Tietosuojaperehdytys tukemassa potilasturvallisuutta terveydenhuollossa

Maria Matilainen

Opinnäytetyö, AMK
Toukokuu 2025
Tieto- ja viestintätekniikan tutkinto-ohjelma

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Kuvailulehti

Matilainen, Maria

Tietosuojaperehdytys tukemassa potilasturvallisuutta terveydenhuollossa

Jyväskylä: Jyväskylän ammattikorkeakoulu. Toukokuu 2025, 32 sivua.

Tieto- ja viestintätekniikan tutkinto-ohjelma. Opinnäytetyö AMK.

Julkaisun kieli: suomi

Julkaisulupa avoimessa verkossa: kyllä

Tiivistelmä

Tietosuoja terveydenhuollossa on ensiarvoisen tärkeää arkaluonteisten potilastietojen turvaamiseksi. Digitalisaation myötä terveydenhuollon organisaatioissa on siirrytty sähköiseen potilastietojen hallintaan, jonka myötä erilaiset riskit erilaisten tietosuojaloukkausten ja tietomurtojen osalta ovat kasvaneet. Tietosuojan toteutuminen potilaan hoidossa velvoittaa terveydenhuollon ammattilaisia toimimaan huomioiden tietoturvan ja yleisen tietosuoja-asetuksen mukaiset periaatteet päivittäisessä työssään. Tavoitteena kehitystyössä oli tarkastella millaisia vaatimuksia lainsäädäntö asettaa tietosuojalle terveydenhuollossa ja millaisella perehdytyksellä näihin vaatimuksiin voidaan vastata.

Henkilötiedoiksi on luokiteltu kaikki tiedot, joista luonnollisen henkilön pystyy tunnistamaan tai on tunnistettavissa. Tietojen käsittelyä terveydenhuollossa ohjaavat monet lait, kuten Euroopan Unionin yleinen tietosuoja-asetus (GDPR), sekä tietosuojalaki. Laissa potilastiedot on määritelty erityisen arkaluonteisiksi tiedoiksi, ja niiden käsittely on hyvin rajattua ja siihen tulee olla lailliset perusteet. Tietosuoja on henkilötietojen turvana tietojen käsittelyssä.

Tietosuojaperehdytystä varten laadittiin koulutusmateriaalin runko sekä koulutuksen sisällölle listaus, joka on esitelty työn liitteessä 1. Työn teoriaosuus käsittelee laajasti tietosuojaa ja tietoturvaa, terveydenhuollon tietojärjestelmiä ja digitaalisia palveluita, sekä terveydenhuoltoa ja tietosuojaa koskevaa lainsäädäntöä. Lisäksi laadittiin mittareita, joilla voidaan arvioida osaamista ja tukea jatkuvaa oppimista.

Liittämällä terveydenhuollon ammattilaisten perehdytykseen tietosuojaosio, voidaan kasvattaa työntekijöiden ymmärrystä tietosuojasta ja tietoturvasta, ja ehkäistä tietosuojaloukkauksia sekä tietomurtoja. Laajentamalla perehdytystä, voidaan kohdentaa tietosuojariskien tarkastelu koskemaan eri työnkuvia. Organisaatioissa päivittämällä ohjeistuksia ja tiedottamalla henkilökuntaa tietosuojaa ja tietoturvaa koskevista aiheista, voidaan edesauttaa potilasturvallisuutta ja korkealaatuista potilaan hoitoa.

Avainsanat (asiasanat)

tietosuoja, terveydenhuolto, lainsäädäntö, perehdyttäminen

Muut tiedot (salassa pidettävät liitteet)

jamk

Description

Matilainen, Maria

Familiarisation to data protection supporting patient security in health services

Jyväskylä: JAMK University of Applied Sciences. May 2025, 32 pages.

Degree Programme in Information and Communication Technology. Bachelor´s thesis.

Permission for open access publication: Yes

Language of publication: Finnish

Abstract

Data protection in healthcare is crucial to keep sensitive patient data safe. Within the digital era, healthcare organisations have moved towards to using electronic health record management, which has increased the risks of various types of data violations and data breaches. The implementation of data protection in patient care requires healthcare staff to act in line with the principles of data security and the General Data Protection Regulation in their daily work. The aim of the development work was to examine the legal requirements for data protection in healthcare and how this can be addressed.

Personal data is considered to be information, which a person can be identified or is able to be identified. The processing of data in healthcare field is governed by several laws, including the European Union's General Data Protection Regulation (GDPR) and the data protection law. The law defines patient data as particularly sensitive information, and its processing is very limited and must a have a legal basis. Data protection is the safeguard for personal data when processing data.

For the data protection familiarisation, a framework of training material was developed and a list of the context was drawn up, which is introduced in the appendix 1 of the thesis. The theory part of the thesis deals extensively with data protection and information security, healthcare information systems and digital services, and legislation on healthcare and data protection. In addition, indicators were developed to assess competences and support continuous learning.

Including a data protection part in the familiarisation of healthcare professionals would increase their understanding of data protection and information security and prevent data violations and data breaches. By broadening the scope of the induction, it is possible to focus the familiarisation of data protection risks across different job titles. In organisations, updating guidelines and informing staff about data protection and security issues can contribute to safe and high-quality patient care.

Keywords/tags (subjects)

data protection, health services, legislation, familiarisation

Miscellaneous (Confidential information)

Sisältö

Kuviot

1 Johdanto

Terveydenhuoltoala on kokenut valtavan muutoksen digitalisaation edetessä tietojärjestelmien kehittyessä ja paperisten reseptien muuttuessa sähköisiksi. Terveydenhuollossa käsitellään päivittäin ihmisten arkaluontoisia tietoja, ja tietovuotojen sekä tietosuojaloukkausten ehkäisemiseksi henkilökunnalla täytyy olla riittävät valmiudet tietojen sähköiseen käsittelyyn. Järjestelmät kehittyvät jatkuvasti ja alalla tulee sopeutua alati tapahtuviin muutoksiin ja vaatimuksiin.

Erilaiset kyberuhat sosiaali- ja terveysalalla ovat kasvaneet digitaalisten potilastietojen käyttöönoton myötä, joista on tullut arvokas hyödyke rikollisille tavoiteltavaksi. Organisaatiot ovat haavoittuvaisia esimerkiksi vanhentuneiden järjestelmien vuoksi, ja näin ollen altistuvat palvelunestohyökkäyksille, tietomurroille sekä kiristyshaittaohjelmille, jotka vaarantavat järjestelmissä olevat potilastiedot. Henkilötiedot ovat haluttuja hyödyntää erilaisissa petoksissa sekä identiteettivarkauksissa. Työntekijöihin sosiaali- ja terveysalalla kohdistuu sosiaalista manipulointia sähköposteilla ja viesteillä, kuten tietojenkalastelua ja käyttäjätunnusten anastamista. (Klauenbösch 2024.)

Elina Niemistö kirjoittaa lokakuussa 2024 julkaistussa Ylen artikkelissa terveydenhuoltoalaan kohdistuvista kyberuhista ja niiden torjunnasta. Artikkelissa on haastateltu sote-tilannekeskuksen koordinaattoria Eija Loukoa, sekä sosiaali- ja kriisipäivystyksen johtajaa Marjaana Rajasaari-Lahtea, jotka uskovat olevansa perillä tietoturva-asioista melko hyvällä tasolla ja suorittavat itse työssään tietoturvakoulutuksen joka vuosi. Loukon mukaan erilaiset varmenteet ja vahva tunnistautuminen ovat tärkeitä, kun käsitellään asiakkaiden tietoja, vaikka kirjautuminen useilla eri tunnuksilla eri järjestelmiin vie aikaa. (Niemistö 2024).

Tietoturvan parantaminen tietosuojan osalta liittyy olennaisesti potilasturvallisuuden varmistamiseen. Hoitohenkilökunnan perehdytykseen liitettävällä erillisellä tietosuojaa käsittelevällä osiolla voidaan työnantajan puolesta tukea, että uusi työntekijä ymmärtää, millä tavoin aihe käsittelee jokapäiväistä työtä. Yleisesti aiheena henkilötietojen turvaaminen ja tietosuoja linkittyvät jokaisen terveydenhuoltoalalla toimivan henkilön työhön. Klauenböschin kirjoittamassa artikkelissa todettujen johtopäätösten mukaan henkilökunnan koulutuksen priorisointi ja järjestelmien uudistaminen auttavat organisaatioita puolustautumaan kyberhyökkäyksiltä. Lähestymistapa kyberturvallisuuteen tulee olla proaktiivinen tietojen suojaamiseksi sekä luottamuksen ylläpitämiseksi. (Klauenbösch 2024.)

Kehittämistyönä tehdyssä tutkimuksessa käsitellään yleisesti tietosuojaan sekä terveydenhuoltoon liitettyjen lakien vaatimuksia, jotka koskevat henkilötietojen käsittelyä sekä tietojärjestelmien käyttöä. Näitä vaatimuksia sovelletaan sekä julkiseen että yksityiseen terveydenhuoltoon, sekä sosiaalipalveluihin. Perehdytysmateriaalin sisältö on luotu työn teoriaosuuden pohjalta, ja materiaaliin on koottu tärkeimmät ja välttämättömät läpikäytävät aihepiirit. Perehdytyksen lopussa olevan testin avulla voidaan tarkastella oppimiskokemusta ja tulosta, ja testissä työnkuvaan liitetyillä esimerkeillä voidaan havainnollistaa työntekijälle, miten perehdytyksessä käsitelleitä asioita sovelletaan käytännössä. Työssä esiteltävä perehdytysmalli on helposti päivitettävissä mahdollisten muutosten ilmi tullessa, ja perehdytystä voidaan jatkokehittää mallin pohjalta.

2 Tutkimuksen lähtökohdat

2.1 Tutkimusasettelu ja tutkimuskysymykset

Tutkimusasetelmana on tietosuojan ja sen erityispiirteiden tarkastelu terveydenhuoltoalalla ja riittävän tietosuojaperehdytyksen takaaminen terveydenhuollon henkilökunnalle. Tietosuojaa tarkastellaan terveydenhuollossa käytettävien tietojärjestelmien sekä valtiollisten että kansallisten lakipykälien ja asetusten kautta. Tutkimuksen tuloksena luotua perehdytykseen käytettävää mallia voidaan hyödyntää ennaltaehkäisemään tietosuojaloukkauksia potilastietojen käsittelyssä.

