

Tietoturva ja tietosuoja hyvinvointialueilla syksyllä 2025

Tuulikki Vehko¹, Maiju Kyytsönen¹, Tuula Wester², Antti-Olli Taipale², Juha Mykkänen³

¹ Hyvinvointivaltion tutkimus, Terveyden ja hyvinvoinnin laitos, Helsinki; ² Sote-tietojärjestelmäpalvelujen ohjaus, Terveyden ja hyvinvoinnin laitos, Helsinki; ³ Tietotuotannon ohjaus, Terveyden ja hyvinvoinnin laitos, Helsinki

Tuulikki Vehko FT, tutkimuspäällikkö, Palvelujärjestelmän tutkimus, Terveyden ja hyvinvoinnin laitos, PL 30, 00271 Helsinki. Sähköposti: tuulikki.vehko@thl.fi

Tiivistelmä

Asiantunteva tietoturvan ja tietosuojan rakentaminen sekä niiden aktiivinen ylläpito muodostavat edellytyksen digipalveluiden ja tietojärjestelmien turvalliselle käytölle sosiaali- ja terveydenhuollossa. Tutkimuksen tarkoituksena oli selvittää hyvinvointialueiden tietohallinnon johdon näkemyksiä tietoturva- ja tietosuojakäytännöistä hyvinvointialueilla.

Syyskuussa 2025 toteutettu Hyvinvointialueiden digitaalinen palvelujärjestelmä -kysely kohdennettiin kahdenkymmenenhyden hyvinvointialueen tietohallinnossa toimiville johtajille. Alueita oli yhteensä 23, koska kysely lähetettiin myös Helsingin kaupungille ja HUS-yhtymälle. Vastaajien yhteystiedot oli haettu organisaatioiden verkkosivuilta. Vastaajille lähetettiin sähköposti, jossa oli linkki kyselyyn. Ei-vastanneita muistutettiin kyselyyn vastaamisesta sähköpostitse, soittamalla tai tekstiviestillä. Kyselyyn vastaaminen oli vapaaehtoista.

Saatujen vastausten mukaan (N=21) alueet päivittävät tietoturvasuunnitelmia aktiivisesti. Alihankintaketjut oli huomioitu tietoturvasuunnitelmissa kohtalaisesti noin kolmasosassa alueista (n=8/21) ja noin puolella alueista ne oli huomioitu kattavasti tai erittäin kattavasti. Suurimmalla osalla alueista (n=15/21) laadittiin säännöllisesti tietotilinpäätös. Alle puolet alueista (n=9/21) on viimeisen kolmen vuoden aikana toteuttanut ei-lakisäateistä viestintää alueen asukkaille digitaalisten palveluiden tai asiakastietojen käsittelyn tietoturvasta ja tietosuojasta.

Tietoturva ja tietosuoja muodostavat perustan rakentaa ja toteuttaa luotettavia ja turvallisia palveluja väestölle. Päivittämällä tietoturvasuunnitelmaa säännöllisesti mahdollistetaan uusien riskien huomiointi riittävän ajoissa. Tietotilinpäätökset ovat osoittautuneet hyödyllisiksi organisaatioiden tilannekuvan muodostamisessa. Hyvinvointialueiden tietoturvan kehittämisessä painopisteitä tulisi siirtää resurssien vahvistamiseen, alihankintaketjujen yhä kattavampaan huomioimiseen organisaation tietoturvasuunnitelmassa ja tietoturvaan liittyvien asioiden lisäämiseen asiakasviestinnässä luottamuksen rakentamiseksi.

Tässä tutkimuksessa tehty tiedonkeruu ja sen seuranta on jatkossakin tärkeää, sillä ajantasainen tieto mahdollistaa tietoon perustuvat päätökset ja parantaa kokonaisuuden hallintaa.

Published under a CC BY 4.0 license (<https://creativecommons.org/licenses/by/4.0/>).

Avainsanat: tietoturva, organisaatio ja hallinto, terveyspalvelujen tarjonta ja järjestäminen, terveystiedon hallinta, survey-tutkimukset ja kyselylomakkeet

Abstract

Building information security and data protection by experts, along with regular updates, is a prerequisite for the safe use of digital services and information systems in healthcare and social services. The purpose of the study was to examine the views of chief information officers or chief digital officers in wellbeing services counties (WSCs) regarding information security and data protection practices.

The Digital Service System Survey for WSCs was conducted in September 2025 and targeted chiefs working in the information management of 21 WSCs. There was a total of 23 areas because the survey was also sent to the City of Helsinki and HUS Group, the joint authority for Helsinki and Uusimaa. Respondents' contact details were obtained from the organisations' websites. An email containing a link to the survey was sent to the respondents. Non-respondents were reminded by email, phone call, or text message. Participation in the survey was voluntary.

Based on the responses (N=21), the counties actively update their Information Security Plan. Subcontracting chains had been moderately take account in these plans in one third of the counties (n=8/21), and in about half of the counties they had been take account comprehensively or very comprehensively. Most counties (n=15/21) regularly prepare an information accountability report. Fewer than half of the counties (n=9/21) have, during the past three years, carried out non-statutory communication to residents about information security and data protection related to digital health services or the processing of client data.

