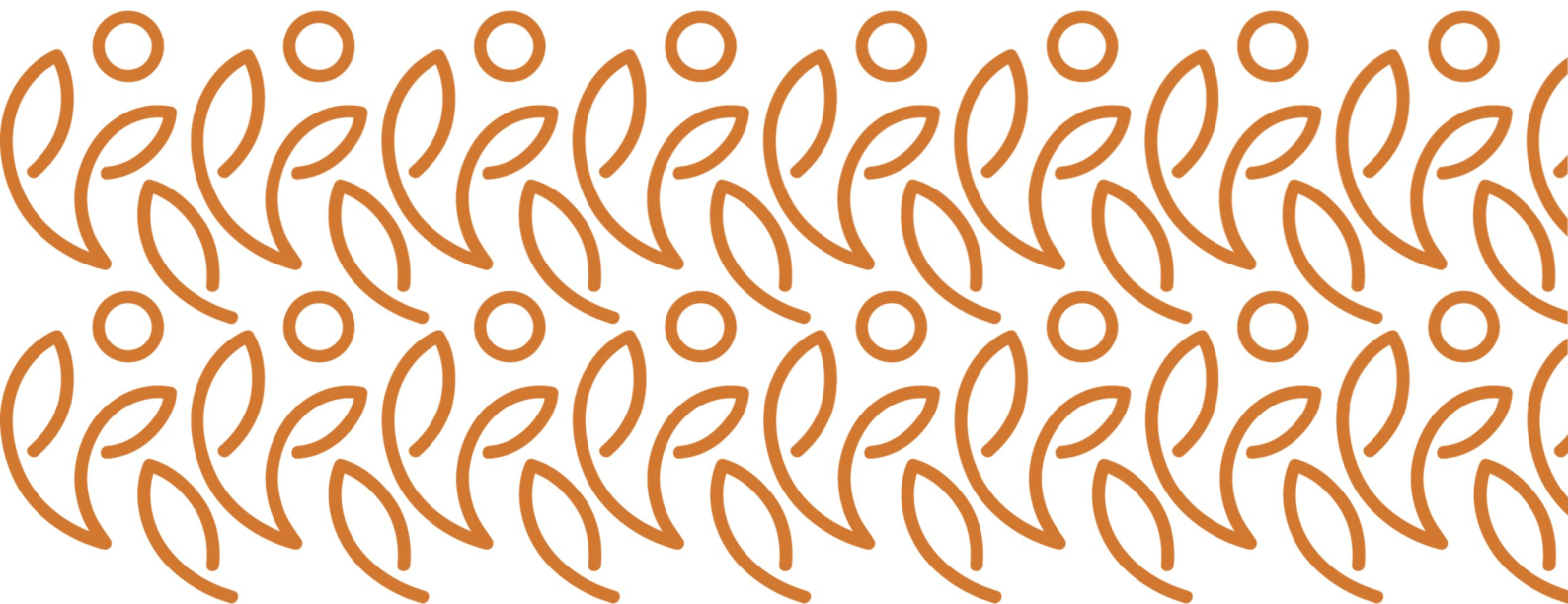


# Etelä-Pohjanmaan hyvinvointialueen tietotilinpäätös

Vuosi 2025

Hyväksytty 24.3.2026, aluehallitus



## Sisälllys

1	Johdanto.....	3
2	Toimintaympäristön muutokset vuonna 2025 .....	3
3	Merkittävimmät lakimuutokset vuonna 2025 .....	4
4	Tieto- ja korjauspyynnöt asiakastietoihin .....	4
5	Tiedonhallintalain muutosvaikutusten arvioinnit .....	5
6	Henkilöstön tietoturva- ja tietosuojasaaminen.....	6
	Tietoturva- ja tietosuojakoulutukset (Oppiportin koulutukset) .....	6
	Muut tietoturva- ja tietosuojakoulutukset .....	6
7	Tietoturva .....	7
	Tietoturva- ja tietosuojapolitiikka .....	7
	Tietoturvan kehittäminen.....	7
	Tietoturvapoikkeamat .....	7
8	Tietosuoja .....	8
	Tietosuojavastaavan tehtävistä vuonna 2025 .....	8
	Tietosuojavastaavan verkostot ja kouluttautuminen.....	9
	Vaikutustenarvioinnit osana riskienhallintaa .....	9
9	Asiakastietolain mukainen asiakastietojen käytön ja luovutuksen valvonta lokien avulla .....	9
	Rekisteröidyn oikeus saada tietoa asiakastietojensa käsittelystä.....	10
	Säännöllinen lokivalvonta .....	11
10	Henkilötietojen tietoturvaloukkaukset .....	12
11	Kehitysnäkymät ja –tarpeet .....	13
	Tietoturvan kehittämistarpeet .....	13
	Tiedonhallinnan kehitystarpeet.....	14
	Tietosuojavastaavan kokonaisarvio vuodesta 2025 sekä tietosuojan kehittämistarpeet.....	14
	Tietosuojavaltuutetun linjauksia yleisesti sekä ratkaisukäytäntöä vuonna 2025 .....	15