Tutkimuskysymyksiä tarkastellaan lainsäädännön tuomien vaatimusten pohjalta, ja kuinka varmistetaan, että henkilökunta on riittävän koulutettu käsittelemään arkaluontoisia tietoja. Tutkimuksessa pyrkimyksenä on vastata kahteen seuraavanlaiseen kysymykseen:

1. Mitä vaatimuksia lainsäädäntö asettaa tietosuojalle terveydenhuoltoalalla?
2. Millaisella henkilökunnan perehdyttämisellä voidaan tukea vaatimusten toteutumista?

2.2 Tutkimusmenetelmä

Työ toteutetaan kehittämistyönä, jonka lopputuloksena saadaan terveydenhuoltoalalle kehitettyä perehdytystä varten koulutusmateriaali tietosuojaan ja tietojen käsittelyyn liittyen. Tietosuojaperehdytyksen lähtökohdat perustuvat laissa esitettyihin vaatimuksiin potilasturvallisuuden ja henki-

lötietojen suojaamisen osalta. Vaatimusten perusteella perehdytyksessä nostetaan esille päivittäiseen työhön vaikuttavat tärkeimmät asiakohdat. Nämä tuodaan esille niillä tavoin, että perehdytysmalli on helposti jatkokehitettävissä ja sovellettavissa terveydenhuoltoalan eri ammattilaisten perehdytykseen.

Tutkimuksellisella kehittämistoiminnalla yhdistetään aiheeseen lähestyminen tutkimuksellisesti sekä konkreettinen toiminta. Tutkimuksen lähtökohtana on työelämän käytännön ongelmat, ja olennaiset kysymykset, joilla ohjataan tutkimuksen toteutumista. Tutkimuksen tarkoituksena ei ole ratkaista yhtä yksittäistä esille noussutta ongelmaa, vaan luoda aiheesta laajempaa keskustelua. (9 Työelämän tutkiva kehittämistoiminta 2022.)

3 Tietosuoja ja tietojärjestelmät

3.1 Tietosuoja henkilötietojen turvana

Tietosuoja turvaa henkilön oikeuksia sekä vapauksia, kun hänen henkilötietojansa käsitellään. Tietosuojalla säilytetään tietojen luottamuksellisuus ja niiden luvaton käyttö. Tämän pohjalta henkilötietoja on oikeutettu käsittelemään vain ne, joiden työtehtäviin tämä kuuluu. Tietosuojalla osoitetaan, millaisin edellytyksin ja missä tilanteissa tietoja käsitellään ja millaisia oikeuksia henkilöllä on omiin tietoihinsa. (Tietoturva sosiaali- ja terveydenhuollossa 2024.)

Henkilötiedoiksi luokitellaan kaikki tieto, joiden avulla luonnollinen henkilö voidaan tunnistaa tai on tunnistettavissa. Tietosuoja turvaa henkilötietoja, ja on perusoikeus, jonka avulla taataan yksilön oikeudet henkilötietoja käsiteltäessä. Henkilötiedoiksi luokitellaan esimerkiksi nimi, puhelinnumero, henkilötunnus, IP-osoite, sähköpostiosoite, potilastiedot ja sijaintitiedot. (Tietosuoja n.d.) Euroopan Unionissa henkilötietojen keräämistä ja säilyttämistä, sekä hallinnointia ohjaa yleinen tietosuoja-asetus: GDPR. Asetuksen vaatimuksia sovelletaan EU:ssa käsiteltyjen tietojen lisäksi ulkopuolisiin organisaatioihin, jotka käsittelevät EU:ssa asuvien ihmisten henkilötietoja (Yleinen tietosuoja-asetus n.d.)

Ihmistä tai organisaatiota, joka käsittelee henkilötietoja, kutsutaan rekisterinpitäjäksi. Rekisterinpitäjä, esimerkiksi terveydenhuollon yksikkö, määrittelee, millä tavoin tietoja kerätään ja millaiseen

tarkoitukseen. Rekisterinpitäjän lukuun henkilötietoja käsittelevää ihmistä tai organisaatiota kutsutaan henkilötietojen käsittelijäksi, ja tällainen voi olla esimerkiksi IT-henkilöstö, jolla on vastuu ja pääsy rekisterinpitäjän henkilötiedoista (Henkilötietojen käsittely n.d.)

Henkilötietoja keräävillä yrityksillä on velvollisuus julkisesti ilmaista tietosuojaselosteessa, mitä tietoja rekisteröidyistä, esimerkiksi asiakkaista kerätään ja miten tietoja käsitellään. Selosteessa kuvaillaan, miksi ja millä tavoin tietoja kerätään, ja kuinka ne säilytetään. Euroopan Unionin yleisen tietosuoja-asetuksen, GDPR, mukaan viestinnän henkilötietojen käsittelyä koskien tulee olla ymmärrettävää ja helposti saavutettavissa. Selosteen tulee olla saatavilla maksutta, sekä erillään sopimus- sekä käyttöehdoista. (Tietosuojaselosteen laatiminen – lataa malli Sopimuskoneesta 2024.)

Tietosuojapoikkeamalla tai -loukkauksella tarkoitetaan henkilötietojen vaarantumista, häviämistä, tuhoutumista, luvatonta luovutusta tai tilannetta, jossa luvaton taho pääsee tietoihin käsiksi. Tilanteen havaittuaan rekisterinpitäjän on tehtävä ilmoitus viranomaiselle (ks. 4.1) 72 tunnin sisällä. Lisäksi tilanteesta on ilmoitettava viivyttämättä rekisteröidylle ymmärrettävällä ja selkeällä kielellä. Rekisteröidylle tulee myös toimittaa organisaation tietosuojavastaavan yhteystiedot. (Usein tietosuojaloukkaus havaitaan liian myöhään, joskus ei lainkaan n.d.). Tietosuojavastaava on organisaation työntekijä, jonka tehtävänä on ylläpitää tietosuojaohjeistuksien noudattamista ja valvoa henkilötietojen käsittelyä. Lisäksi hän ohjeistaa työntekijöitä, toimii rekisteröityjen yhteyshenkilönä tietosuoja- ja henkilötietoasioissa ja toimii yhteistyössä tietosuojavaltuutetun toimiston kanssa. (Tietosuojavastaavat n.d.)

3.2 Tietoturva

Tietoturvan avulla suojataan käyttäjien arkaluonteisia tietoja, ja sen avulla käyttäjä voi ymmärtää oman toimintansa ja asiayhteyden tiedoissa, ja estämään tietojen menettämisen tai niiden luvattoman käytön. Tietoihin liittyvien riskien lieventäminen on tärkeää lisääntyneiden kyberturvallisuusuhkien myötä. Tietoturvaan ja tietojen suojaamiseen liittyen Microsoftin verkkosivuilla on kuvattu tietoturvan määritelmää ja erilaisia tietoturvatyyppejä seuraavasti alla olevan listauksen mukaan (Mitä tietoturva on? N.d.):

- käyttöoikeudet
- salasanat ja biometriset tunnisteet

- varmuuskopiot ja niiden palautukset
- tietojen vikasietoisuus järjestelmien palautusta ja liiketoiminnan jatkuvuutta varten
- tietojen poistaminen, asianmukainen hävittäminen
- tietojen peittäminen
- tietojen katoamisen estäminen
- tiedostojen salaukset
- tietojen salaaminen, tietojen luokittelu
- käyttäjien riskien hallinta

Tietosuojan toteutumiseen yksi keino on tietoturva. Sen avulla voidaan suojata aineistoa sekä järjestelmiä, joissa säilytetään tietoja. Tietoturvan osalta tarkoitetaan organisaation sisäisiä sekä teknisiä toimia, joiden avulla voidaan varmistaa tietojen eheys sekä luottamuksellisuus, rekisteröidyn osalta oikeuksien toteutuminen ja järjestelmien käytettävyys. (Mitä eroa on tietosuojalla ja tietoturvalla? n.d.)

Tietoturvan osalta organisaation työntekijät voivat vaikuttaa päivittäisellä toiminnallaan sen toteutumiseen. Arkisia toimenpiteitä terveydenhuollossa ovat työaseman luvattoman käytön estäminen lukitsemalla työasema, kun poistuu tämän ääreltä. Fyysisesti turvallisuudesta voi huolehtia lukitsemalla ovet ja siirtämällä esillä olevat paperit lukittuun tilaan välttääkseen tilanteen, jolloin ulkopuoliset pääsisivät näihin käsiksi. Työasemalla on tärkeää olla ajantasainen virustorjuntaohjelma, sekä palomuuri, joista vastaa organisaation IT- tai käyttötuki. Työntekijällä ammattikortit, salasanat, ja käyttäjätunnukset ovat henkilökohtaisia, ja toisen henkilön tunnisteilla potilaan tietojen tarkistaminen katsotaan luvattomaksi käytöksi. Asiakastietojen katselusta potilastietojärjestelmissä jää lokiin merkintä, ja luvaton käyttö on rikoslain nojalla rangaistavaa. Lisäksi työntekijän tulee pitää huoli sähköpostin, verkkokalenterien sekä kokousympäristöjen turvallisuudesta pitämällä tiedot ja viestit yksityisinä niiltä osin, kun niitä ei ole tarvetta jakaa. (Tietoturva sosiaali- ja terveydenhuollossa 2024.)

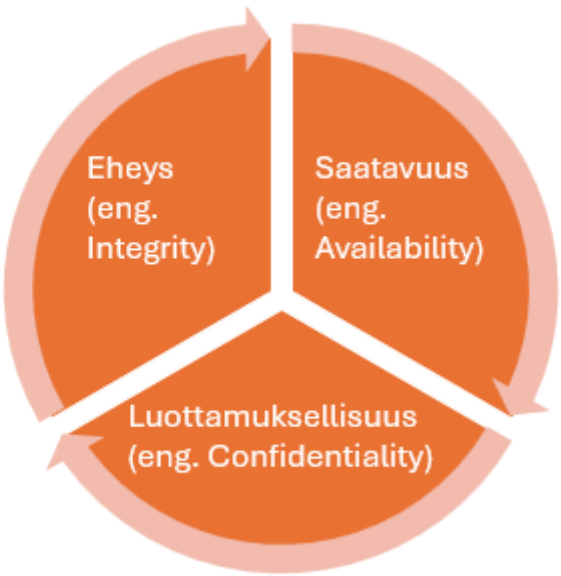
ISO/IEC 27001-standardin mukaisella sertifioinnilla yrityksen tietoturvallisuuden hallintajärjestelmästä voidaan todeta, että yrityksessä tunnistetaan mahdolliset tietoturvariskit ja että yritys työskentelee aktiivisesti tietoturvallisuuden kehittämiseksi. Sertifioitu hallintajärjestelmä osoittaa, että yritys johtaa tietojen turvaamista pitääkseen ne suojattuna, käytettävissä sekä eheinä. Erityisesti terveydenhuoltoalan yritykset hyötyvät sertifioinnista. Keskeisiä vaatimuksia sertifioinnin saa-

miseksi ovat esimerkiksi tietoturvariskien hallinta, henkilöstön asianmukainen koulutus, dokumentoitu tietoturvallisuuden hallintajärjestelmä sekä yrityksen johdon sitoutuminen tietoturvallisuuden hallintaan. (Tietoturvan hallintajärjestelmän ISO/IEC 27001- sertifiointi n.d.)