Information security and data protection form the foundation for building and delivering reliable and secure services for the population. Regular updating of the Information Security Plans enables to take new risks into account in time. The voluntary information accountability report has proved useful in drawing a situational picture of the counties. In the development of information security in WSCs, the focus should be shifted to strengthening resources, taking increasingly comprehensive account of subcontracting chains in organization's information security plans, and increasing communication with the inhabitants about information security related issues to build trust.

The data collection carried out in this study and its follow-up will be important in the future, as up-to-date information enables informed decisions and improves overall management.

Keywords: computer security, organization and administration, delivery of health care, health information management, surveys and questionnaires

Johdanto

Sosiaali- ja terveysministeriön Digitalisaatio kivijalaksi -strategiassa tietoturvan ja tietosuojan periaatteiden noudattaminen on tunnistettu

avaintekijäksi strategisten tavoitteiden saavuttamiseksi [1]. Kansallisia strategioita on Suomessa hyödynnetty sosiaali- ja terveydenhuollon digitalisaation ohjaamisessa pitkään [2,3]. Vuonna 2023 voimaan tulleen sosiaali- ja terveydenhuollon

uudistuksen myötä myös hyvinvointialueet ovat laatineet omia digitalisaatiostrategioita [4]. Digitalisaatio nähdään niissä eräänä ratkaisukeinona sosiaali- ja terveydenhuollon haasteisiin, jotta voidaan tehostaa toimintaa, edistää resurssien riittävyyttä, helpottaa sosiaali- ja terveydenhuollon henkilöstön työtä sekä sujuvoittaa asiakkaille tarjottavia palveluja [1].

Terveydenhuollon digitalisaatioon liittyy kuitenkin myös riskejä, koska arkaluonteiset potilas- ja asiakastiedot liikkuvat yhä enemmän. Tämä aiheuttaa tarpeen hallita riskejä ja huolta siitä, miten riskeihin pystytään varautumaan [5–7]. Organisaatioiden luotettavan toiminnan kannalta suunnitelmat häiriötilanteita ja niistä toipumista varten ovat oleellisia, jotta haittoja, kuten tietojen menetystä tai tietojärjestelmien alasajoa, voidaan välttää. Tietoturva- ja häiriöidenhallintasuunnitelmien säännöllinen arviointi ja päivitys on tarpeen, koska uhat muuttuvat jatkuvasti. [8] Kaiken kaikkiaan digitaalisissa palveluissa käytettyjen ratkaisujen turvallisuuden varmistaminen tukee terveydenhuoltojärjestelmien kestävyttä ja luottamusta järjestelmään väestössä, jota varten palveluita tuotetaan [9–11].

Digitaalista turvallisuutta voidaan kehittää organisaatiossa esimerkiksi hankkeiden, tukimateriaalien ja osaamisen kehittämisen tukivälineiden avulla. Hallinnollisten toimien lisäksi teknisen tietoturvallisuuden ja jatkuvuuden hallinnan parantaminen vaativat organisaatiokohtaisia keinoja, jotka liittyvät käytössä oleviin teknisiin järjestelmiin ja palveluihin [12]. Hyvinvointialueiden toisen toimintavuoden syksyllä 2024 asiakas- ja potilastyötä tekevien sosiaali- ja terveydenhuollon ammattilaisten tietoturva- ja tietosujoasaamisen kehittämiseksi on muun muassa järjestetty koulutusta ja tarjottu viestinnällistä tukea useimmilla hyvinvointialueilla [13]. Toisaalta digitalisaation eteneminen sosiaali- ja

terveydenhuollossa edellyttää, että asiakkaat omaksuvat elinikäisen oppimisen periaatteen tietoturvaosaamisensa kehittämiseksi [14].

Suomessa Traficomien Kyberturvallisuuskeskus tuottaa säännöllisesti Kybersää-arvioita, jota voidaan hyvin hyödyntää myös sosiaali- ja terveydenhuollossa [15]. Tietoturva- ja häiriöidenhallintasuunnitelmat on tunnustettu keskeiseksi kyvykkyydeksi tuottaa turvallisesti digitaalisia palveluita hyvinvointialueilla. On tärkeää, että suunnitelmat on liitetty osaksi koko hyvinvointialueen strategiaa. Hyvinvointialueilla on kehittämistarpeita digitaalisten palvelujen toimintamalleissa ja osaamisen kasvattamisessa sosiaali- ja terveydenhuollon ammattilaisten ja tietohallinnon henkilöstön keskuudessa [16]. Tietohallinnon henkilöstö koostuu asiantuntijoista, jotka työskentelevät tieto- ja viestintäteknologian parissa vastaten laitteiden, ohjelmistojen ja verkkojen hallinnasta ja kehittämisestä tiedon käsittelyn tueksi. Teknisellä tuella ja sen saatavuudella on tärkeä rooli tietoturvalisessa työskentelyssä [17]. Digitaalisten palvelujen vaatimustenmukaisuus ja tietoturvalisisuuden sekä kyberturvallisuuden varmistaminen oli alueiden itsearviossa melko hyvällä tasolla 2024 [16]. Tietojärjestelmien ylläpidossa on siirrytty enenevästi ulkopuolisten palvelujen tuottajien ratkaisuihin, mikä lisää tiedonhallinnan eri toimijoiden rajapintojen ja vastuiden kuvaamisen tärkeyttä.