## 1 Johdanto

Tämä tietotilinpäätös kokoaa yhteen Etelä-Pohjanmaan hyvinvointialueen vuoden 2025 keskeiset havainnot, tunnusluvut ja toimenpiteet tiedonhallinnan, tietoturvan ja tietosuojan näkökulmista. Dokumentin tavoitteena on raportoida Etelä-Pohjanmaan hyvinvointialueen johdolle sekä alueen asukkaille HYVAEP:n tiedonhallinnan, tietoturvan ja tietosuojan tilasta ja kehitysnäkymistä. Tietotilinpäätös toimii sekä raportointivälineenä että kehittämisen tukena, ja sen tarkoituksena on vahvistaa toiminnan läpinäkyvyyttä

## 2 Toimintaympäristön muutokset vuonna 2025

Digitaalisten palveluiden kehittäminen on jatkunut suunnitelmallisesti vuonna 2025 ja kansalaisia on kannustettu markkinoinnin avulla sähköisen asioinnin pariin. Digitaalisten palveluiden lisääntyminen onkin vaikuttanut toimintaympäristöön ja muuttanut työskentelyä ja toimintatapoja HYVAEP:llä. Digitalisaation edistäminen on nimetty yhdeksi hyvinvointialueen strategian painopisteeksi ja digitaalisten palveluiden edistäminen on koko hyvinvointialueen yhteinen tehtävä. Strategian mukaan voimavaroja tulee käyttää siihen, että henkilöstö tunnistaa digitaalisten palveluiden hyödyt ja osaa niitä työssään soveltaa.

OmaEP digipalvelu on lisännyt asiakaslähtöisyyttä ja parantanut asiakkaiden mahdollisuuksia asioida sähköisesti. Erilaiset tietopyynnöt (lokitietopyynnöt, selvityspyynnöt, asiakirjapyynnöt) on helppoa täyttää ja lähettää käsiteltäväksi OmaEP digipalvelun kautta. Suuri osa tietopyynnöistä saapuukin nykyään käsiteltäväksi OmaEP:n kautta.

Digitaalisten palveluiden lisääntyminen on vaikuttanut siihen, että erilaisten tietopyyntöjen määrät ovat selkeästi nousseet. Tähän on mahdollisesti osasyynä OmaEP digipalvelun aktiivinen markkinointi, mutta myös se, että asiakkaat ovat nykyään hyvin tietosuoajatietoisia ja tietävät oikeuksistaan ja osaavat käyttää niitä.

Turvallisuusympäristön yleinen muutos vaikuttaa myös tietoturvaan ja tietosuojaan ja on huomioitava toiminnassa.

### 3 Merkittävimmät lakimuutokset vuonna 2025

Vuonna 2025 kansallinen lainsäädäntö päivittyi kyberturvallisuuden osalta EU:n CER- ja NIS2-direktiivien myötä. CER-direktiivi toimeenpantiin lailla Laki yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta, NIS2-direktiivi toimeenpantiin lailla Kyberturvallisuuslaki. Muutoksia tehtiin myös tiedonhallintalakiin tämän pohjalta. Uudet lait velvoittavat hyvinvointialueen toimintaa. Muun muassa tietoturvapoikkeamien ilmoittamiseen ja riskienhallintaan tuli uutta sääntelyä.

EU:n tekoälyasetus (EU AI Act) ja sen kansallinen toimeenpano täsmentävät hyvinvointialueiden velvollisuuksia tekoälyjärjestelmien käytössä. Kansallisen lainsäädännön täydennykset määrittävät tarkemmin valvonnan, vastuut ja seuraamukset sekä kytkevät tekoälyn käytön olemassa olevaan sääntelyyn, kuten tietosuojaan, potilasturvallisuuteen ja hyvän hallinnon periaatteisiin.

Hyvinvointialueiden on tunnistettava ja luokiteltava käyttämänsä tekoälyjärjestelmät sekä varmistettava erityisesti korkean riskin järjestelmien vaatimustenmukaisuus. Lisäksi organisaatioiden tulee huolehtia henkilöstön riittävästä osaamisesta ja käytön ohjeistuksesta. Kansalliset täydennykset vahvistavat oikeusvarmuutta, mutta edellyttävät samalla systemaattista hallintaa, dokumentointia ja jatkuvaa seurantaa tekoälyn käytön osalta.