3.3 Kyberturvallisuus ja tiedon suojaaminen

Kyberturvallisuus voidaan luokitella yhdeksi tietoturvan osa-alueeksi niissä olevien erojen vuoksi. Tietoturvaan sekä kyberturvallisuuteen liittyvät uhat ovat erilaisia, kun kyberturvallisuuden osalta pyritään estämään haittaohjelmien aiheuttamia vahinkoja, niin tietoturvaan liittyy myös väärien tietojen välttämisen lisäksi myös tiedon levittämisen estäminen. Kyberturvallisuudessa keskitytään verkossa olevien laitteiden ja tietojärjestelmien, sekä näiden sisältämän tiedon turvallisuuden varmistamiseen. (Mitä on kyberturvallisuus? n.d.)

Kyberturvallisuudesta puhuttaessa voidaan käyttää lyhennettä CIA, tai CIA-mallia kuvaamaan sen eri osa-alueita. CIA-mallissa kolme eri osatekijää ovat tiedon luottamuksellisuus, eheys ja saatavuus (CIA-arvojen mukaisen luokittelun käyttöönotto Digiturvamallissa n.d.), jotka voidaan kuvata liittyvän toisiinsa kuviossa 1 esitetyllä tavalla.



Kuvio 1. CIA-malli

Terveydenhuoltoalalla CIA-mallia voidaan hyödyntää kuvaamaan eri tietojärjestelmien tietoturvavaatimuksia, jotta voidaan varmistaa asiakas- ja potilastietojen käsittelyn luottamuksellisuus, eheys ja saatavuus. Saatavuutta voidaan kuvata tässä tapauksessa käytettävyydellä. Luottamuksellisuudella tarkoitetaan sitä, että asiakas- ja potilastietoja käsittelevät vain ne henkilöt, joilla on siihen oikeus, esimerkiksi tietojärjestelmässä henkilöllä tulee olla hoitosuhde olemassa. Tiedot säilyvät eheinä, mikäli niiden muuttamisessa käytetään ammattilaisen varmistusta allekirjoituksella, ja tiedoissa ei ole ristiriitoja tietojärjestelmän ja Kanta-palveluiden välillä. Palvelunantajien tulee pystyä hakemaan potilastietoja esimerkiksi Kannasta, silloin kun tietoja tarvitaan, jotta ne ovat saatavilla tai käytettävissä. (Sosiaali- ja terveydenhuollon tietojärjestelmät n.d.)

3.4 Terveydenhuollossa käytetyt tietojärjestelmät

Asiakastietolain 3 §:n 19. kohdassa tietojärjestelmä määritetään ohjelmistona, järjestelmänä tai sen osana, joka on tarkoitettu asiakastietojen sähköiseen käsittelyyn, asiakirjojen tallentamiseen, ja jolla sosiaali- ja terveydenhuollon henkilökunta hyödyntää tietoja. Terveydenhuollossa näitä järjestelmiä kutsutaan potilastietojärjestelmiksi, ja näissä käsitellään potilaiden tietoja sekä asiakirjoja. Esimerkkejä potilastietojärjestelmistä ovat esimerkiksi kuvantamisen, laboratorion ja suun terveydenhuollon tietojärjestelmät. Sosiaalihuollossa käytettävistä tietojärjestelmistä käytetään nimitystä asiakastietojärjestelmä. (Kurvinen & Voutilainen 2024, 49.)

Terveyden ja hyvinvoinnin laitos (THL) on julkaissut vuonna 2024 määräyksen, jonka pohjalta terveydenhuollossa käytettävät tietojärjestelmät voidaan jakaa kahteen eri luokkaan, sertifioitavat (A) ja ei-sertifioitavat (B). Sovellusten ja järjestelmien luokittelun pohjalta suoritetaan sertifiointiin ja rekisteröintiin liittyviä toimenpiteitä. Asiakkaan tietojen käsittelyyn liittyvien riskien osalta tehdään arvio palveluntuottajien ja sovellusten valmistajien toimesta, ja järjestelmien tietoturvallisuus suunnitellaan tehdyn riskiarvion pohjalta. (Määräys sosiaali- ja terveydenhuollon tietojärjestelmien ja hyvinvointisovellusten luokittelusta ja sertifioinnista 2024.)

Terveydenhuollossa käytetyt asiakas- sekä potilastietojärjestelmät on rekisteröitävä Valviran ylläpitämään rekisteriin. Asiakastietolain 80 §:n 1 momentissa on määritelty, että palvelun tuottajan on ilmoitettava järjestelmästä Valviraan ennen käyttöönottoa tuotannossa. Lain 2 momentin mukaan rekisteristä on löydyttävä tietyt, ajantasaiset tiedot. Luokan A potilas- sekä asiakastietojärjes-

telmien osalta tämä tarkoittaa muun muassa käyttötarkoitusta, järjestelmän täyttämiä vaatimuksia, tehtyjen testauksien tulokset, tietoturvallisuuden arviointia sekä mahdollisia poikkeamia niiden keston ajan. (Kurvinen & Voutilainen 2024, 51.)

Asiakastietolain nojalla palveluiden tuottajia velvoitetaan seuraamaan järjestelmän tuotantokäyttöä sekä vaatimusten muutoksia. Poikkeamista on viipymättä ilmoitettava järjestelmää käyttäville apteekeille, sekä palvelunantajille. Luokan A tietojärjestelmien osalta ilmoitus on tehtävä olennaisten muutosten osalta myös Kansaneläkelaitokselle, Valviralle, sekä tietoturvallisuutta arvioivalle laitokselle. (Kurvinen & Voutilainen 2024, 52.)

3.5 Asiakkaiden käytössä olevat digitaaliset palvelut

Nykyisin sosiaali- ja terveyspalveluita tarjotaan yhä enemmän erilaisten digitaalisten palveluiden tai ratkaisujen kautta. Digitaaliset vastaanotot, sekä neuvonta ovat yleistymässä, ja asiakkaat käyttävät palveluita myös omien tietojen tarkastamiseen sekä aikojen varaamiseen ammattilaiselle. Digitaaliset ratkaisut voivat täydentää tai jopa korvata perinteiset vastaanotot ja toimintatavat, ja luoda täysin uusia tapoja palvelujen tarjoamiseen. (Digitaaliset palvelut 2024.)

Digitaalisten palveluiden osalta tiedonhallintalain 14 § edellyttää, että tietojen vastaanottajan on tunnistauduttava tai henkilöllisyydestä on varmistuttava, ennen kuin hän pääsee käsittelemään salassa pidettävää tietoa. Tiedonsiirron tapahtuessa tietojärjestelmien välillä, varmistuksena voidaan käyttää palvelinvarmennetta. Luonnollisen henkilön tapauksessa voidaan käyttää esimerkiksi sähköistä tunnistautumista, tai turvasähköpostia, jos tämä voidaan suojata esimerkiksi henkilön matkapuhelimeen lähetettävällä koodilla. (Kurvinen & Voutilainen 2024, 56.)

2021 annetun lain sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä 24 § mukaan henkilö voi valtuutuksen tai holhoustoimesta annetun lain (442/1999) 29 §:n 2 momentin mukaan käsitellä toisen henkilön puolesta hänestä tietojärjestelmiin tallennettuja tietoja. Lisäksi huoltajalla on pääsääntöisesti oikeus käsitellä huollettavansa tietoja. (Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä 2021.)

3.6 Tapaus Psykoterapiakeskus Vastaamo

3.6.1 Tietomurron tausta ja tapahtumat

Psykoterapiakeskus Vastaamoon kohdistui tietomurto, joka tuli ilmi julkisesti 21.10.2020, ja tietomurrossa varastettiin noin 40 000 potilaan nimiä, henkilötunnukset sekä potilastietoja. Potilastietokantaan hakkeroitunut henkilö julkaisi tiedot salatussa Tor-verkossa, ja näillä tiedoilla kiristettiin psykoterapiakeskuksen johtoa sekä asiakkaita. Tietomurron yhteydessä käyttäjärekisteristä tehtiin kopio ja se tuhottiin palvelimilta. (Case Vastaamo n.d.)

Vastaamon tietomurrosta tehtiin tietoturvayhtiö Nixun toimesta tekninen tutkinta, joka valmistui lokakuussa 2020, ja tämän perusteella todettiin, että potilastietoihin oli päästy käsiksi joulukuussa 2018 sekä maaliskuussa 2019 luvatta. Tapahtumista ei ollut kuitenkaan säilytetty lokitietoja, joten tarkkaa aikaa ei pystytty määrittelemään. Ulkopuolisten hyökkääjien käytössä olleita tekniikoita tai verkko-osoitteita ei myöskään pystytty määrittelemään, sillä dokumentaatio on ollut puutteellista. (Psykoterapiakeskus Vastaamolle seuraamusmaksu tietosuojarikkomuksista 2021.)

Tutkinnan perusteella apulaistietosuojavaltuutetun mukaan Vastaamon olisi täytynyt olla jo 2019 tapahtuneen luvattoman pääsyn jälkeen tietoinen siitä, että potilastietojärjestelmässä olevat tiedot ovat päätyneet ulkopuolisen käsiin. Tuolloin maaliskuussa yhden päivän aikana tietokanta todennäköisesti tuhottiin, ja sen ohella palvelimelle jätettiin hyökkääjän toimesta kiristysviesti, jossa hyökkääjä ilmoitti ladanneen potilastietokannan itselleen. Tietoturvaloukkauksesta olisi jo tuolloin täytynyt ilmoittaa viipymättä rekisteröidyille sekä tietosuojavaltuutetulle sen korkean riskin vuoksi. (Psykoterapiakeskus Vastaamolle seuraamusmaksu tietosuojarikkomuksista 2021.)

Potilastietokannan vuotamiseen ja tietomurtoon todennäköisin syy Nixun tekemän tutkinnan mukaan on ollut tietokannassa ollut MySQL-portti, joka on ollut suojaamaton ja sen pääkäyttäjätunnusta ei ollut suojattu salasanalla ollenkaan. Tunnukselle oli myös mahdollista kirjautua minkä tahansa IP-osoitteen takaa. Tietokannan palvelin on ollut ilman suojausta auki 26.11.2017-13.3.2019 välisen ajan, jopa pidempään. (Psykoterapiakeskus Vastaamolle seuraamusmaksu tietosuojarikkomuksista 2021.)