Suomen monituottajamallisessa sosiaali- ja terveydenhuollon palvelujärjestelmässä [3,18] tietosuojan ja tietoturvalisisuuden toteuttamiseen vaikuttavat useat sosiaali- ja terveydenhuoltoa sekä tiedonhallintaa koskevat lait ja säädökset [1]. Lisäksi turvallinen tietojen käsittely on osa hyvinvointialueen valmiussuunnitelmaa, sillä hyvinvointialueiden on vastattava kaikissa oloissa kriittisten tietojärjestelmiensä toimintavarmuudesta ja turvallisuudesta [19]. Suomessa sosiaali- ja

terveydenhuollon tietoturvallisuutta ohjaavat ja tukevat useat viranomaiset. Toimialat ylittävien tietoturva- ja tietosuojasäädösten lisäksi mm. asiakastietolaki ja sen nojalla Terveyden ja hyvinvoinnin laitoksen antamat määräykset ohjaavat sosiaali- ja terveydenhuollon toimijoiden tietoturvasuunnitelmia ja tietojärjestelmille asetettavia tietosuoja- ja tietoturvallisuusvaatimuksia [20].

Toimintaympäristö on muutoksessa myös Euroopan unionin terveysdata- ja kyberturvallisuussäädösten myötä, esimerkiksi eurooppalainen terveys-tietoalue -asetus (EHDS), EU:n kyberkestävyyssäädökset (CRA) sekä kyberturvallisuusdirektiivi (NIS 2), asettavat toimijoille ja järjestelmille tietoturva-vaatimuksia. Siitä huolimatta terveysdatan yhdistäminen Euroopan unionin tasolla voi olla kyberrikollisille ja haitallisille valtiollisille toimijoille houkutteleva hyökkäyskohde [21]. Euroopan unionin alueella toteutetun tietosuojarikkomusten analyysin perusteella yleisimpiä kyberrikollisuuden toimintamuotoja ovat olleet kiristysohjelmahyökkäykset, tietoihin kohdistuvat uhat kuten data-vaadot sekä palvelunestohyökkäykset [22].

Hyvinvointialueet aloittivat vuonna 2023 toimintansa erilaisista lähtökohdista. Ennen hyvinvointialueuudistusta osa kunnista tuotti palvelut itsenäisesti, kun taas osa sosiaali- ja terveydenhuollon palveluiden järjestämisestä toteutettiin laajempien kuntayhtymien kautta. Vuonna 2023 kaikista 21 hyvinvointialueesta sekä Helsingin kaupungista kahdeksan jatkoi aikaisemman organisaation mukaista toimintaa, kun taas neljätoista hyvinvointialuetta aloitti toiminnan sirpaleisista lähtökohdista [23]. Digi- ja väestötietoviraston arvion mukaan organisaation toimintaprosessit ja menettelyt tietoturvan osalta ovat aloittavissa organisaatioissa väistämättä vasta kehitysvaiheessa [12].

Arviointitutkimus on systemaattinen tutkimusprosessi, jonka tarkoituksena on määrittää

toimenpiteiden, ohjelmien tai hankkeiden arvo ja vaikutukset keräämällä, analysoimalla ja tulkitsemalla empiiristä aineistoa [24]. Tässä tutkimuksessa hyödynnetään summatiivista, tuloksia arvioivaa, arviointitutkimuksen otetta. Tutkimuksen tarkoituksena on selvittää hyvinvointialueiden tietohallinnon johdon näkemyksiä tietoturva- ja tietosuojakäytännöistä hyvinvointialueilla. Koska arviointitutkimuksen keskeisiin tavoitteisiin kuuluu tulosten hyödyntäminen [25], korostamme pohdinnassa tulosten merkitystä hyvinvointialueiden kehittämistyössä. Tuloksia tarkastellaan sen mukaan, aloittiko hyvinvointialue sirpaleisista lähtökohdista vai kuntayhtymäpohjaisesti sosiaali- ja terveydenhuollon uudistuksen (sote-uudistuksen) voimaantullessa [23].

Aineisto ja menetelmät

Hyvinvointialueiden digitaalinen palvelujärjestelmä -kysely kohdennettiin hyvinvointialueiden tietohallinto- tai digitalisaatiojohtajille. Kyselyn kommentointiin osallistui 21 asiantuntijaa Terveyden ja hyvinvoinnin laitokselta ja eri yhteistyötahoilta. Kysely testattiin ajattele ääneen -menetelmällä [26] yhden kohderyhmään kuuluvan vastaajan kanssa. Tunnin kestäneen kuuntelun pohjalta tutkijat (MK, TV) jättivät pois yhden raskaaksi vastattavaksi osoittautuneen tietojärjestelmäkysymyksen ja muutaman väittämän sanoitusta täsmennettiin.