Data-asetus (EU Data Act) puolestaan edellyttää hyvinvointialueilta aiempaa järjestelmällisempää datan hallintaa ja selkeyttä, milloin ja miten digitaalisista palveluista syntyvää dataa voidaan käyttää, jakaa tai pyytää. Samalla korostuvat tietosuojan, potilas- ja asiakasturvallisuuden sekä sopimuskäytäntöjen yhteensovittaminen muun sote-lainsäädännön kanssa.

### 4 Tieto- ja korjauspyynnöt asiakastietoihin

Sosiaali- tai terveydenhuollon asiakkaalla on oikeus saada tietää, mitä häntä koskevia tietoja on tallennettu hyvinvointialueella ylläpidettävään henkilörekisteriin. Tarkastusoikeus on rinnakkainen julkisuuslakiin pohjautuvan oikeuden itseä koskeviin tietoihin kanssa.

Vuonna 2024 otettiin käyttöön OmaEP digipalvelu, jonka kautta voi sähköisesti tehdä tietopyynnön omista sosiaali- ja terveydenhuollon asiakastiedoista. Vastaavia tietoja on edelleen mahdollista pyytää myös kirjallisesti internet –sivuilta löytyvillä lomakkeilla. Alla olevan taulukon luvut eivät ole verrannolliset aiempien vuosien vastaaviin lukuihin, koska tietopyyntöjen seuranta on vakiintunut vasta OmaEP digipalvelun käyttöönoton ja käytäntöjen kehittämisen jälkeen. Tästä syystä alla olevassa taulukossa on vain vuoden 2025 lukuja.

	2025
Tietopyyntö sosiaali- ja terveydenhuollon asiakastiedoista, sis. asianosaispyynnöt	558
Tietopyyntö omista potilasasiakirjoista	874

Tietosuoja-asetuksen mukaan sisällöltään virheellinen, tarpeeton, puutteellinen tai vanhentunut henkilötieto voidaan korjata eli oikaista, poistaa tai täydentää rekisteröidyn vaatimuksesta rekisterinpitäjän päätöksen perusteella. Rekisteröidyn oikeuden toteuttaminen on pääsääntö. Oikeutta tutustua tietoihin voidaan rajoittaa vain lakiin perustuvasta syystä. Jos rekisterinpitäjä kieltäytyy rekisteröidyn pyynnöstä, sillä on oltava kieltäytymiselle lainmukainen peruste.

Alla olevassa taulukossa on nähtävissä korjauspyyntöjen määrät vuodelta 2025 sekä määrien kehitys vuosien 2023–2025 aikana.

	2023	2024	2025
Terveydenhuollon korjauspyyntö	100	126	158
Sosiaali- ja terveydenhuollon korjauspyyntö	11	4	2

## 5 Tiedonhallintalain muutosvaikutusten arvioinnit

Tiedonhallintalain mukaan tiedonhallintayksikön (HYVAEP) on laadittava muutosvaikutusten arviointi merkittävän tietojärjestelmä- tai hallinnollisen uudistuksen yhteydessä. Vuonna 2025 ei muutosvaikutusten arviointeja laadittu. Tiedonhallintayksiköllä on kuitenkin lakisääteinen velvollisuus

tarvittavilta osin arvioinnit tehdä harkintansa mukaan. HYVAEP:llä ei ole vakiintunutta toimintamallia arviointien toteuttamiseen. Edelleen on muistettava, että tiedonhallintamallin ajantasaisuus, ylläpito ja kehittäminen on hyvinvointialueen johdon vastuulla.

## 6 Henkilöstön tietoturva- ja tietosuojiosaaminen

Henkilöstön tiedonhallinnan, tietoturvan ja tietosuojan osaamisen tasosta vastaa organisaation johto. Osaamisen varmistaminen on lakisääteistä ja riskienhallinnan kannalta keskeinen tekijä.

### Tietoturva- ja tietosuojakoulutukset (Oppiportin koulutukset)

Säännöllinen tietoturva- ja tietosuojakoulutus kuuluu kaikille HYVAEP:n työntekijöille. Jokainen työntekijä käy koulutukset palvelussuhteen alussa sekä linjauksen mukaisesti säännöllisin väliajoin. Suoritettujen koulutustietojen tulee olla tallennettuina kehittämisen ja osaamisen järjestelmään.

Lainsäädännön alati muuttuessa henkilöstön tietoturva- ja tietosuojasuojiosaamista on syytä ylläpitää peruskoulutusten lisäksi säännöllisesti.

### Muut tietoturva- ja tietosuojakoulutukset

Tietosuojavastaava toteutti reilut 12 räätälöityä ja kohdennettua tietosuojakoulutusta, joissa on painotettu muun muassa asiakassuhteen merkitystä asiakastietojen käytön lakisääteisenä perusteena. Koulutuksissa on käsitelty henkilötietojen käsittelyä lainsäädännön, rekisterinpitäjän velvollisuuksien, rekisteröityjen oikeuksien ja ammattilaisten oikeusturvan näkökulmista.

