arvoisa terveydenhuollon ammattilainen,

Olen tekemässä Pro Gradu-tutkielmaa **yksityisen terveydenhuollon henkilöstön tietoturva- ja tietosuojaosaamisesta ja sen kehittämisestä**. Tutkimus toteutetaan osana Itä-Suomen yliopiston sosiaali- ja terveydenhuollon tiedonhallinnan maisteritutkintoani.

Kutsu tutkimukseen
Kutsun teidät mukaan tutkimukseen ja pyydän ystävällisesti vastaamaan tutkimuskyselyyn. Tutkimus kartoittaa yksityisen terveydenhuollon henkilöstön tietoturva ja tietosuojaosaamista, jonka vuoksi teillä on aiheesta kaikkein arvokkain tieto.

Anonyymiys
Tutkimukseen osallistuminen on täysin vapaaehtoista. Tutkimusaineistoa ja tutkimustuloksia käsitellään luottamuksellisesti, eikä vastauksista voida tunnistaa yksittäistä vastaajaa tai tämän henkilöllisyyttä. Vastaamalla kyselyyn suostut siihen, että vastauksiasi voidaan hyödyntää tässä tutkimuksessa. Tietosuojaselosteen löydät kyselyn lopusta. Kyselyyn vastaaminen vie noin 15–20 minuuttia.

Tutkimuslupa
Tutkimuslupa on saatu organisaatiostasi 15.2.2023.

Kysyttävää tutkimuksesta
Annan mielelläni lisätietoja tutkimuksesta. Jos sinulla on kysyttävää, voit olla yhteydessä STTHM-opiskelija Jaila Tuoviseen.

Pyydän teitä ystävällisesti vastaamaan kyselyyn xx.xx.xxxx mennessä seuraavan linkin kautta:

VASTAA KYSELYYN

Tervetuloa vastaamaan kyselyyn!

Vastauksista etukäteen kiittäen,

Jaila Tuovinen Tiina Hassinen Heli Kumpulainen

Liite 2. Tutkimuskysely

UNIVERSITY OF
EASTERN FINLAND

TUTKIMUSKYSELY

Yksityisen terveydenhuollon henkilöstön tietoturva- ja tietosuojaosaaminen

Tervetuloa vastaamaan kyselyyn!

Tämän kyselyn tarkoituksena on kartoittaa **terveydenhuollon henkilöstön tietoturva ja tietosuojaosaamista** sekä eritellä kehityskohteita tietoturva- ja tietosuojakoulutuksen kehittämiseksi.

Kysely on anonyymi, eikä sen vastauksista ole mahdollista tunnistaa yksittäisen vastaajan henkilöllisyyttä. Vastaathan jokaiseen kysymykseen rehellisesti oman osaamisesi mukaisesti, kyselyssä ei ole oikeita tai vääriä vastauksia. Vastauksesi tuo arvokasta tietoa tietoturva- ja tietosuojaosaamisen tason kartoitukseen.

Kyselyn tallentaminen keskeneräisenä ei ole mahdollista anonymisoinnin vuoksi, joten siihen tulee vastata kerralla loppuun asti. Tutkimuksen tietosuojaselosteen löydät kyselyn lopusta.

Vastaathan kyselyyn **XX.XX.XXXX** mennessä.

Suuri kiitos vastauksestasi!

Kysymykset ovat yhden vastauksen monivalintakysymyksiä. Voit siis valita jokaiseen kysymykseen yhden itsellesi sopivimman vaihtoehdon.

Taustatiedot

1. **Työskentelen organisaatiossa**

- ◯ Lääkärinä
- ◯ Sairaanhoitajana/Terveydenhoitajana
- ◯ Terapeuttina
- ◯ Lähihoitajana
- ◯ Muussa työtehtävässä

2. **Työsuhteeni organisaatiossa on**

- ◯ Vakituinen
- ◯ Keikkalainen
- ◯ Määräaikainen
- ◯ Ammatinharjoittaja
- ◯ Muu

3. **Olen työskennellyt organisaatiossa**

- ◯ 0–5 vuotta
- ◯ 5–10 vuotta
- ◯ 10–15 vuotta
- ◯ 15–20 vuotta
- ◯ Yli 20 vuotta

Koulutustausta

Tässä osa-alueessa kartoitetaan koulutustaustaa ammatillisen koulutuksen ja tietoturva- ja tietosuojakoulutuksen osalta.