Kyselyn tietoturva ja tietosuoja -osio muodostui strukturoiduista kysymyksistä:

- 1) Oletteko päivittäneet tietoturvasuunnitelman hyvinvointialuesiirtymän myötä? vastausvaihtoehdot: Kyllä, Ei.
- 2) Kuinka tiheästi päivitätte tietoturvasuunnitelman? vastausvaihtoehdot: Emme ole määritelleet päivitystiheyttä, Merkittävien uudistusten yhteydessä, Merkittävien tapahtumien tai poikkeamien

yhteydessä, Vuosittain, Joka toinen vuosi, Kolmen vuoden välein tai harvemmin.

3) Asteikolla 0–6, kuinka kattavasti tietoturvasuunnitelmassa on huomioitu alihankintaketjut? vastausvaihtoehdot: 0=En lainkaan, 1=Erittäin suppeasti, 2=Suppeasti, 3=Kohtalaisesti, 4=Kattavasti, 5=Erittäin kattavasti, 6=Täysin.

4) Teettekö tietotilinpäättöksen säännönmukaisesti? vastausvaihtoehdot: Kyllä, Ei.

5) Oletteko viimeisten kolmen vuoden aikana levittäneet asiakkaille/potilaille suunnattua ei-lakisääteistä viestintämateriaalia, joka käsittelee digitaalisten palveluiden tai asiakastietojen sähköisen käsittelyn tietoturvaa tai tietosuojaa (esim. seinäjuuste tai somekampanja)? Vastausvaihtoehdot: Kyllä, Ei, En osaa sanoa.

Tiedonkeruu toteutettiin Webropol-kyselynä, jossa vastaajaa pyydettiin vastaamaan oman organisaationsa puolesta yksin tai yhdessä muiden asiantuntijoiden kanssa. Kyselyyn ohjeistettiin vastaamaan joko suomeksi tai ruotsiksi. Kyselyn raportoinnista

kerrottiin, että tuloksia raportoidaan hyvinvointialueittain. Aineiston analyysi toteutettiin hyödyntäen kuvailevia menetelmiä.

Tulokset

Kaikissa hyvinvointialueilta ja Helsingin kaupungilta saaduissa vastauksissa todettiin, että tietoturvasuunnitelma oli päivitetty hyvinvointialuesiirtymän myötä (jatkossa: alueet). Kyselyyn vastasi 21 aluetta.

Vastanneista alueista tietoturvasuunnitelman päivitti vuosittain enemmistö alueista (16 aluetta), seuraavaksi yleisin vastausvaihtoehto (11 aluetta) oli ”Merkittävien uudistusten yhteydessä”, ja ”Merkittävien tapahtumien tai poikkeamien yhteydessä”, jota oli käyttänyt puolet vastanneista alueista (9). Vastausvaihtoehtoa ”Kolmen vuoden välein tai harvemmin” ei ollut käyttänyt vastaajista kukaan. (Taulukko 1). Selkeää eroa vastauksissa ei havaittu sen suhteen, oliko hyvinvointialue toiminnut kuntayhtymäpohjaisena jo ennen sote-uudistusta vai ei.

Taulukko 1. Kuinka tiheästi päivitätte tietoturvasuunnitelman? Eri vaihtoehtoihin kyllä vastanneet alueittain (n=21).

Alue 2025	Vuosittain	Merkittävien tapahtumien tai poikkeamien yhteydessä	Merkittävien uudistusten yhteydessä	Emme ole määritelleet päivystiheyttä
Etelä-Karjala*	X	X	X	
Etelä-Pohjanmaa	X	X	X	
Etelä-Savo	X	X	X	
Helsinki*	X	X	X	
Itä-Uusimaa	X			
Kainuu*	X	X		
Kanta-Häme	X		X	
Keski-Pohjanmaa*				X
Keski-Uusimaa*	X			
Kymenlaakso*	X		X	
Lappi	X			
Länsi-Uusimaa	X	X		
Pirkanmaa				X
Pohjanmaa	X			
Pohjois-Karjala*	X		X	
Pohjois-Pohjanmaa	X		X	
Pohjois-Savo		X		
Päijät-Häme*			X	
Satakunta		X	X	
Vantaa ja Kerava	X	X	X	
Varsinais-Suomi	X			

*kuntayhtymäpohjaisena jo ennen sote-uudistusta aloittaneet alueet

Hyvinvointialueet olivat huomioineet alihankintaketjut tyypillisesti kohtalaisesti (n=8/21) tai kattavasti (n=7/21). Erittäin kattavasti tai täysin tietoturvasuunnitelmissa alihankintaketjut oli huomioitu kolmella (n=3/21) alueella. Kuntayhtymäpohjaisten ja sirpalemaisista lähtökohdista aloittaneiden alueiden välillä ei ilmennyt selkeitä eroja.

Tietoturvaa ja tietosuojaa tukevia toimintatapoja alueilla tutkittiin tietotilinpäätöksen ja asiakkaille ja potilaille suunnatun viestinnän osalta (Taulukko 2). Tietojen käsittelyn läpinäkyvyyttä lisäämään tarkoitettu tietotilinpäätös on organisaation itse laatima raportti, joka antaa kokonaiskuvan tietojenkäsittelystä, tietoturvallisuudesta ja tietosuojasta.