3.6.2 Seuraukset ja yhteiskunnallinen näkökulma

Kortesoja (2022) käsittelee tapaustutkimuksessaan psykoterapiakeskus Vastaamon tietomurtoa, jolloin keskuksen asiakkaiden potilas- sekä henkilötietoja vuodettiin verkkoon vuonna 2020. Tutkimuksessa käsitellään tapausta yhteiskunnallisen ongelman esimerkkinä, joka kulminoituu siihen, kuinka merkittävä ongelma on asiakkaiden luottamuksellista informaatiota keräävien yritysten puutteellinen valvonta, jonka seurauksena potilaan tietosuojaa voidaan pitää entistä haavoittuvampana. Tapaustutkimuksessa esitetään, että tietoturvaan keskittyvien teknologiaan liittyvien ratkaisujen lisäksi tarvitaan yhteiskunnallista keskustelua. (Kortesoja 2022.) Keskustelua voitaisiin parantaa jo terveydenhuollon henkilökunnan perehdytysvaiheessa.

Kortesoja tuo tapaustutkimuksessaan ilmi sen, mikäli Vastaamon tietomurron taustalla syynä olisi ollut laiskuutta tai budjettisyitä, tähän voitaisiin yksinkertaisena ratkaisuna kehittää yritysten tietoteknistä osaamista sekä kasvattaa resursseja kyberuhkien torjunnassa, ja toteuttaa auditointia sekä tiukentaa lainsäädäntöä. Potilastietoja käsittelevissä yrityksien osalta Kortesoja mainitsee, että julkisuudessa olisi tärkeää tuoda ilmi kansalaisille, minkä vuoksi heiltä kerätään luottamuksellista tietoa ja kenellä, sekä millaisilla ehdoilla tietoihin päästään käsiksi. (Kortesoja 2022.)

4 Lainsäädäntö

4.1 Yleiseen tietosuojaan liittyvä lainsäädäntö

Tietosuojalaissa täsmennetään sekä täydennetään luonnollisten henkilöiden suojelua heidän henkilötietojansa käsitellessä ja tietojen vapaasta liikkuvuudesta perustuen Euroopan parlamentin sekä neuvoston yleiseen tietosuoja-asetukseen (EU) 2016/679. Lakia ei sovelleta henkilötietojen käsittelyyn, josta säädetään rikosasioissa ja kansallisen turvallisuuden ylläpitämiseen annetussa laissa (1054/2018). Suomen lakia sovelletaan, mikäli rekisteripitäjän toimipaikka on Suomessa ja henkilötietojen käsittely tapahtuu Euroopan Unionin alueella sijaitsevan rekisterinpitäjän toimintojen yhteydessä. (Tietosuojalaki 2018.)

Yleistä tietosuoja-asetusta sovelletaan laissa laajasti silloin, kun henkilötietojen käsittely on jollain osin tai kokonaisuudessaan automaattista, tai mikäli se muodostaa tai sen on tarkoituksena muodostaa osa rekisteristä. Henkilötietojen osalta tietosuoja-asetuksessa on määriteltynä reunaehdot

käsittelylle, jonka avulla pyritään EU:n alueella henkilötietojen vapaaseen liikkuvuuteen. Tietosuoja-asetuksessa täsmennetään esimerkiksi henkilötiedon ja rekisterinpitäjän käsitteet, ja säädetään rekisteröidyllä olevista oikeuksista, tietojen käsittelyn periaatteista ja sisäänrakennetusta sekä oletusarvoisesta tietosuojasta. (12.5 Tietosuojalainsäädäntö n.d.)

Henkilötietojen käsittelyn ollessa lainmukaista, täytyy olla sopiva käsittelyperuste. Tällainen peruste voi olla rekisteröidyn oma suostumus tietojen käsittelyyn, rekisterinpitäjää koskeva lakisääteinen velvoite ja rekisterinpitäjän, kolmannen osapuolen tai yleinen etu, sekä julkinen valta. Käsittelyn tulee olla asianmukaista, ja suhteutettu kohtuullisesti käsittelyn tarkoitukseen. Henkilötietojen käsittelyn vaikutuksia rekisteröidylle tulee rekisterinpitäjän arvioida, ja käsittelystä on kerrottava läpinäkyvällä tavalla selkeästi. (Lainmukaisuus, asianmukaisuus ja läpinäkyvyys n.d.)

Tietosuoja-asetuksen 5 artiklan 2 kohdan mukaan henkilötietojen rekisterinpitäjää koskee osoitusvelvollisuus, jolloin on pystyttävä osoittamaan, että tietojen käsittelyssä on noudatettu tietosuojaperiaatteita. Periaatteita on noudatettava tietojen käsittelyn kaikissa vaiheissa. Noudattamisen osoittaminen vaatii rekisterinpitäjältä tietojen käsittelyn osalta yhä tarkempaa suunnittelua sekä dokumentointia. (Andreasson, Riikonen & Ylipartanen 2019, 31.)

Tietosuojalain valvontaviranomaisena kansallisesti, oikeusministeriön hallinnonalalla toimii tietosuojavaltuutettu. Tietosuojavaltuutettu toimii riippumattomasti ja itsenäisesti. Tietosuojavaltuutetun toimistossa virallisesti toimii vähintään kaksi apulaistietosuojavaltuutettua, ja lisäksi työhön perehtynyt muu henkilöstö sekä esittelijät. Toimikausi varsinaisella tietosuojavaltuutetuilla ja apulaistietosuojavaltuutetuilla on valtioneuvoston nimittämänä viisi vuotta, jolloin heidät vapautetaan muun viran suorittamisesta täksi ajaksi. (Tietosuojalaki 2018.)

Omien henkilötietojen osalta rekisteröidyllä on oikeus ilmoittaa tietosuojavaltuutetulle, mikäli tietojen käsittelyssä rikotaan tietosuojalakia. Valtuutetun tulee käsitellä 77 artiklan nojalla vireillä oleva kantelu kolmen kuukauden kuluessa, tai viivästyessä ilmoitettava rekisteröidylle arvio päätöksen antoajankohdasta. Tietosuojavaltuutetun laiminlyödessä velvollisuuttaan 3 momentissa ilmoitetun kolmen kuukauden kuluessa, rekisteröity voi tehdä valituksen hallinto-oikeuteen. (Tietosuojalaki 2018.)

4.2 Terveydenhuoltoon liittyvä lainsäädäntö

Terveydenhuoltopalvelut Suomessa jaetaan julkisen terveydenhuollon sekä yksityisen terveydenhuollon tarjoamin sosiaali- ja terveyspalveluihin. Julkisesta terveydenhuollosta vastaavat hyvinvointialueet, HUS-yhtymä sekä Helsingin kaupunki. Yksityinen terveydenhuolto perustuu potilaan omaan tai vakuutuksen kautta saatuun rahoitukseen, ja terveyspalvelut täydentävät julkisen terveydenhuollon palveluita. (Terveyspalvelut n.d.) Sosiaali- ja terveydenhuollon järjestämisestä koskevaa lakia sovelletaan hyvinvointialueiden vastuulla olevaan sosiaali- ja terveydenhuoltoon, sekä Helsingin kaupunkiin ja HUS-yhtymään niiltä osin, kun ne järjestävät Uudellamaalla annetun lain (20.12.2022/1185) mukaista terveydenhuoltoa (29.6.2021/612 Laki sosiaali- ja terveydenhuollon järjestämisestä 2023.)

Lainsäädännön mukaan sosiaali- ja terveydenhuolto hyvinvointialueilla on suunniteltava ja toteuttava asiakkaiden tarpeiden edellyttämällä tavalla. Yksilöllisestä hoidon tarpeen arvioinnista säädetään erikseen. Yhdenvertaisuuden tulee toteutua palveluiden toteutuksessa, ja hyvinvointialueen on turvattava sen tarjoamien palveluiden saavutettavuus sekä esteettömyys. (29.6.2021/612 Laki sosiaali- ja terveydenhuollon järjestämisestä 2023.)

Yhdenvertaisuutta edistää kaksikielisellä hyvinvointialueella asiakkaan mahdollisuus saada palvelua valitsemallaan kielellä, suomeksi tai ruotsiksi. Lisäksi saamelaisissa kunnissa asiakkaalla on oikeus käyttää saamen kieltä. Pohjoismaiden kansalaisilla on myös oikeus käyttää suomen, islannin, ruotsin, norjan tai tanskan kieltä Pohjoismaisen sosiaalipalvelusopimuksen 5. artiklassa esitetyllä tavalla. (29.6.2021/612 Laki sosiaali- ja terveydenhuollon järjestämisestä 2023.)

Potilaslaissa määritellään potilaan oikeudet terveydenhuollossa ja sairaanhoidossa. Laissa on määritetty, että jokaisella Suomessa asuvalla on oikeus terveydentilan vaatimaan hoitoon. Hoidon kiireellisyyden mukaan se toteutetaan viipymättä, mikäli kyseessä on potilaan henkeä tai terveyttä uhkaava tilanne. Terveydenhuoltolaissa määritellään hoidolle hoitotakuu, eli määräaika, jolloin potilaan tulee päästä hoidon piiriin. Potilaalla on itsemääräämisoikeus, jolloin terveydenhuollon ammattilaisen tulee toteuttaa hoito yhteisymmärryksessä potilaan kanssa. Potilaan ollessa tyytymätön saamaansa hoitoon, hän voi tehdä asiasta ilmoituksen terveydenhuollon yksikön johtoon, tai kantelun valvontaviranomaiselle. (Potilaslaki eli laki potilaan asemasta ja oikeuksista n.d.)

4.3 Tietojen käsittely terveydenhuoltoalalla

Terveydenhuoltoalalla kaikki potilas- ja asiakastiedot luokitellaan henkilötiedoiksi, ja näiden käsittelyssä sovelletaan kansallista lainsäädäntöä Euroopan Unionin yleiseen tietosuoja-asetukseen. Henkilötietoja käsitellessä toimenpiteet suunnittelusta mahdolliseen henkilötietojen poistamiseen saakka luokitellaan tietojen käsittelyyn. Yleisen tietosuoja-asetuksen lisäksi sovelletaan sähköisestä käsittelystä, potilaan sekä sosiaalihuollon asiakkaan oikeuksista ja asemasta annettuja lakeja. (Potilas- ja asiakastietojen ja henkilötietojen käsittely n.d.)