Räätälöityjä tietoturva- ja tietosuojakoulutuksia toteutettiin myös yhdessä tietoturvapäällikön kanssa. Lisäksi toteutettiin yksi tietoturva- ja tietosuojakävely.

## 7 Tietoturva

### Tietoturva- ja tietosuojapolitiikka

Etelä-Pohjanmaan hyvinvointialueen tietoturva- ja tietosuojatoiminnan perustana toimii aluehallituksen hyväksymä tietoturva- ja tietosuojapolitiikka.

Politiikassa määritellään tietoturva- ja tietosuojatoiminnan tavoitteet ja periaatteet sekä kuvataan seurannan ja valvonnan vastuut. Tietoturva- ja tietosuojapolitiikkaa on päivitetty viimeisimpänä vastuiden ja organisoitumisen osalta erityisesti vastaamaan päivitettyä hallintosääntöä. Aluehallitus on hyväksynyt päivitetyn dokumentin 8.9.2025.

Tietoturva- ja tietosuojatoiminnan tavoitteena on:

- Tukea hyvinvointialueen strategiaa, arvoja ja palveluja
- Turvata hyvinvointialueen toiminnan jatkuvuus, lainmukaisuus ja sopimuksenmukaisuus
- Ehkäistä mahdollisia häiriöitä ja vahinkoja

Tietoturva- ja tietosuojapolitiikkaa täydennetään organisaation sisäisillä ohjeilla ja dokumenteilla. Tietoturva- ja tietosuojapolitiikkaa noudatetaan hyvinvointialueen kaikessa toiminnassa, ja se velvoittaa koko henkilöstöä sekä sidosryhmiä. Sidosryhmiä ovat esimerkiksi luottamushenkilöt sekä palveluntoimittajat, joiden kanssa organisaatiolla on sopimussuhde.

### Tietoturvan kehittäminen

Vuonna 2025 tietoturvaa kehitettiin HYVAEP:n kyberturvallisuusstrategian mukaisesti. Kehitystoimenpiteet kattoivat hallinnollisia, toiminnallisia ja teknisiä osa-alueita.

HYVAEP on osallistunut kansalliseen yhteistyöhön ja harjoitteluun, kuten:

- Taisto 2025 -harjoitus
- DVV:n VAHTI-työryhmät
- STM:n Digitaalisen turvallisuuden jaosto
- SOTE-ISAC

### Tietoturvapoikkeamat

Kuten edellisenäkin vuonna, myös vuonna 2025 HYVAEP:lla korostuivat erityisesti sähköpostin välityksellä tulleet huijausyritykset. Organisaatiossa vastaanotettiin muun muassa tutun tahon nimissä lähetettyjä

tiedonkalasteluviestejä, joilla pyrittiin saamaan vastaanottajaa klikkaamaan haitallista linkkiä tai liitetiedostoa sekä antamaan käyttäjätunnus ja salasana lähettäjälle.

Onnistuakseen, hyökkäys vaatii käyttäjän toimia, kuten:

- Sähköpostissa olevan haitallisen linkin tai liitetiedoston avaaminen
- Käyttäjätunnuksen ja salasanan syöttäminen huijaussivustolle
- Hyökkääjän kirjautumispyynnön vahvistaminen

Onnistunut hyökkäys voi johtaa sähköpostitilin päätymiseen hyökkääjän haltuun, tilillä olevan tiedon vaarantumiseen sekä kaapatun sähköpostitilin käyttämiseen roskapostittamisessa käyttäjän nimissä.

## 8 Tietosuoja

Tietosuojavastaavan tehtävistä vuonna 2025

EU yleisen tietosuoja-asetuksen 38 artikla määrittelee tietosuojavastaavan asemasta. Tietosuojavastaava toimii rekisteröityjen ja Tietosuojavaltuutetun toimiston yhteyspisteenä.

Tietosuojavastaavan saamat yhteydenotot vuonna 2025 liittyivät yleiseen ohjaukseen tai neuvontaan, käyttäjälokitietoja koskeviin selvityspyyntöihin sekä tietoturvaloukkauksia koskeviin selvityksiin. Tietosuojavastaavaan otettiin yhteyttä, kun rekisteröidyillä on ollut painavia ja erityisiä perusteita siihen, että rekisterinpitäjän tulisi helpottaa rekisteröidyn asiointia. Tietosuojavastaavalle tuotiin edelleen huolta erityisryhmien asiointin heikentymisestä hyvinvointialueella. Tietosuojavastaava tekikin HYVAEP-rekisterinpitäjälle vuonna 2025 suosituksia siitä, että rekisteröidyn asiointia tulisi helpottaa, esimerkiksi asiamiehen välityksellä, ilman lomakkeita ja esimerkiksi sähköpostitse.