Tietotilinpäätöksen toteutti säännönmukaisesti enemmistö (n=15/21) alueista. Alle puolet (n=9/21) vastanneista alueista oli toteuttanut viimeisen kolmen vuoden aikana tietoturvaa tai tietosuojaa koskevaa ei-lakisääteistä viestintää asiakkaille tai potilaille. Alueista Etelä-Pohjanmaa, Helsinki, Kymenlaakso, Lappi, Länsi-Uusimaa, Pirkanmaa ja Pohjois-Karjala toteuttivat tietotilinpäätöksen säännönmukaisesti ja olivat myös toteuttaneet asiakkaille tai potilaille suunnatun viestintäkampanjan viimeisen kolmen vuoden aikana. Merkittävää eroa vastauksissa ei havaittu sen suhteen, oliko hyvinvointialue toiminut kuntayhtymäpohjaisena jo ennen sote-uudistusta vai ei.

Taulukko 2. Tietoturva- ja -suojaa tukevien toimintatapojen toteutus alueilla (n=21).

Alue	Säännönmukainen tietotilinpäättös	Ei-lakisääteistä viestintää asiakkaille/ potilaille tietoturvasta tai tietosuojasta
Etelä-Karjala*	Ei	Ei
Etelä-Pohjanmaa	Kyllä	Kyllä
Etelä-Savo	Kyllä	Ei
Helsinki*	Kyllä	Kyllä
Itä-Uusimaa	Ei	Ei
Kainuu*	Kyllä	Ei
Kanta-Häme	Kyllä	En osaa sanoa
Keski-Pohjanmaa*	Kyllä	En osaa sanoa
Keski-Uusimaa*	Kyllä	Ei
Kymenlaakso*	Kyllä	Kyllä
Lappi	Kyllä	Kyllä
Länsi-Uusimaa	Kyllä	Kyllä
Pirkanmaa	Kyllä	Kyllä
Pohjanmaa	Kyllä	En osaa sanoa
Pohjois-Karjala*	Kyllä	Kyllä
Pohjois-Pohjanmaa	Ei	Kyllä
Pohjois-Savo	Ei	Ei
Päijät-Häme*	Ei	Kyllä
Satakunta	Kyllä	En osaa sanoa
Vantaa ja Kerava	Kyllä	Ei
Varsinais-Suomi	Ei	Ei

*kuntayhtymäpohjaisena jo ennen sote-uudistusta aloittaneet alueet

Pohdinta

Tutkimuksessa selvitimme hyvinvointialueiden tietohallinnon johdon näkemyksiä tietoturva- ja tietosuojakäytännöistä hyvinvointialueilla. Vastauksia saatiin lähes kaikilta alueilta ja vastaajat vastasivat oman alueensa edustajina kyselyyn. Julkisella sektorilla sosiaali- ja terveydenhuollon toimijat päivittävät organisaation tietoturvasuunnitelmaa aktiivisesti. Alihankintaketjut oli huomioitu suunnitelmissa useimmiten vähintään kohtalaisesti. Tietotilinpäättöksen teki säännönmukaisesti useampi kuin kaksi kolmasosaa vastaajista. Sen sijaan reilusti alle puolella alueista oli edellisen kolmen vuoden aikana toteutettu asiakkaiden suuntaan ei-lakisääteistä viestintää, joka käsittelee

digitaalisten palveluiden tai asiakastietojen sähköisen käsittelyn tietoturva- tai tietosuojaa.

Tutkimuksessamme tietoturvasuunnitelmaa päivitettiin aktiivisesti, mikä on tärkeää, sillä Suomen kyberturvallisuuskeskuksen Kybersää-arvion mukaan tietoturvapoikkeamien määrä ja vakavuus olivat kasvussa kyselymme tiedonkeruun aikana [15]. Hyvinvointialueiden toiminta on alkanut taloudellisesti haastavissa olosuhteissa, mikä heijastuu myös digitaalisiin palveluihin ja niiden tarvitsemiin tukipalveluihin. Hyvinvointialueiden kypsyystason seurannan mukaan digitaalisten palvelujen resurssointia tulisi kehittää [16]. Koko julkista sektoria tarkastelevassa digiturvan selvityksessä taas todetaan, että monissa organisaatioissa digiturvaan ei ole budjetoitu riittävästi, eikä organisaatioilla ole

riittävästi osaavaa henkilöstöä digiturvan toteutukseen [12]. Resurssitasosta riippumatta tietoturvasuunnitelman ajan tasalla pitäminen edesauttaa tietoturvariskien ehkäisyssä ja niihin varautumisessa.

Lähes puolet alueista huomioi tietoturvasuunnitelmaansa alihankintaketjut kattavasti, mikä on tärkeää Suomen monituottajamallisessa sosiaali- ja terveydenhuollon palvelujärjestelmässä [3,18]. Vastaajien joukossa oli kuitenkin myös alueita, joissa alihankintaketjuja oli huomioitu suppeasti tai erittäin suppeasti. Organisaation omien suunnitelmien laatimisen ja päivittämisen lisäksi on tärkeää, että myös palveluntuottajien kanssa yhteistoiminnassa suunnitellaan ja varmistetaan tietoturvallisuuden ja tietosuojan toteutuminen.