4. **Ammatillinen koulutukseni on**

- ◯ Ylempi korkeakoulututkinto
- ◯ Alempi korkeakoulututkinto
- ◯ Toisen asteen tutkinto
- ◯ Perusasteen tutkinto
- ◯ Muu

5. **Ammatilliseen koulutukseeni on sisältynyt tietoturvaan ja tietosuojaan liittyviä opintoja**

- ◯ Paljon
- ◯ Jonkin verran
- ◯ En osaa sanoa
- ◯ Vähän
- ◯ Ei ollenkaan

6. **Olen suorittanut organisaation järjestämän tietoturva- ja tietosuojakoulutuksen**

- ◯ Kyllä
- ◯ En osaa sanoa
- ◯ En

7. **Koulutus on jäänyt suorittamatta, koska**

- ◯ En ole tietoinen koulutuksesta
- ◯ Koulutuksen suoritukseen ei ole ollut aikaa
- ◯ En osaa käyttää järjestelmää, jossa koulutus on
- ◯ En koe koulutusta tärkeäksi
- ◯ Muu syy

8. **Olen suorittanut organisaation ulkopuolisia koulutuksia tietoturvaan ja/tai tietosuojaan liittyen**

- ◯ Paljon
- ◯ Jonkin verran
- ◯ En osaa sanoa
- ◯ Vähän
- ◯ En lainkaan

Turvalliset tietotekniikan käyttötaidot

Tässä osa-alueessa kartoitetaan turvallisia tietotekniikan käyttötaitoja. Vastaa kysymyksiin rehellisesti oman osaamisesi mukaisesti.

9. **Lukitsen tietokoneeni poistuessani työpisteeltä**

- ◯ Aina
- ◯ Usein
- ◯ Joskus
- ◯ Harvoin
- ◯ En koskaan

10. **Käytän työssäni vain organisaation määrittämiä työvälineitä**

- ◯ Täysin samaa mieltä
- ◯ Osittain samaa mieltä
- ◯ Ei samaa eikä eri mieltä
- ◯ Osittain eri mieltä
- ◯ Täysin eri mieltä

11. Voin käyttää työvälineitä henkilökohtaisten asioiden hoitamiseen

- ◯ Täysin samaa mieltä
- ◯ Osittain samaa mieltä
- ◯ Ei samaa eikä eri mieltä
- ◯ Osittain eri mieltä
- ◯ Täysin eri mieltä

12. Käytän samaa salasanaa useassa eri palvelussa

- ◯ Täysin samaa mieltä
- ◯ Osittain samaa mieltä
- ◯ Ei samaa eikä eri mieltä
- ◯ Osittain eri mieltä
- ◯ Täysin eri mieltä

13. Säilytän salasanoja tallessa kirjallisesti, jotta ne eivät unohdu

- ◯ Täysin samaa mieltä
- ◯ Osittain samaa mieltä
- ◯ Ei samaa eikä eri mieltä
- ◯ Osittain eri mieltä
- ◯ Täysin eri mieltä

14. Voin ladata huoletta tuntemattoman lähettäjän sähköpostin liitetiedoston

- ◯ Täysin samaa mieltä
- ◯ Osittain samaa mieltä
- ◯ Ei samaa eikä eri mieltä
- ◯ Osittain eri mieltä
- ◯ Täysin eri mieltä

Tietoturvatiedot

Tässä osa-alueessa kartoitetaan tietoturvatietoja. Vastaa kysymyksiin rehellisesti oman osaamisesi mukaisesti.

15. Tiedän mitä tietoturva tarkoittaa

- ◯ Täysin samaa mieltä
- ◯ Osittain samaa mieltä
- ◯ Ei samaa eikä eri mieltä
- ◯ Osittain eri mieltä
- ◯ Täysin eri mieltä

16. Tiedän mitä tietosuoja tarkoittaa

- ◯ Täysin samaa mieltä
- ◯ Osittain samaa mieltä
- ◯ Ei samaa eikä eri mieltä
- ◯ Osittain eri mieltä
- ◯ Täysin eri mieltä

17. Minulla on mielestäni riittävä tietoturva- ja tietosuojaosaaminen

- ◯ Täysin samaa mieltä
- ◯ Osittain samaa mieltä
- ◯ Ei samaa eikä eri mieltä
- ◯ Osittain eri mieltä
- ◯ Täysin eri mieltä

18. Tiedän keneltä voin kysyä apua tietoturva- ja tietosuoja-asioissa

- ◯ Täysin samaa mieltä
- ◯ Osittain samaa mieltä
- ◯ Ei samaa eikä eri mieltä
- ◯ Osittain eri mieltä
- ◯ Täysin eri mieltä

19. Tiedän miten toimia tilanteissa, joissa tietoturva tai tietosuoja on vaarantunut

- ◯ Täysin samaa mieltä
- ◯ Osittain samaa mieltä
- ◯ Ei samaa eikä eri mieltä
- ◯ Osittain eri mieltä
- ◯ Täysin eri mieltä

20. Tiedän mistä löydän organisaation kirjalliset tietoturva- ja tietosuojaohjeet

- ◯ Täysin samaa mieltä
- ◯ Osittain samaa mieltä
- ◯ Ei samaa eikä eri mieltä
- ◯ Osittain eri mieltä
- ◯ Täysin eri mieltä

Tietoturvataidot

Tässä osa-alueessa kartoitetaan tietoturvataitoja. Vastaa kysymyksiin rehellisesti oman osaamisesi mukaisesti.