1.1.2024 voimaan tullut laki asiakastietojen käsittelystä sosiaali- ja terveydenhuollossa selkiyttää sääntelyä ja säännöksiä sosiaalihuollossa kirjattavien potilastietojen käsittelystä, sekä tiedonsaantioikeutta sosiaali- ja terveydenhuollon välillä. Lakeja on uudistettu asiakaslähtöisesti niin, että palvelut yhdessä muodostavat asiakkaalle sopivan kokonaisuuden. (Uusi laki sääntelemään sosiaali- ja terveydenhuollon asiakastietojen käsittelyä 2023.)

Jotta sosiaali- ja terveydenhuollon palveluita on mahdollista järjestää, täytyy käsitellä potilaiden ja asiakkaiden tietoja. Terveydenhuollossa käsiteltävät tiedot liittyvät potilaan terveydentilaan tai toimintakykyyn, ja näitä ovat esimerkiksi henkilön elintavat, perhe-elämään tai vapaa-aikaan liittyvät asiat sekä muut henkilökohtaiseen omaan oloon liittyvät asiat. Tietosuoja-asetuksessa johdanto-osan 51 kohdan mukaan nämä tiedot määritellään erityisen arkaluonteisiksi, sillä näiden joutuessa vääriin käsiin vaarannetaan henkilön perusoikeuksien toteutumista. (Kurvinen & Voutilainen 2024, 56.)

Potilaalla eli rekisteröidyllä sosiaali- sekä terveydenhuollossa on oikeus saada tietoon hänestä järjestelmiin tallennetut tiedot, omat oikeudet sekä velvollisuudet ja muut tärkeät asiaan liittyvät toimenpiteet ja niiden vaikutukset. Potilaalla on oikeus pyytää virheellisten tietojen korjaamista, sekä saada tietoon asiakirjat, jotka ovat vaikuttaneet tai voineet vaikuttaa asian käsittelyyn. Rekisteröidyn tulee antaa yksilöllinen suostumus tietojen luovuttamiseksi henkilörekisteristä sosiaali- ja terveydenhuollossa. (Asiakkaan ja potilaan oikeudet n.d.). Potilaan asiakirjoissa olevia tietoja koskee salassapitovelvollisuus, ja arkaluontoisuuden vuoksi tietoja koskee käsittelykielto, joka rajaa tietojen käsittelyn laissa säädettyisiin perusteisiin. Salassapitovelvollisuus perustuu potilaslakiin, ja

tietoja ei saa luovuttaa sivullisille ilman potilaan omaa suostumusta. Hoitoa tarjonnut yksikkö vastaa potilasasiakirjojen säilytyksestä, ja säilytysajan päätyttyä asiakirjat tulee hävittää. Salassapitovelvollisuuden lisäksi potilastietoja koskee vaitiolovelvollisuus. (Potilasasiakirjojen käsittely n.d.)

5 Tietosuojaperehdytyksen suunnittelu

5.1 Suunnittelun lähtökohta

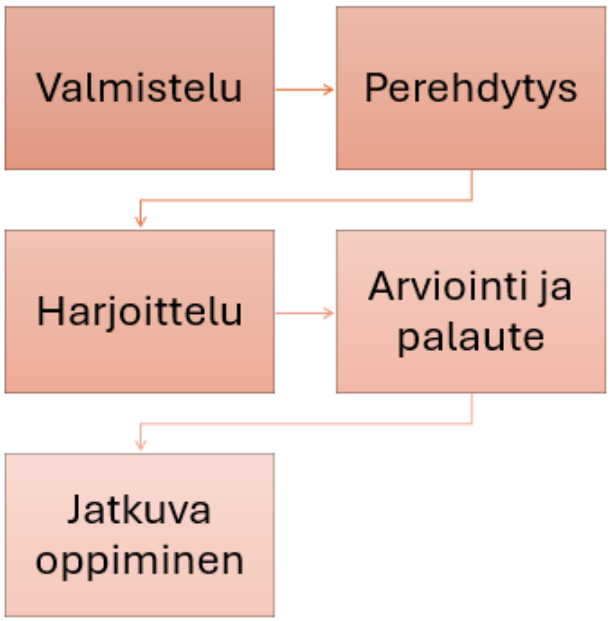
Perehdytyksen suunnittelussa on hyvä ottaa huomioon työpaikan arvot, ja se, miten esimerkiksi digitaalisuus voidaan yhdistää luontevasti osaksi perehdytysprosessia. Hyvällä perehdytyksellä ylläpidetään veto- sekä pitovoimaa palvelualoilla, ja perehdytykseen panostaminen on kannattava investointi taloudellisesta näkökulmasta. Lisäksi työturvallisuus, sekä työhyvinvointi parantuu ja lisääntyy, sekä henkilöstö viihtyy työssään. (Perehdytys lähtee suunnittelusta n.d.)

Perehdytyksen aikana on hyvä pohtia työpaikan asenteita ja ilmapiiriä, sekä mihin arvoihin perehdytys nojautuu. Yksilöllisesti perehdytys voidaan suunnitella huomioiden eri ikäiset, kieli- ja kulttuuritaustaiset sekä erityistarpeita tarvitsevat työntekijät. Esimerkiksi konkareilla on enemmän tietoa ammattisanastosta sekä työelämän säännöistä työuransa noviisivaiheessa oleviin verrattuna. Digitaalisuuden hyödyntäminen perehdytyksen aikana lisää joustavuutta, ja esimerkiksi juuri erilaiset testit ja harjoitukset verkossa voivat hyödyttää perehdytystä. Suunnitelmallinen työntekijöiden perehdytys säästää aikaa, ja tätä edesauttavat esimerkiksi kirjallisesti tehty perehdytyssuunnitelma, perehdytyksen seuranta ja valmiiden perehdytyspohjien hyödyntäminen uudestaan. (Perehdytys lähtee suunnittelusta n.d.)

Asiakas- ja potilasturvallisuudella tarkoitetaan sitä, että terveydenhuollon palvelut tuotetaan sekä toteutetaan niillä tavoin, että ei vaaranneta potilaan tai asiakkaan turvallisuutta fyysisellä, psyykkisellä, taloudellisella tai sosiaalisella osa-alueella. Potilasturvallisuus on otettava huomioon kaikkien toimintojen sekä päätöksenteon osalta. Laadukas potilaan hoito, hoiva ja tarjottavat palvelut perustuvat siihen, että on osaava henkilökunta, jolla on tiedossa yhteiset käytännöt. (Asiakas- ja potilasturvallisuuden perehdytysmalli 2024.)

5.2 Perehdytysprosessi terveydenhuoltoalalla

Perehdytysprosessi voitaisiin kokonaisuudessaan jakaa viiteen eri osa-alueeseen: valmistelu, perehdytys, harjoittelu, arviointi ja palaute sekä jatkuva oppiminen, joiden pohjalta perehdytys etenee kuviossa 2 esitetyllä tavalla. Valmisteluvaihe alkaa jo uuden työntekijän rekrytoinnista, ja toteutetaan kokonaisuudessaan ennen ensimmäistä perehdytyspäivää. Perehdytyksestä on pääsääntöisesti vastuussa työntekijälle nimetty esihenkilö, mutta perehdytykseen lisäksi voidaan nimetä vastuuohjaaja tai -perehdyttäjä. Ennen perehdytyksen aloitusta tärkeää on tarkistaa perehdytysmateriaalien ajantasaisuus, ja tietosuojan osalta esimerkiksi mahdolliset laki- sekä järjestelmämuutokset.



Kuvio 2. Perehdytysprosessi

Perehdytys keskittyy kappaleissa 3.4 sekä 3.5 esiteltyihin tietojärjestelmiin sekä digitaalisiin palveluihin, ja kappaleessa 4.3 esiteltyyn tietojen käsittelyyn terveydenhuoltoalalla. Perehdytyksen edetessä keskitytään organisaation käytössä oleviin potilastietojärjestelmiin sekä tietojen kirjaamiseen, lisäksi tietoturvan osalta olennaisiin asioihin sähköisissä järjestelmissä. Tärkeää on myös selventää menettelytavat mahdollisten tietosuojapoikkeamien osalta. Kappaleessa 5.3 esitetty koulutusmateriaali on tarkoitettu käytäväksi läpi perehdytysvaiheessa.

Harjoitteluvaiheessa perehdytyksessä läpikäytyjä asioita sovelletaan päivittäiseen työhön ja sen aikana perehdyttäjä tai muu nimetty ohjaaja on työntekijän tukena. Potilaskirjausten tekeminen alkuvaiheessa ohjatusti ja tapausesimerkkien ja erilaisten skenaarioiden läpikäyminen tuovat työntekijälle konkreettisen käsityksen siitä, miten tietojen käsittely tapahtuu oikein ja vahvistaen potilasturvallisuutta.

Arviointi ja palaute- vaiheessa työntekijä tekee itsearvioinnin perehdytyksen ja harjoittelun osalta, sekä antaa palautteen perehdyttäjälle. Perehdyttäjä vastaavasti käy läpi prosessin onnistumisen, työntekijän osaamistason ja yhdessä voidaan keskustella onnistumisista sekä mahdollisista kehityskohteista, ja perehdytyksen ja harjoittelun kehittämisestä. Työntekijää tuetaan jatkuvan oppimisen toteutumiseksi, ja työntekijällä itsellään on myös vastuu kehittää osaamistaan ja tutustua alan ajankohtaisiin tapahtumiin sekä pysyä ajan tasalla mahdollisten muutosten osalta.

5.3 Perehdytykseen sisältyvän koulutusmateriaalin rakenne

Perehdytysmateriaalin rakenne koostuu työssä esitellyistä kokonaisuuksista, joiden pohjalta rakenne voidaan jakaa kuuteen eri osa-alueeseen. Perehdytys alkaa tervetulosanoilla ja lyhyellä johdatuksella tietosuojan perusteisiin, sekä sen merkitykseen terveydenhuoltoalalla. Johdantoa seuraa katsaus tietosuojaan ja sen tehtävään potilastietojen suojaamiseksi. Oma vastuu ja hyvät käytännöt osa-alueena käy läpi lisäksi tietoturvaa ja tietojen suojaamista.

Perehdytyksessä tuodaan esille myös lainsäädännön näkökulmaa, ja millä eri tavoin se velvoittaa eri toimijoita terveydenhuoltoalalla liittyen tietosuojaan. Luotettavaa ja turvallista asiointia tukien perehdytyksessä tuodaan esille myös asiakkaan tunnistamiseen ja tietojärjestelmien toimintaan liittyviä asioita. Lopputesti varmistaa, että henkilö on käynyt läpi perehdytyksen osa-alueet ja tutustunut niihin, ja työntekijä sekä perehdyttäjä pystyvät tarkistamaan koulutuksen jälkeistä osaamisen tasoa. Kokonaisuudessaan koulutusmateriaalin rakenne on esitelty kuviossa 3. Liitteessä 1 on kuvattu tarkemmin aihepiirit ja kokonaisuudet, jotka sisällytetään eri osa-alueiden alle koulutusmateriaalin rakenteessa.