Tietotilinpäätöksen toteuttaminen kuului enemmistön kyselyyn vastanneiden alueiden toimintatapoihin. Organisaation tasolla säännönmukainen tietotilinpäätöksen toteuttaminen mahdollistaa vertailun aiempiin raportointikausiin ja sidosryhmille raportoinnin. Tulostemme perusteella tietotilinpäätöksen toteuttamisessa ei ollut merkittäviä eroja alueiden lähtötilanteen mukaan. Todennäköisesti tietotilinpäätöksen toteuttamiseen vaikuttavat monet organisaatiokulttuuriin ja henkilöstöön tai muuhun resurssointiin liittyvät tekijät [16], eikä vain uusista lähtökohdista toimintatapojaan muodostava organisaatio [12]. Vapaaehtoinen tietotilinpäätös nähdään alueilla mitä ilmeisemmin hyödyllisenä työkaluna, sillä sen tekeminen oli yleistä.

Asiakkaille suunnatut vapaaehtoiset tietoturva- tai tietosuojakampanjat eivät olleet yleinen toimintatapa alueilla sote-uudistuksen alkuvuosina. Valtaosa Suomen väestöstä luottaa omiin kykyihinsä tunnistaa tietoturvariskejä [14]. Toisaalta joka kolmas kokee yksityisyysuolia, jotka liittyvät sosiaali- ja terveydenhuollon digitaalisiin palveluihin [7]. Myös esimerkiksi saksalaisten ja iso-britannialaisten on

todettu olevan huolestuneita tietoturvan ja tietosuojan toteutumisesta yhteiskunnassa [5]. Sosiaali- ja terveydenhuollon tiedonhallinnan muutokset, kuten EHDS ja muut Euroopan unionin säädökset sekä digitaalisen asioinnin lisääntyminen, luovat yhä enemmän painetta huomioida asiakkaiden todellisuutta ja huolenaiheita hyvinvointialueiden viestinnässä. Myös luottamuspuola tietoturvaa kohtaan on tunnistettu keskeiseksi esteeksi digitaaliselle asioinnille terveydenhuollossa [10,11]. Tämä puoltaa asiakasviestinnän merkitystä luottamuksen luomisessa digitaalisiin palveluihin.

Kysely lähetettiin 21 hyvinvointialueelle, Helsingin kaupungille sekä HUS-yhtymälle, jotka ovat järjestämävastuussa julkisen sektorin sosiaali- ja terveydenhuollon palveluista. Kysely testattiin kohderyhmään kuuluvan vastaajan kanssa ajattele ääneen -menetelmällä [26], mikä lisäsi kyselyn luotettavuutta. Vastaajat vastasivat alueensa edustajina. Neljässä vastuksessa kerrottiin, että vastausten muodostamisessa oli käytetty usean asiantuntijan tietämystä, mihin myös kyselyn saatekirjeessä rohkaistiin. Kokonaisuudessaan vastaukset edustavat asiantuntijoiden subjektiivisia näkemyksiä, jolloin raportoidut tulokset tulee suhteuttaa käytettyyn tiedonkeruun menetelmään. Toisaalta kyselyyn vastaaminen oli vapaaehtoista, eivätkä vastaajat saaneet korvausta tai palkintoa vastaamisesta. Lisäksi kyselyn yksittäiset substanssikysymykset eivät olleet pakollisia, mikä lisää saatujen vastausten luotettavuutta. Tietoturvaa ja tietosuojaa koskevissa kysymyksissä ei menty tekniselle tasolle, minkä vuoksi tiedonhallinnan asiantuntijan voidaan olettaa kysyneen vastaamaan kysymyksiin asianmukaisesti myös ilman teknisen tietoturva-asiantuntijan konsultointia. Alihankintaketjujen tietoturvallisuuden arviointi on työläs ja monitahoinen tehtävä, ja tutkimuksessa käytetty yksinkertainen kysymys niiden huomioinnista ei vielä anna kattavaa kuvaa siitä, millaisilla käytännöillä näitä ketjuja on

huomioitu. Vastaukset osoittavat kuitenkin, että aiheen tärkeys on ainakin jossain määrin tunnustettu. Vaikka yksittäiset kysymykset käsittelivät laajoja ja monimutkaisia kokonaisuuksia, voidaan vastausten katsoa tiivistävän asiantuntijatehtävissä työskentelevien hiljaista tietoa ja antavan arvion alueen tilanteesta.

Jatkossa on perusteltua selvittää laajemmin, miten esimerkiksi alihankintaketjujen tietoturvasuorituksia ja tietosuojaa on huomioitu sekä miten tietotilinpäätökset palvelevat hyvinvointialueita. Lisäksi jatkotutkimusta tarvitaan siitä, millaisia toimia asiakkaiden ja potilaiden luottamuksen vahvistamiseksi olisi hyödyllistä toteuttaa. Kuten tämän kyselyn toteutuksessa, myös jatkotutkimuksissa on huolehdittava siitä, että tiedonkeruu ja raportointi toteutetaan tavalla, joka ei paljasta yksittäisten organisaatioiden tietoturvakäytäntöihin tai -tilaan liittyviä yksityiskohtaisia tietoja.