Tietosuojavastaava on antanut henkilötietojen käsittelyä koskevia tietoja ja neuvoja yleisesti sekä henkilötietojen käsittelyn vaikutustenarviointien (DPIA) yhteydessä. Lisäksi hän on seurannut ja valvonut henkilötietojen käsittelyn toteutumista HYVAEP:ssä yleisesti sekä vaikutustenarviointien yhteydessä. Tietosuojavastaavan kalenterissa on vuonna 2025 ollut reilut 60 merkintää vaikutustenarviointeihin liittyvistä ohjaamisista, valmisteluista, arvioinnin käsittelykokouksista ja toimintasuosituksista.

Tietosuojavastaava on enenevässä määrin käyttänyt työkalunaan muun muassa lausumia ja lausuntoja sekä toimintasuosituksia.

Rekisterinpitäjä ja tietosuojavastaava käyvät jatkuvaa dialogia ja yhdessä toimien varmistuvat siitä, että henkilötietojen käsittelyä toteutetaan tietosuojaperiaatteiden mukaisella tavalla.

#### Tietosuojavastaavan verkostot ja kouluttautuminen

Tietosuojavastaava on ylläpitänyt erityisasiantuntemustaan osallistumalla Sosiaali- ja terveydenhuollon tietosuojaseminaariin (18. - 19.11.2025) sekä Kansainvälisen tietosuojapäivän etkot-tapahtumaan (24.1.2025).

Vuonna 2025 HYVAEP:n tietosuojavastaava on osallistunut DVV:n VAHTI-verkoston tietosuojan kehittämisen työryhmään (TIKE) sekä hyvinvointialueiden tietosuojaverkoston toimintaan. Yhteistyö on tärkeää hyvinvointialueiden henkilötietojen yhdenmukaisen käsittelyn näkökulmasta.

HYVAEP:n potilas- ja sosiaalivastaavat ja tietosuojavastaava ovat käyneet ajankohtaisista teemoista keskinäistä keskustelua vuonna 2025.

#### Vaikutustenarvioinnit osana riskienhallintaa

HYVAEP toteuttaa tietosuoja-asetuksen (EU 2016/679) mukaisen vaikutustenarvioinnin (DPIA) järjestelmistä, joissa käsitellään henkilötietoja, jotta mahdolliset riskit voidaan suojatoimenpitein minimoida. Vaikutustenarviointi (DPIA) toteutetaan, kun henkilötietojen käsittely aiheuttaa vähintäänkin kaksi riskinäkökulmaa.

	2023	2024	2025
Hyväksytyt vaikutustenarvioinnit (DPIA)	31	11	21

## 9 Asiakastietolain mukainen asiakastietojen käytön ja luovutuksen valvonta lokien avulla

HYVAEP toteuttaa henkilötietojen käsittelyssä organisaatiolähtöistä säännöllistä lokivalvontaa sekä lokitieto- ja selvityspyyntöihin pohjautuvaa asiakaslähtöistä valvontaa.

Vuonna 2025 on laadittu ensimmäinen koko hyvinvointialuetta koskeva lokivalvontasuunnitelma, joka on käsitelty ensin

yhteistoimintaneuvostossa 4.3.2025 ja jonka ovat sen jälkeen hyväksyneet johtajaylilääkäri ja sosiaalijohtaja.

Lokivalvontasuunnitelma on tehty kuvaamaan Etelä-Pohjanmaan hyvinvointialueen (HYVAEP) työntekijöille sitä, miten HYVAEP:ssä toteutetaan teknistä lokien valvontaa ja analysointia sekä käyttäjälokitietojen valvontaa.

Yksityiskohtaisemmin lokivalvontaa ja sen toteutusta kuvataan vuosittain laadittavassa käyttäjälokivalvonnan vuosisuunnitelmassa, joka on salassa pidettävä asiakirja.

Asiakastietojen käsittelyn valvonta perustuu asiakastietolakiin.

Säännöllisen ja asiakaslähtöisen lokivalvonnan lisäksi tarvittaessa toteutetaan myös lokitietoihin pohjautuvia sisäisiä selvityksiä muun muassa sellaisissa tapauksissa, joissa epäillään asiakastietojen mahdollista väärinkäyttöä. Sisäisiä selvityksiä on tehty vuonna 2025 kuusi.

Käyttäjälokivalvonta painottuu edelleen asiakaslähtöiseen valvontaan, jota voitaneen rekisteröityjen näkökulmasta pitää organisaatiolähtöistä lokivalvontaa tarkempana.