21. Huomioin tietoturvan ja tietosuojan toteutumisen työssäni

- ◯ Täysin samaa mieltä
- ◯ Osittain samaa mieltä
- ◯ Ei samaa eikä eri mieltä
- ◯ Osittain eri mieltä
- ◯ Täysin eri mieltä

22. Olen osaltani vastuussa organisaation tietoturvasta

- ◯ Täysin samaa mieltä
- ◯ Osittain samaa mieltä
- ◯ Ei samaa eikä eri mieltä
- ◯ Osittain eri mieltä
- ◯ Täysin eri mieltä

23. Noudatan työssäni organisaation tietoturvakäytäntöjä ja ohjeita

- ◯ Täysin samaa mieltä
- ◯ Osittain samaa mieltä
- ◯ Ei samaa eikä eri mieltä
- ◯ Osittain eri mieltä
- ◯ Täysin eri mieltä

24. Autan usein kollegoitani tietoturva- tai tietosuoja-asioissa

- ◯ Täysin samaa mieltä
- ◯ Osittain samaa mieltä
- ◯ Ei samaa eikä eri mieltä
- ◯ Osittain eri mieltä
- ◯ Täysin eri mieltä

25. Osaan käyttää salattua sähköpostia ja turvapostia ja tiedän, milloin niitä tulee käyttää

- ◯ Täysin samaa mieltä
- ◯ Osittain samaa mieltä
- ◯ Ei samaa eikä eri mieltä
- ◯ Osittain eri mieltä
- ◯ Täysin eri mieltä

26. Salassapitovelvollisuuteni koskee vain potilastietoja

- ◯ Täysin samaa mieltä
- ◯ Osittain samaa mieltä
- ◯ Ei samaa eikä eri mieltä
- ◯ Osittain eri mieltä
- ◯ Täysin eri mieltä

27. Salassapitovelvollisuuteni päättyy työsuhteeni päättyessä

- ◯ Täysin samaa mieltä
- ◯ Osittain samaa mieltä
- ◯ Ei samaa eikä eri mieltä
- ◯ Osittain eri mieltä
- ◯ Täysin eri mieltä

28. Olen kohdannut työssäni tietoturvauhan

- ◯ Täysin samaa mieltä
- ◯ Osittain samaa mieltä
- ◯ Ei samaa eikä eri mieltä
- ◯ Osittain eri mieltä
- ◯ Täysin eri mieltä

Organisaation tietoturva- ja tietosuojakoulutus

Tämä osa-alue käsittelee organisaatiosi tietoturva- ja tietosuojakoulutusta. Vastaa kysymyksiin rehellisesti oman kokemuksesi mukaisesti. Viimeiseen kysymykseen voit vastata sanallisesti toiveitasi tietoturva- ja tietosuojakoulutuksesta.

29. Perehdytyksessäni on käsitelty tietoturvaa ja tietosuojaa

- ◯ Paljon
- ◯ Jonkin verran
- ◯ En osaa sanoa
- ◯ Vähän
- ◯ Ei ollenkaan

30. Koen organisaation tietoturva ja tietosuojakoulutuksen tärkeäksi

- ◯ Täysin samaa mieltä
- ◯ Osittain samaa mieltä
- ◯ Ei samaa eikä eri mieltä
- ◯ Osittain eri mieltä
- ◯ Täysin eri mieltä

31. Organisaation järjestämä koulutus tietoturvasta ja tietosuojasta on riittävää

- ◯ Täysin samaa mieltä
- ◯ Osittain samaa mieltä
- ◯ Ei samaa eikä eri mieltä
- ◯ Osittain eri mieltä
- ◯ Täysin eri mieltä

32. Toivoisin koulutusta lisää

- ◯ Tietoturvasta
- ◯ Tietosuojasta
- ◯ Tietoturvasta ja tietosuojasta
- ◯ Tarvetta lisäkoulutukselle ei ole

33. Minkälaista koulutusta toivoisit tietoturvasta ja/tai tietosuojasta?

_____

_____

Tutkimuksen tietosuojaseloste

Tutkimuksen tietosuojaselosteeseen pääset seuraavan linkin kautta: xxx