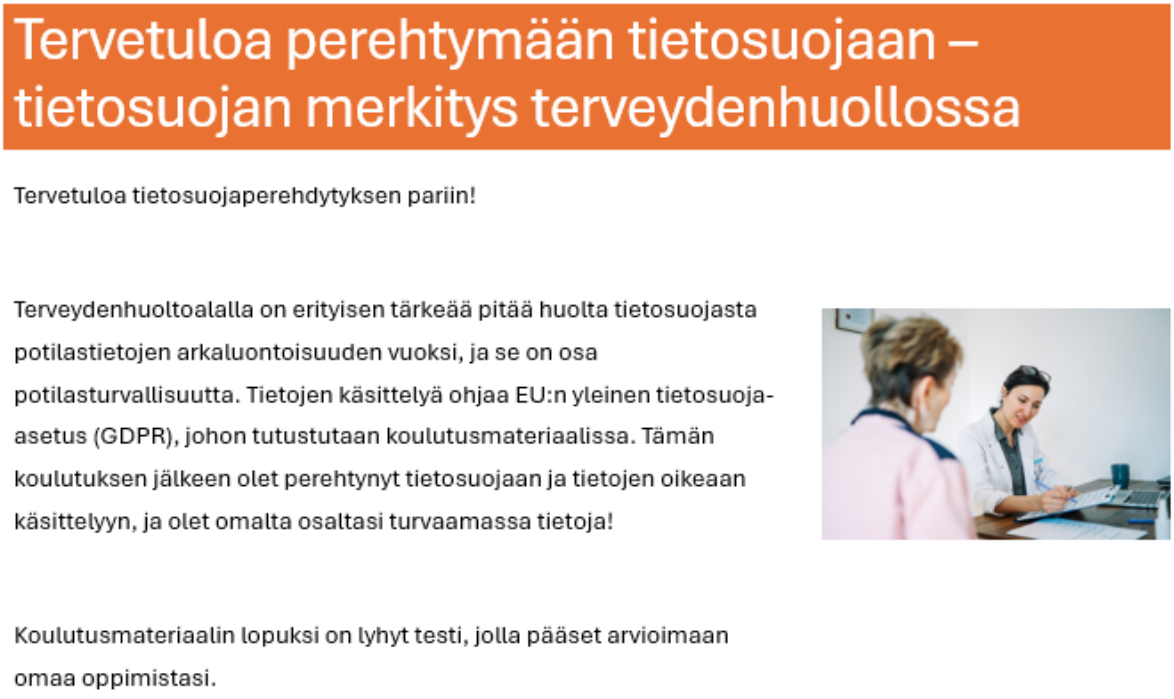
Tervetuloa perehtymään tietosuojaan – tietosuojan merkitys terveydenhuollossa	Tietosuoja – potilastietojen turvana	Oma vastuu ja hyvät käytännöt – jokaisella on tehtävänsä tietojen suojaamisessa	Lainsäädäntö ja velvoitteet – mitä lakeja sovelletaan tietojen käsittelyyn?	Tietojärjestelmät ja asiakkaan tunnistaminen – luotettava ja turvallinen asiointi	Lopputesti – varmista oma osaaminen!

Kuvio 3. Perehdytysmateriaalin rakenne

Kokonaisuudessaan tämän koulutusmateriaalin läpikäyntiin varataan noin tunnin verran aikaa, jolloin työntekijä ehtii pohtia aiheita, ja kirjoittaa mahdollisia muistiinpanoja ja valmistautua lopuksi olevaan testiin. Testin läpipääsyvaatimuksena on saada kaikkiin kysymyksiin oikea vastaus, jotta varmistutaan, että materiaalin läpikäyntiin on käytetty aikaa ja aiheita on pohdittu omaan työnkuvaan liittyen. Lopputestin laajuus on noin kymmenen kysymystä, joka kattaa kahden kysymyksen verran jokaisesta osa-alueesta.

5.4 Koulutusmateriaalin sisältö

Koulutusmateriaali alkaa johdanto-osiolla, jossa kuvataan koulutuksen tarkoitus sekä tavoitteet. Johdanto-osion lisäksi alussa voidaan kuvata tietosuojan perusteita ennen varsinaiseen koulutukseen siirtymistä, jotta työntekijä ymmärtää jo aluksi, kuinka oikealla henkilötietojen käsittelyllä turvataan tietoja niiden luvattomalta käytöltä ja väärältä käsittelyltä. Potilastietojen ollessa erityisen arkaluontoisia on tärkeää varmistaa, että tietoja säilytetään luottamuksellisesti ja käsitellään lain mukaan oikein. Terveydenhuollossa tietojen käsittelyä ohjaa EU:n yleinen tietosuoja-asetus (GDPR). Perehdytys käsittelee tietosuojan merkitystä potilasturvallisuuden tukemiseksi. Johdanto-osion näkymä on esitetty kuviossa 4.



Kuvio 4. Koulutusmateriaalin johdanto

Koulutusmateriaalin seuraavassa osiossa käsitellään tietosuojan perusteet ja käsitteitä, joita on esitetty kappaleessa 3.1. Osion sisältö on esitelty kuviossa 5. Käsitteiden ja perusteiden läpikäyminen alkuun on tärkeää, jotta työntekijällä on käsitys siitä, mitä henkilötietojen käsittelyyn liittyy ja ymmärtää asiakkaan oikeudet, sekä rekisterinpitäjän ja tietojen käsittelijän velvollisuudet. Tarkemmin tietosuojaa ja sitä ohjaavia lakeja käydään läpi koulutuksen lainsäädäntöosiossa. Lisäksi tietosuojaosiossa kerrotaan, miten toimia oikein kohdatessa tietosuojapoikkeaman ja mistä saada organisaation sisällä apua tietosuoja-asioissa, esimerkiksi yrityksen IT-tuki ja tietosuojavastaava, jonka työnkuvaa on esitelty kappaleen 3.1 lopuksi. Lisäksi osiossa käydään läpi potilastietojen kirjaamista ja käsittelyä koskevia säännöksiä, jotka on esitelty kappaleessa 4.3. Potilastietojen ollessa erityisen arkaluontoisia, niitä koskee useat eri velvollisuudet, kuten salassapito- ja vaitiolovelvollisuus.

Kuvio 5. Koulutusmateriaalin tietosuojaosio

Terveydenhuollossa ja yleisesti organisaatiossa jokaisella työntekijällä on omalta osaltaan vastuu tietojen käsittelystä, ja työntekijän vastuut käydään läpi koulutuksen seuraavassa osiossa, joka on esitelty kuvassa 6. Työntekijälle kuvataan organisaation yleisiä ohjeistuksia, sekä päivittäiseen työhön ja arkielämään liittyviä tietosuojaan ja tietoturvaan vaikuttavia toimenpiteitä.

Hyvät käytännöt perustuvat työn tietoturvaan ja kyberturvallisuuteen keskittyviin kappaleisiin 3.2 ja 3.3. Tällaisia käytäntöjä terveydenhuoltoalalla ovat esimerkiksi omien käyttäjätunnusten, salasanojen sekä ammattikortin henkilökohtaisuus, ja nämä tiedot tulee pitää salassa. Lisäksi osiossa esitellään esimerkiksi kappaleessa 3.2 esitellyn päivittäisten toimenpiteiden osalta esimerkiksi työpisteen ja oman työaseman turvallisuutta, myös fyysisesti: työasema tulee lukita poistuessa sen ääreltä ja pitää salassa pidettävät paperit niin, ettei ulkopuolisilla ole pääsyä näihin.

Kuvio 6. Oma vastuu ja hyvät käytännöt

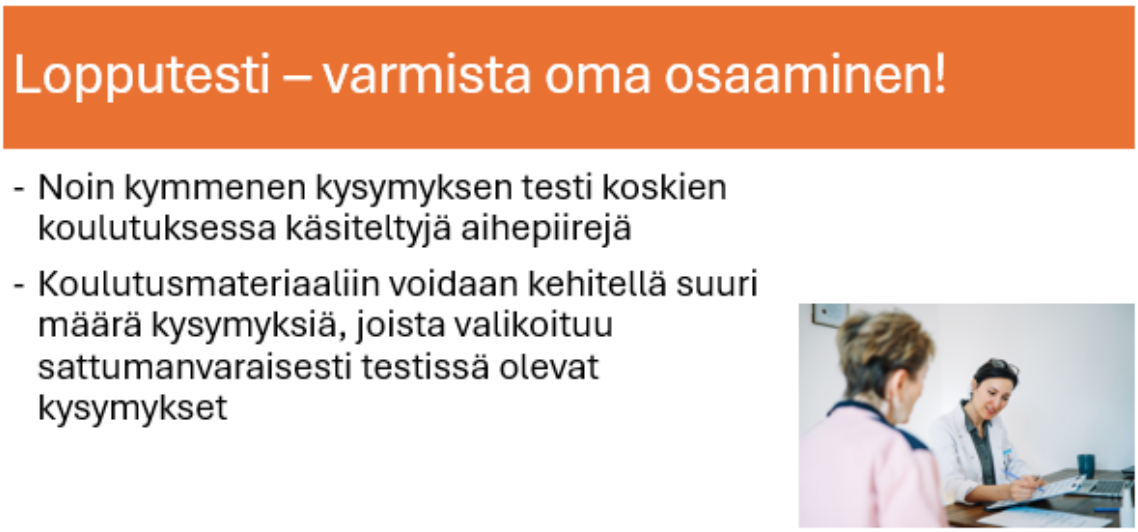
Kuviossa 7 esitetyllä tavalla perehdytyksessä tuodaan esiin lain velvoitteet terveydenhuollossa sekä tietosuojalain ja EU:n yleisen tietosuoja-asetuksen (GDPR) osalta. Yleisen tietosuoja-asetuksen merkitys on suuri henkilötietojen käsittelyssä, ja tähän voidaan soveltaa suoraan lakiasetuksia, jotka on käsitelty kappaleissa 4.1 ja 4.2. Lainsäädännön osalta perehdytettävän on tärkeää ymmärtää, miten potilastietoja käsitellään ja säilytetään, ja voidaan luovuttaa. Henkilötietoja käsitellessä tietosuoja-asetuksen mukaan rekisterinpitäjällä on vastuu valvoa, että käsittely tapahtuu tietosuojaperiaatteiden mukaan. Tämän osalta tietosuojaperehdytyksessä työntekijöille organisaatio rekisterinpitäjänä varmistaa, että laissa määrätyt kohdat toteutuvat päivittäisessä työssä terveydenhuollossa.