Vuonna 2025 sosiaalihuollon käyttäjälokitiedoissa havaittiin järjestelmätason virheellisyyttä. Järjestelmätoimittajan näkökulmasta virheet ovat valtakunnallisia, ja se korjaa virheet viiveellä tietyn järjestelmäversion päivityksen yhteydessä. HYVAEP:llä tapahtumaa on käsitelty henkilötietojen tietoturvaloukkauksena ja tapahtumasta on ilmoitettu tietosuojaviranomaiselle. HYVAEP on pyrkinyt verkkosivuillaan informoimaan rekisteröityjä oikea-aikaisesti sosiaalihuollon käyttölokijärjestelmästä sekä järjestelmätoimittajan järjestelmäkehittämisestä.

#### Rekisteröidyn oikeus saada tietoa asiakastietojensa käsittelystä

Lokitietoihin pohjautuvien lokitieto- ja selvityspyyntöjen määrät jatkavat edelleen kasvuaan. Alla olevassa taulukossa on nähtävillä viime vuonna käsiteltyjen tieto- ja selvityspyyntöjen tarkemmat määrät.

	Vuosi 2023	Vuosi 2024	Vuosi 2025
Tietopyynnöt terveydenhuollon tietojen käsittelystä	65	122	134
Tietopyynnöt sosiaalihuollon tietojen käsittelystä	1	18	48
Terveydenhuollon selvityspyynnöt	11	8	22
Sosiaalihuollon selvityspyynnöt		4	7

Vireille tulleiden ja käsiteltyjen tieto- ja selvityspyyntöjen lisäksi vuonna 2025 on OmaEP:n kautta lähetetty myös useita sellaisia lokitieto- ja selvityspyyntölomakkeita, jotka eivät lopulta ole johtaneet vireilletuloon ja pyynnön käsittelyyn saakka. Lokitieto- ja selvityspyyntölomakkeilla on muun muassa pyydetty asiakirjoja, yhteydenottoa jostain tietystä yksiköstä, annettu palautetta sekä pyydetty toista hyvinvointialuetta koskevia tietoja. Lokitietopyyntöjä ja selvityspyyntöjä saapuu käsiteltäviksi usein myös puutteellisin tiedoin.

Puutteellisesti täytettyjen tietopyyntöjen osalta otetaan asiakkaaseen aina yhteyttä ja pyydetään tarkennuksia, jotta tietopyyntö voidaan käsitellä. Asiakkaita myös ohjataan ja neuvotaan aktiivisesti, jotta he saavat asiansa hoidettua esimerkiksi tilanteissa, joissa lomakkeella on pyydetty muita kuin lokitietoihin liittyviä tietoja. Lokitietopyyntölomaketta on muokattu käyttökokemusten perusteella ja lomakkeeseen on tehty täsmennyksiä, jotta lomake palvelisi paremmin tarkoitustaan.

#### Säännöllinen lokivalvonta

Säännöllistä lokivalvontaa on toteutettu vuoden 2025 vuosisuunnitelman mukaisesti. Tällä hetkellä säännöllinen lokivalvonta on pitkälti vielä manuaalisesti tehtävää työtä, mutta tulevaisuudessa on tavoitteena, että valvontaa pystyttäisiin toteuttamaan tekoälyavusteisesti.

Tekoälyavusteinen valvonta vaatii kuitenkin edelleen AI:n kouluttamista ja koulutustyö on vielä kesken.

## 10 Henkilötietojen tietoturvaloukkaukset

Henkilötietojen tietoturvaloukkausten tunnistamisesta ja ilmoittamiskäytänteistä on olemassa kirjallinen ohjeistus henkilökunnalle sekä ohjeistus ilmoitusten käsittelystä esihenkilöille. Molemmat ohjeet on päivitetty vuonna 2025.

Tyypillisimmin henkilötietojen tietoturvaloukkausilmoitukset (HaiPro) ovat vuonna 2025 koskeneet inhimillisistä syistä johtuneita virheitä henkilötietojen käsittelyssä. Useat ilmoitukset ovat koskeneet esimerkiksi tilanteita, joissa kirjallinen henkilötietoja sisältävä dokumentti (lääkelista, epikriisi, kutsukirje tms. asiakirja) on lähetetty väärälle vastaanottajalle tai potilas-/ asiakastietojärjestelmässä on menty väärän henkilön tietoihin, eikä henkilöä haettaessa ole käytetty henkilötunnusta. Usein näissä tilanteissa on kuvattu korostuvan kiireinen työtahti, hälyinen työympäristö ja keskeytykset työn tekemisessä, jolloin virheiden mahdollisuudet kasvavat.