Yhteenveto

Digitalisaation laajentuessa ja toimintaympäristön muuttuessa tulee julkisissa sosiaali- ja terveyspalveluissa huolehtia tietoturvasta ja tietosuojasta

Lähteet

- [1] STM. Digitaalisuus sosiaali- ja terveydenhuollon kivijalaksi: Sosiaali- ja terveydenhuollon digitalisaation ja tiedonhallinnan strategia 2023–2035. Sosiaali- ja terveysministeriön julkaisuja 2023:32. STM; 2023. <http://urn.fi/URN:ISBN:978-952-00-9889-6>
- [2] Jormanainen V. Miten sähköisiä palveluja halutaan kehittää – kansallinen strategia. Suomen Lääkärilehti 2021;76(46):2719–2723.
- [3] Jormanainen V, Hämäläinen P, Reponen, J. The Finnish healthcare and social care system and ICT-policies. Teoksessa: Vehko T. (toim.) E-health and e-

ajantasaisesti. Tietoturvasta huolehtiminen tukee alueiden ydintehtävien ylläpitoa ja toimintaedellytyksiä, minkä tulisi strategisen johtamisen kautta heijastua myös resursointiin.

Tässä tutkimuksessa esitetty vertailutieto (benchmark-tieto) tietoturvasuunnitelmista ja tietoturvaa ja tietosuojaa tukevien toimintatapojen toteutuksesta, auttaa toimijoita ymmärtämään, missä organisaatio on suhteessa muihin. Se tukee myös kansallisten tukitoimenpiteiden ja koulutusten suunnittelua. Tiedonkeruun säännöllisyys on tärkeää, sillä toistuvat vertailutiedot mahdollistavat kehityksen seuraamisen ajan myötä. Toisaalta toimintaympäristön muutos haastaa tiedonkeruun keskittymään kulloinkin keskeisiin ja merkityksellisiin asioihin.

Kiitokset

Lämmin kiitos Hyvinvointialueiden digitaalinen palvelujärjestelmä -kyselyyn vastanneille.

Sidonnaisuudet

Kirjoittajat työskentelevät Terveyden ja hyvinvoinnin laitoksella. Ei muita sidonnaisuuksia.

- welfare of Finland. Checkpoint 2022. THL Report 6/2022. Helsinki: THL; 2022. <http://urn.fi/URN:ISBN:978-952-343-891-0>
- [4] Kärkkäinen E, Virtanen L, Kainiemi E, Heponiemi T, Vehko T. Digitalisaatio ja sen strateginen johtaminen sosiaali- ja terveyspalvelujen järjestämisessä: Tilannekuva reilu vuosi hyvinvointialueiden toiminnan aloittamisen jälkeen. Terveyden ja hyvinvoinnin laitos, työpaperi 45/2024. THL; 2024. <https://urn.fi/URN:ISBN:978-952-408-343-0>

- [5] Pleger LE, Guirguis K, Mertes A. Making public concerns tangible: An empirical study of German

and UK citizens' perception of data protection and data security. *Comput Human Behav.* 2021;122:106830.

<https://doi.org/10.1016/j.chb.2021.106830>

[6] Baines R, Stevens S, Austin D, Anil K, Bradwell H, Cooper L, Maramba ID, Chatterjee A, Leigh S. Patient and public willingness to share personal health data for third-party or secondary uses: Systematic review. *J Med Internet Res.* 2024;26(1):e50421. <https://doi.org/10.2196/50421>

[7] Kyytsönen M, Vehko T, Jylhä V, Kinnunen UM. Privacy concerns among the users of a national patient portal: A cross-sectional population survey study. *Int J Med Inform.* 2024 Mar;183:105336. <https://doi.org/10.1016/j.ijmedinf.2023.105336>

[8] Snigdha EZ, Jalil MS, Dahwal FM, Saeed M, Mehedy MTJ, Al Mamun A, Khan MN, Hasan SK. Cybersecurity in Healthcare IT Systems: Business Risk Management and Data Privacy Strategies. *The American Journal of Engineering and Technology.* 2025;7(3):163–184.

<https://doi.org/10.37547/tajet/Volume07Issue03-15>

[9] WHO. Cybersecurity and privacy maturity assessment and strengthening for digital health information systems. World Health Organization. Regional Office for Europe; 2025. <https://www.who.int/europe/publications/i/item/WHO-EURO-2025-11827-51599-78854>

[10] Kruse CS, Williams K, Bohls J, Shamsi W. Telemedicine and health policy: A systematic review. *Health Policy Technol.* 2021 Mar;10(1):209–29. <https://doi.org/10.1016/j.hlpt.2020.10.006>

[11] Kemp M, Rising KL, Laynor G, Miao J, Worster B, Chang AM, Monick AJ, Guth A, Esteves Camacho T, McIntosh K, Amadio G, Shughart L, Hsiao T, Leader AE. Barriers to telehealth uptake and use: a scoping review. *JAMIA Open.* 2025;8(2):ooaf019. <https://doi.org/10.1093/jamiaopen/ooaf019>