Kuvio 7. Lainsäädäntö

Kuviossa 8 on esitelty koulutusmateriaalin viimeinen osio ennen lopputestiä, joka keskittyy tietojärjestelmiin sekä asiakkaan tunnistamiseen, joka varmistaa luotettavan asioinnin. Tunnistaminen on tärkeää etenkin sähköisessä asioinnissa, mutta myös vastaanotolla. Aiheeseen liittyen sisältö voidaan koostaa työn kappaleiden 3.4 ja 3.5 pohjalta. Kappaleessa 3.5 on keskitytty sähköisessä asioinnissa tapahtuvaan tunnistautumiseen, joka tapahtuu vahvoilla tunnistusmenetelmillä, esimerkiksi pankkitunnistautumisella tai mobiilivarmenteella.

Kuvio 8. Tietojärjestelmät ja asiakkaan tunnistaminen

Perehdytyksen lopussa olevalla testillä voidaan varmistaa, että työntekijä on käynyt perehdytysmateriaalin läpi, ja on tutustunut aihepiireihin ja osaa soveltaa asioita omaan työnkuvaan terveydenhuoltoalalla. Lopputestin tavoitteena on, että työntekijä jäisi pohtimaan perehdytyksen lopuksi tietosuojan merkitystä omassa työssään, ja yhdistäisi tietoturva- ja tietosuojaperiaatteita päivittäiseen työskentelyyn. Lopputestin rakenne on esitelty kuviossa 9, ja yksi mahdollinen versio kysymysten kokoonpanosta on esitelty liitteessä 1.



Kuvio 9. Lopputesti

5.5 Mittarit ja jatkuvuus

Perehdytyksen onnistumista sekä terveydenhuollon henkilökunnan tietosuojaosaamisen kehittymistä voidaan seurata erilaisten mittareiden avulla. Tietosuojaperehdytyksen lopussa olevan testin avulla saadaan selkeä kuva heti materiaalin läpikäymisen jälkeen henkilön sen hetken osaamistasosta, ja näiden tulosten perusteella voidaan tarkastella koko henkilöstön tilannetta. Perehdytyksen lopuksi toteutettavan arvioinnin ja palautteen pohjalta saadaan myös dataa perehdytysmateriaalin mahdollisista kehityskohteista sekä tarkennusta vaativista aiheista.

Materiaalin ja perehdytysprosessin läpikäytyään työntekijän on tarkoitus lisäksi kehittää omaa osaamistaan työn ohessa. Työnantajaorganisaation puolesta voidaan järjestää lisäkoulutusta, tarjota tietoturvakatsauksia ja pitää ohjeistukset ajan tasalla, sekä tiedottaa tapahtuvista muutoksista henkilökunnalle. Matalan kynnyksen tiedonjako voi olla esimerkiksi jakaa Kyberturvallisuuskeskuksen tarjoama katsaus, jossa käsitellään viikoittain esille nousseita kyberturvallisuuteen liittyviä tapauksia ja erityisesti Suomessa näkyviä ajankohtaisia teemoja. Katsauksen tarkoituksena on lisätä ihmisten tietoisuutta kyberturvallisuudesta. (Viikkokatsaus n.d.).

6 Tulokset

Työn aluksi tutkimuskysymykseksi määriteltiin ensimmäisenä: ”Mitä vaatimuksia lainsäädäntö asettaa tietosuojalle terveydenhuoltoalalla?”. Lainsäädännön osalta tietojen käsittelyä terveydenhuoltoalalla ohjaa EU:n yleinen tietosuoja-asetus (GDPR), ja potilastiedot luokitellaan arkaluontoisiksi tiedoiksi. Potilastietojen käsittely on hyvin rajattua, ja kappaleessa 4.1 esiteltyjen käsittelyperusteiden mukaan läpinäkyvää, selkeää ja asianmukaista. Lainsäädännössä määritellään potilaan oikeuksista, jotta rekisteröidyllä on oikeus saada tietoon, millä tavoin hänen tietojaan käsitellään ja säilytetään, ja kappaleen 4.3 mukaan potilaalla on myös oikeus pyytää tietojärjestelmissä mahdollisesti esiintyvien virheellisten tietojen korjaamista. Tietosuoja-asetuksen mukaan organisaatiolla eli rekisterinpitäjällä on velvollisuus osoittaa, että henkilötietojen käsittely noudattaa vaatimuksia.

Toisena tutkimuskysymyksenä oli: ”Millaisella henkilökunnan perehdyttämisellä voidaan tukea vaatimusten toteutumista?”. Uuden terveydenhuollon työntekijän perehdytykseen liitettävällä tietosuojaosiolla varmistetaan, että käsitteet ja potilastietojen kirjaamista ohjaavat lait ja muut säädökset tulevat tutuksi. Laissa määriteltyjen vaatimusten toteutuminen päivittäisessä potilastyössä edellyttää, että työntekijöille tarjottava materiaali sekä koulutus ovat selkeitä ja terveydenhuollon ammattilaisella on vähintään perustiedot käytettävistä järjestelmistä, potilastiedoista, erityistapauksista, organisaation tietosuojaohjeistuksista, sekä tietoturvaan liittyvistä toimenpiteistä.

Perehdytyksen jälkeen tehtävällä arvioinnilla ja työntekijöiltä saadulla palautteella voidaan kehittää perehdytystä, ja työnantaja saa tällöin arvokasta tietoa siitä, millä tasolla tietosuojaosaaminen on, ja miten perehdytystä voidaan kehittää. Tiedottamisella ja lisäkoulutuksilla osaamista voidaan parantaa, ja tarkentaa ohjeistuksia ajan tasalle. Työntekijän on myös tärkeää kehittää osaamistaan työn ohessa.

Tietoturva kulkee käsi kädessä tietosuojan kanssa, ja arjen työhön liittyviä toimenpiteitä on kuvattu kappaleessa 3.2. Organisaatiotasoisen perehdytyksen pohjalta jokainen työntekijä ymmärtää oman vastuunsa, ja organisaatio pystyy toimimaan yhdessä potilasturvallisuuden varmistamiseksi. Riittävä ja kohdistettu perehdytys vahvistaa työntekijöiden motivaatiota ja osaamista, jolloin pystytään vähentämään virheiden määrää ja laskemaan tietosuojaloukkausten ja -poikkeamien, sekä myös isommassa mittakaavassa tietomurtojen riskiä.

7 Pohdinta

Työn tavoitteena oli tarkastella tietosuojaan ja terveydenhuoltoon liittyviä lakeja, ja millä tavoin ne vaikuttavat terveydenhuollon henkilökunnan perehdytykseen. EU:n yleinen tietosuoja-asetus, tietosuojalaki sekä terveydenhuollon lait löytyivät verkosta selkeästi tiivistettyinä, jotta näistä oli mahdollista poimia tärkeimmät kohdat työn teoriaosioon. Työn tuloksena toteutettiin koulutusmateriaalin runko sekä liitteenä koulutuksen sisältölistaus, jolla tietosuojaperehdytystä voisi lähteä toteuttamaan terveydenhuollon organisaatiossa.

Työn tavoitteen toteutumisen jälkeen seuraavana vaiheena olisi käytännön testaus. Mahdollisten testausten myötä ennen perehdytysmateriaalin tuotantoon vientiä kokonaisuutta voidaan parantaa ja tuoda vielä lähemmäksi käytäntöä. Koulutusmateriaaliin olisi mahdollista yhdistää lopputestin lisäksi aktivoivia osuuksia koulutusosioiden väleissä olevilla välitehtävillä. Välitehtävät voisivat olla esimerkiksi aikaisemmassa osiossa läpikäytyihin aiheisiin liittyviä väärinoikein väittämiä tai monivalintatehtäviä, joista tulisi valita tilannetta parhaiten kuvaava vaihtoehto. Tällaisia tehtäviä olisi myös perehdytystä jatkokehittäessä mahdollista luoda eri tilanteiden pohjalta perustuen henkilön työnkuvaan, jolloin tehtävät voisivat erilaisia esimerkiksi sairaalassa toimivan yleislääkärin tai lastensuojeluyksikössä toimivan ohjaajan kohdalla. Perehdytysmateriaalia voitaisiin myös jatkokehityksellä kytkeä enemmän tietoturva-aiheisiin, tai materiaali voidaan tarvittaessa liittää osaksi tietoturvaperehdytystä.

Työn teoriaosioon kytkettynä perehdytyksen koulutusmateriaalien voidaan todeta kattavan terveydenhuollossa tarvittavan perusosaamisen tietosuojasta. Lopputuloksien osalta päästiin työn tavoitteisiin, ja työssä käytettiin monipuolisesti terveydenhuollon alan viranomaisten, ja muiden toimijoiden, sekä lakitekstien osalta kattavasti eri verkkolähteitä, ja myös painettuja kirjalähteitä.

Lähteet

12.5 Tietosuojalainsäädäntö. N.d. Lainkirjoittajan opas, Finlex- julkaisut. Viitattu 25.4.2025. https://lainkirjoittaja.finlex.fi/12-yleislait-ja-eraat-yleiset-saantelyt/12-5/.

29.6.2021/612 Laki sosiaali- ja terveydenhuollon järjestämisestä. 2023. Finlex. Viitattu 15.10.2024. https://www.finlex.fi/fi/laki/ajantasa/2021/20210612#L8P58.

9 Työelämän tutkiva kehittämistoiminta. 2022. Jamk. Viitattu 29.3.2025. https://help.jamk.fi/opinnaytetyon-ohjaus/fi/tyoelaman-tutkiva-kehittamistoiminta/.

Andreasson, A., Riikonen, J. & Ylipartanen, A. 2019. Osaava tietosuojavastaava ja EU:n yleinen tietosuoja-asetus. Tietosanoma. p. Tallinna: Printon.

Asiakas- ja potilasturvallisuuden perehdytysmalli. 2024. Asiakas- ja potilasturvallisuuskeskus. Viitattu 14.3.2025. https://asiakasjapotilasturvallisuuskeskus.fi/ammattilaisille-ja-opiskelijoille/materiaalipankki/kuvauksia-ja-toimintamalleja/asiakas-ja-potilasturvallisuuden-perehdytysmalli/.

Asiakkaan ja potilaan oikeudet. N.d. Valvira. Viitattu 5.5.2025. https://valvira.fi/sosiaali-ja-terveydenhuolto/asiakkaan-ja-potilaan-oikeudet.

Case Vastaamo. N.d. Tietosuojakeskus. Viitattu 25.4.2025. https://tietosuojakeskus.fi/case-vastaamo/.