Vuonna 2025 HYVAEP:llä on tullut ilmi 2 tapausta, joissa hyvinvointialueen työntekijät ovat käyttäneet asiakas- tai potilastietoja luvattomasti uteliaisuudesta tai muusta henkilökohtaisesta syystä. Edellä mainittujen lisäksi HYVAEP on rekisterinpitäjänä tehnyt valvontaviranomaiselle henkilötietojen tietoturvaloukkausilmoituksen yhdestä tapahtumasta, jossa palveluntuottajan (henkilötietojen käsittelijä) työntekijä on luvattomasti tarkastellut oman järjestelmänsä kautta 35 asiakkaan tietoja.

Alla olevassa taulukossa on tarkempia lukuja HaiPro-ilmoitusten sekä TSV-ilmoitusten määristä ja määrien kehityksestä vuosien 2023–2025 välillä:

	Vuosi 2023	Vuosi 2024	Vuosi 2025
Henkilötietojen tietoturvailmoitukset (HaiPro-ilmoitus)	268	227	276
Henkilötietojen tietoturvaloukkausilmoitukset Tietosuojavaltuutetun toimistolle (TSV-ilmoitus)	27	62	93

## 11 Kehitysnäkymät ja –tarpeet

### Tietoturvan kehittämistarpeet

Käyttäjien koulutusta on kehitettävä. Koulutusmerkinnät näkyvät esihenkilölle kehittämisen ja osaamisen järjestelmässä, mutta koulutusten raportointia ja seuranta johdolle tulisi tietoturvan ja tietosuojan osalta kehittää. Tietoturva- ja tietosuojakoulutusten tulisi olla aktiivista ja säännöllistä toimintaa. Etupainotteinen koulutus tulee edullisemmaksi kuin tietoturvaloukkausten aiheuttamat taloudelliset kustannukset.

Tietoturva- ja tietosuojakoulutukset kuuluvat yleisperehdytykseen, joka jokaisen työntekijän on suoritettava. Kyseiset koulutukset ovat HYVAEP:n johtoryhmän päätöksellä voimassa viisi vuotta, jonka jälkeen ne on uusittava. Koulutusten suorittamistiheyttä tulee arvioida suhteessa niiden sisältöön ja muuhun tietoturva- ja tietosuojakoulutukseen.

Riskienhallinnan kehittäminen. Riskienhallinnan kokonaisuutta on kehitetty hyvinvointialueella vuonna 2025 muun muassa laatimalla riskienhallintasuunnitelma, jonka aluehallitus on hyväksynyt 10.11.2025 § 349. Suunnitelman mukainen toiminta parantaa myös tietosuojan ja tietoturvan riskienhallintaa. Edelleen tulee kuitenkin tarkentaa, miten näiden riskien arviointia ja hallintakeinoja toteutetaan, jotta prosessit ovat kattavat ja tarkoituksenmukaiset.

## Tiedonhallinnan kehitystarpeet

Digipalveluiden laajentuminen on parantanut tietopalvelun saavutettavuutta asiakkaille. Valtakunnallisten Kanta-palveluiden käytön laajeneminen sosiaalihuollon tietoihin on lisännyt omien tietojen tarkastelun mahdollisuuksia OmaKannassa. Digitaalisten palveluiden kehittyessä trendi on, että tietopyyntöjen määrä on edelleen kasvussa. Tietopalvelussa arvioidaan tiedonsaantioikeus ja tietojen luovutuksen laajuus tapauskohtaisesti lainsäädäntöön nojaten. Tietopalvelutehtävä vaatii vahvaa asiantuntemusta, jonka ylläpitäminen ja kehittäminen on hyvinvointialueella keskeistä. Lisäksi tietopalveluun on jatkossa turvattava entistä paremmat resurssit. Tietopyyntöprosesseja pyritään kehittämään tulevaisuudessakin.

Eduskuntakäsittelyssä oleva uusi arkistointilaki vahvistaa digitaalisen tiedon ensisijaisuutta ja edellyttää, että arkistointi myös digitaalisesti toteutettuna huomioidaan jo tietojärjestelmien, prosessien ja palveluiden suunnitteluvaiheessa. Arkistointi ei ole pelkästään erillinen tiedon elinkaaren loppuvaiheessa huomioitava toiminto, vaan se on otettava kiinteästi osaksi tiedonhallintalain vaatimaa tiedonhallintamallia hyvinvointialueella. Tarve kehittää sekä osaamista että teknistä valmiutta digitaaliseen arkistointiin tulee kasvamaan.

Hyvinvointialueen palveluiden kanssa on pyritty laatimaan asiakastietojen käsittelyn ohjeistuksia niin, että tiedon elinkaari otetaan kokonaisuudessaan huomioon. Lisäksi on laadittu intra-ohjeistusta asiakastietojen käsittelyyn sekä analogisen aineiston arkistointiin palveluiden saataville. Tällainen ohjaus- ja kehittämistyö on jatkossakin resursoitava riittävästi.