[12] Digi- ja väestötietovirasto. Suomi.fi kehittäjille. Digiturvan kokonaiskuvapalvelu. Raportti ja keskeiset havainnot 21.5.2025. Digi- ja väestötietovirasto; 2025 [viitattu 24.11.2025]. Saatavilla: <https://kehittajille.suomi.fi/palvelut/digiturva/selvitykset/raportit/organisaation-digiturvakyselyt>

[13] Vehko T, Kärkkäinen E, Kaihlanen A, Kainiemi E, Taipale AO, Mykkänen J. Tietosuoja ja tietoturva – näkymiä hyvinvointialueille syksyllä 2024. Tutkimuksesta tiiviisti 53/2024. Helsinki: Terveystieteiden tutkimuskeskus; 2024. <http://urn.fi/URN:ISBN:978-952-408-427-7>

[14] Kyytsönen M, Ikonen J, Aalto AM, Vehko T. The self-assessed information security skills of the Finnish population: A regression analysis. *Comput Secur.* 2022;118:102732. <https://doi.org/10.1016/j.cose.2022.102732>

[15] Traficom. Kybersää Syyskuu 2025. Traficom; 2025 [viitattu 29.10.2025]. Saatavilla: <https://www.kyberturvallisuuskeskus.fi/fi/ajan-kohtaista/kybersaa>

[16] Pelkonen I (toim). Hyvinvointialueiden digitaalisten palvelujen kypsyystason arviointi: tulokset 2022 ja 2025. Terveystieteiden tutkimuskeskus, työpaperi 46/2025. THL; 2025. <https://urn.fi/URN:ISBN:978-952-408-593-9>

[17] Vehko T, Kärkkäinen E, Kaihlanen AM, Virtanen L, Kainiemi E, Heponiemi T. Sosiaali- ja terveydenhuollon tietojärjestelmät. Teoksessa: Tynkkynen LK, Paatela S, Aalto AM, Keskimäki I, Nykänen E, Peltola M, Sinervo T, Tammi T, Viita-aho M, toim. Tilannekuvia hyvinvointialueilta – muutokset palvelujärjestelmässä sote-uudistuksen alkuvuosina. Raportti 3/2025 s. 64–70. Helsinki: Terveystieteiden tutkimuskeskus; 2025. <https://urn.fi/URN:ISBN:978-952-408-459-8>

[18] Tynkkynen LK, Keskimäki I, Karanikolos M, Litvinova Y. Finland: health system summary 2023. Health system summaries. European Observatory on Health Systems and Policies; 2023.

<https://eurohealthobservatory.who.int/publications/i/finland-health-system-summary>

[19] Valtioneuvosto. Hyvinvointialueiden tehtäviä koskevat valtakunnalliset tavoitteet vuosille 2025–2029. Valtioneuvoston julkaisuja 2025: 57. Valtioneuvosto; 2025. <https://urn.fi/URN:ISBN:978-952-383-525-2>

[20] THL. Määräys tietoturvasuunnitelmaan sisällytettävistä selvityksistä ja vaatimuksista. Määräys 3/2024, THL/4/4.05.00/2024. Tiedonvälittäjät, Tieto ja tiedonhallinnan ohjaus 20.2.2024. THL; 2024 [viitattu 5.12.2025]. Saatavilla: https://thl.fi/documents/155392151/190361269/THL_Maarays_3_2024_Tietoturvasuunnitelmaan_sisallytettavista_sevityksista_ja_vaatimuksista.pdf/9123733d-c1ae-09f5-e05d-a33894441c6c/THL_Maarays_3_2024_Tietoturvasuunnitelmaan_sisallytettavista_sevityksista_ja_

[21] van Kessel R, Haig M, Mossialos E. Strengthening Cybersecurity for Patient Data Protection in Europe. *J Med Internet Res*. 2023 Aug 24;25:e48824. <https://doi.org/10.2196/48824>

[22] ENISA.Threat Landscape: Health sector, July 2023. ENISA Reports; 2023. <https://www.enisa.europa.eu/publications/health-threat-landscape>

[23] Croell K, Hetemaa T, Knape N, Leipälä J, Louet-Lehtoniemi T, Nieminen J, Ridanpää H, Suomela T, Syrjä V, Syrjänen T. Sosiaali- ja terveydenhuollon järjestäminen Suomessa. Valtakunnallinen asiantuntija-arvio, kevät 2023. Päätösten tueksi 1/2023. Terveyden ja hyvinvoinnin laitos; 2023. <https://urn.fi/URN:ISBN:978-952-408-049-1>

[24] Scriven M. Evaluation Thesaurus. 4. painos. Thousand Oaks, CA: Sage; 1991.

[25] Cousins JB. Commentary: Minimizing Evaluation Misuse as Principled Practice. *American Journal of Evaluation* 2004;25(3):391–397. <https://doi.org/10.1177/109821400402500311>

[26] Krishna-Naik V, Palmer A, Hodson NA, Tugnait A, O'Connor DB. Utilisation of a think-aloud protocol to validate a self-reported periodontitis questionnaire. *J Dent*. 2024 Nov;150:105381. <https://doi.org/10.1016/j.jdent.2024.105381>