CIA-arvojen mukaisen luokittelun käyttöönotto Digiturvamallissa. N.d. Digiturvamalli | Akatemia. Viitattu 19.10.2024. https://www.digiturvamalli.fi/ohjeartikkelit/cia-arvojen-mukaisen-luokittelun-kayttoonotto-digiturvamallissa.

Digitaaliset palvelut. 2024. Terveyden ja hyvinvoinnin laitos. Viitattu 15.3.2025. https://thl.fi/aiheet/sote-palvelujen-johtaminen/kehittyva-palvelujarjestelma/digitaaliset-palvelut.

Henkilötietojen käsittely. N.d. Tietosuojavaltuutetun toimisto. Viitattu 17.10.2024. https://tietosuoja.fi/henkilotietojen-kasittely.

Klauenbösch, J. 2024. Kyberturvakatsaus sote-ala. Kyberasema. Viitattu 21.4.2025. https://digiasema.fi/kyberturvakatsaus-sote-ala/.

Kortesoja, M. 2022. Tapaus Vastaamo: Symptomaattinen luenta potilastietosuojan murtumisen yhteiskunnallisista syistä ja seurauksista. Tutkimus & kritiikki. https://doi.org/10.55294/tk.113346.

Kurvinen, E. & Voutilainen, T. 2024. Asiakas- ja potilastietojen käsittelyn sääntely. Alma Insights. E-kirja Jyväskylän ammattikorkeakoulun verkkokirjastossa. Viitattu 20.10.2024. https://janet.finna.fi/.

Lainmukaisuus, asianmukaisuus ja läpinäkyvyys. N.d. Tietosuojavaltuutetun toimisto. Viitattu 5.5.2025. https://tietosuoja.fi/lainmukaisuus-asianmukaisuus-lapinakyvyys.

Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä. 2021. Finlex. Viitattu 15.3.2025. https://www.finlex.fi/fi/lainsaadanto/saadoskokoelma/2021/784.

Mitä eroa on tietosuojalla ja tietoturvalla? N.d. Tietosuojavaltuutetun toimisto. Viitattu 11.3.2025. https://tietosuoja.fi/tietosuoja.

Mitä on kyberturvallisuus? N.d. F-Secure. Viitattu 27.10.2024. https://www.f-secure.com/fi/articles/what-is-cyber-security.

Mitä tietoturva on? N.d. Microsoft. Viitattu 19.10.2024. https://www.microsoft.com/fi-fi/security/business/security-101/what-is-data-security.

Määräys sosiaali- ja terveydenhuollon tietojärjestelmien ja hyvinvointisovellusten luokittelusta ja sertifioinnista. 2024. Terveyden ja hyvinvoinnin laitos. Viitattu 17.10.2024. https://thl.fi/documents/155392151/190361269/THL-Maarays4-2024_Sosiaali-ja_terveydenhuollon_tietojarjestelmien_ja_hyvinvointisovellusten_luokittelusta_ja_sertifioinnista.pdf/c2c4ce1b-540e-0f0d-490e-468ca5975165/THL-Maarays4-2024_Sosiaali-ja_terveydenhuollon_tietojarjestelmien_ja_hyvinvointisovellusten_luokittelusta_ja_sertifioinnista.pdf?t=1714978021090.

Niemistö, E. 2024. Terveysala on tietojenkalastelijoille mieluisa kohde, ja siksi kyberuhkia opetellaan torjumaan yhä tanakammin. Artikkeli Ylen verkkosivuilla. Viitattu 8.4.2025. https://yle.fi/a/74-20119732.

Perehdytys lähtee suunnittelusta. N.d. Työterveyslaitos. Viitattu 6.4.2025. https://www.ttl.fi/oppimateriaalit/onnistunut-perehdytys-palvelualoilla/perehdytys-lahtee-suunnittelusta.

Potilas- ja asiakastietojen ja henkilötietojen käsittely. N.d. Valvira. Viitattu 15.10.2024. https://valvira.fi/sosiaali-ja-terveydenhuolto/potilas-ja-asiakastietojen-ja-henkilotietojen-kasittely.

Potilasasiakirjojen käsittely. N.d. Minilex. Viitattu 5.5.2025. https://www.minilex.fi/a/potilasasiakirjojen-k%C3%A4sittely.

Potilaslaki eli laki potilaan asemasta ja oikeuksista. N.d. Minilex. Viitattu 5.5.2025. https://www.minilex.fi/a/potilaslaki-eli-laki-potilaan-asemasta-ja-oikeuksista.

Psykoterapiakeskus Vastaamolle seuraamusmaksu tietosuojarikkomuksista. 2021. Tietosuojavaltuutetun toimisto. Viitattu 14.3.2025. https://tietosuoja.fi/-/psykoterapiakeskus-vastaamolle-seuraamusmaksu-tietosuojarikkomuksista.

Sosiaali- ja terveydenhuollon tietojärjestelmät. N.d. Valvira. Viitattu 29.3.2025. https://valvira.fi/sosiaali-ja-terveydenhuollon-tietojarjestelmat.

Terveyspalvelut. N.d. Sosiaali- ja terveysministeriö. Viitattu 15.10.2024. https://stm.fi/terveyspalvelut.

Tietosuoja. N.d. Tietosuojavaltuutetun toimisto. Viitattu 15.10.2024. https://tietosuoja.fi/tietosuoja.

Tietosuojalaki. 2018. Finlex. Viitattu 6.4.2025. https://www.finlex.fi/fi/lainsaadanto/2018/1050.

Tietosuojaselosteen laatiminen – lataa malli Sopimuskoneesta. 2024. Procountor. Viitattu 11.3.2024. https://procountor.fi/blogi/tietosuojaseloste-malli/.

Tietosuojavastaavat. N.d. Tietosuojavaltuutetun toimisto. Viitattu 5.5.2025. https://tietosuoja.fi/tietosuojavastaavat.

Tietoturva sosiaali- ja terveydenhuollossa. 2024. Duodecim Oppiportti. Verkkokurssin oppimateriaali. Viitattu 4.5.2025. https://www.oppiportti.fi/dvk00150.

Tietoturvan hallintajärjestelmän ISO/IEC 27001- sertifiointi. N.d. Kiwa. Viitattu 6.4.2025. https://www.kiwa.com/fi/fi/palvelumme2/sertifiointi-arviointi-ja-todentaminen/tietoturva-ja-tietoturvallisuuden-hallintajarjestelman-sertifiointi-iso-iec-27001/.

Usein tietosuojaloukkaus havaitaan liian myöhään, joskus ei lainkaan. N.d. Tietosuojaloukkaus. Viitattu 5.5.2025. https://www.tietosuojaloukkaus.fi/.

Uusi laki sääntelemään sosiaali- ja terveydenhuollon asiakastietojen käsittelyä. 2023. Valtioneuvosto. Viitattu 16.10.2024. https://valtioneuvosto.fi/-/1271139/uusi-laki-saantelemaan-sosiaali-ja-terveydenhuollon-asiakastietojen-kasittelya-1.

Viikkokatsaus. N.d. Traficom, liikenne- ja viestintävirasto, Kyberturvallisuuskeskus. Viitattu 4.5.2025. https://www.kyberturvallisuuskeskus.fi/fi/viikkokatsaus?active=0&limit=20&offset=0.

Yleinen tietosuoja-asetus. N.d. Your Europe – Euroopan unionin virallinen verkkosivusto. Viitattu 16.10.2024. https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_fi.htm.

Liitteet

Liite 1. Koulutusmateriaalin sisältö ja lopputesti

Tervetuloa perehtymään tietosuojaan – tietosuojan merkitys terveydenhuollossa

- Tervetuloa koulutusmateriaalin pariin
- Tietosuojan peruskäsitteet
- Mitä tietosuojalla tarkoitetaan terveydenhuollossa
- Potilasturvallisuus
- Tietosuoja päivittäisessä työssä
- Tietosuojan ja tietoturvan eroavaisuudet

Tietosuoja – potilastietojen turvana

- Rekisteröity ja rekisteröidyn oikeudet
- Rekisterinpitäjä ja rekisterinpitäjän velvollisuudet, esimerkiksi osoitusvelvollisuus
- Henkilötieto
- Henkilötietojen käsittely
- Arkaluontoiset tiedot, potilastiedot
- Tietosuojan periaatteet, esimerkiksi läpinäkyvyys, lainmukaisuus
- Organisaation tietosuojaseloste

Oma vastuu ja hyvät käytännöt – jokaisella on tehtävänsä tietojen suojaamisessa

- Jokaisen työntekijän vastuu tietosuojan toteutumisessa
- Käyttäjätunnukset, salasanat, ammattikortit
- Työpisteen ja työaseman tietoturva
- Salassapitovelvollisuus ja vaitiolovelvollisuus
- Potilasasiakirjojen säilytys sekä hävitys
- Viestintäkäytännöt
- Kyberturvallisuuden periaatteet
- Tietosuojapoikkeamat

Lainsäädäntö ja velvoitteet – mitä lakeja sovelletaan tietojen käsittelyyn?

- Euroopan Unionin yleinen tietosuoja-asetus (GDPR)

- Tietosuojalaki
- Potilaslaki
- Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä
- Tietosuojavaltuutettu

Tietojärjestelmät ja asiakkaan tunnistaminen – luotettava ja turvallinen asiointi

- Potilastietojärjestelmä
- Asiakastietojärjestelmä
- Järjestelmien luokittelu
- Valvontaviranomainen (Valvira)
- Riskien arviointi ja hallinta järjestelmiä käyttöönotettaessa
- Asiakkaan sähköinen tunnistaminen esimerkiksi pankkitunnistautumisella
- Asiakkaan tunnistaminen vastaanotolla henkilöllisyystodistuksella
- Turvasähköposti
- Potilastietojen katselu, lokitiedot

Lopputesti – varmista oma osaaminen!

1. Miksi tietosuoja on tärkeää terveydenhuollossa?
2. Miten tietosuojalla tuetaan potilasturvallisuutta?
3. Mitä tarkoittaa rekisteröity/rekisterinpitäjä?
4. Mitkä luokitellaan arkaluonteisiksi tiedoiksi?
5. Mitä työntekijän tulisi tehdä, jos hän havaitsee tietosuojapoikkeaman?
6. Miksi tietokoneen näyttö tulisi lukita, kun poistuu työpisteen ääreltä?
7. Mitä tarkoitetaan rekisterinpitäjän osoitusvelvollisuudella?
8. Mikä viranomainen valvoo tietosuojaa?
9. Mitä tarkoitetaan vahvalla tunnistautumisella sähköisessä asioinnissa?
10. Mitä oikeuksia rekisteröidyllä on?