## Tietosuojavastaavan kokonaisarvio vuodesta 2025 sekä tietosuojan kehittämistarpeet

Tietosuojavastaava on antanut HYVAEP:ssä tietoja ja neuvoja mm. lainsäädäntömuutoksiin liittyen. Esimerkiksi DPIA-lomakkeeseen lisättiin tekoälyasetukseen liittyen perusoikeuksien arviointia koskeva välilehti.

Vuonna 2025 tietosuojavastaava antoi suosituksia muun muassa diagnoositietojen teknisen täydentämisen osalta. Täydentämistä toteutettiin THL:n ohjeistuksen mukaisesti ja asiasta tiedotettiin HYVAEP:n verkkosivuilla.

HYVAEP:n tietosuojavastaava toimii merkittävän kokoisessa organisaatiossa, jossa henkilötietoja käsitellään laajasti terveydenhuollon,

sosiaalihuollon ja pelastustoimen toimialueilla. Tietosuojavastaavan näkemyksen mukaan henkilötietojen käsittelyn kokonaiskuva on se, että henkilötietojen käsittelyn merkitys ymmärretään enenevässä määrin nimenomaisesti omaehtoisesti ja että tietosuoja halutaan huolellisesti toimien edistää.

Rekisteröidyt ovat varsin tyytyväisiä saamiinsa käyttäjälökiraportteihin terveydenhuollon puolella. Sosiaalipuolella käyttölokijärjestelmä on vaatinut järjestelmätoimittajan kehitystoimenpiteitä.

Tietosuojavastaava on suositellut HYVAEP:n johdolle, että johtoryhmän ja toimialuejohtoryhmien asialista sisältäisi säännöllisesti tietosuojaan vuosikellon mukaisia aiheita. Näin tietosuojavastaavan raportointi epäkohdista suoraan ylimmälle johdolle mahdollistuisi tietosuoja-asetuksessa tarkoitettulla tavalla. Tässä on edelleen kehitettävää.

Tietosuojavastaava antaa edelleen erityisen maininnan siitä, että HYVAEP-rekisterinpitäjä toimii aktiivisesti ja huolellisesti vaikutustenarviointien (DPIA) osalta. HYVAEP-rekisterinpitäjä ohjaa siihen merkittävällä tavalla resursseja.

Tietosuojavaltuutetun toimiston linjaukset sekä lainsäädäntömuutosten valmistelutyö näyttäisivät etenevän siihen suuntaan, että hallinnolliset seuraamusmaksut olisivat mahdollisia myös julkiselle sektorille 1.1.2027 alkaen. Oletusarvona on nähty, että tietosuojavastaavan seurattua ja valvottua rekisterinpitäjän henkilötietojen käsittelyä, myös tietosuojavastaavan lausunnolla voi olla merkitystä esimerkiksi hallinnollisten seuraamusmaksujen yhteydessä.

Tietosuojavaltuutetun linjauksia yleisesti sekä ratkaisukäytäntöä vuonna 2025

Tietosuojavaltuutetun toimisto on linjannut, että rekisterinpitäjän tulee helpottaa rekisteröityjen asiointia – asiamiehen välityksellä, ilman lomakkeita ja esimerkiksi sähköpostitse.

Tietosuojavaltuutetun toimiston sivuilla todetaan terveydenhuoltoa koskevien kysymysten osalta vastauksena mm. seuraavasti (9.3.2026):

”Jos potilasasiakirjoihin merkitty diagnoosi vastaa lääkärin arviota, ei tietoa ole tarpeen oikaista, koska se kuvaa lääkärin näkemystä potilaan terveydentilasta kirjaamishetkellä. Oikaisua ei tällöin voida tehdä myöskään muualta saadun lääkärinlausunnon perusteella.

Vaikka potilaan diagnoosi myöhemmin muuttuisi, se ei tarkoita, että tieto alkuperäisestä diagnoosista pitäisi oikaista. Potilasasiakirjoista on tärkeä löytyä tieto myös potilaan aiemmista diagnooseista, jotta tiedetään, millaisten tietojen perusteella häntä on hoidettu.

Sen sijaan, jos lääkäri on esimerkiksi vahingossa kirjannut potilaan diagnoosin väärin tai diagnoosi on kirjattu väärälle potilaalle, pitää tällainen virheellinen kirjaus poistaa tai oikaista.

Tietosuojavaltuutetun toimivaltaan ei kuulu arvioida, onko lääkäri tehnyt oikean arvioinnin potilaan terveydentilasta tai diagnoosista. Jos potilas on tyytymätön saamaansa hoitoon tai terveydenhuollon ammattihenkilön toimintaan, hän voi tehdä potilaslain mukaisen muistutuksen kyseisen terveydenhuoltoyksikön johtajalle. Potilas voi myös kannella lääkärin ammattitoiminnasta Lupa- ja valvontavirastolle.”