

Ohjeen nimi	Vankiterveydenhuollon tietosuojapolitiikka
Ohjeen sisältöalue	Omavalvonta
Ohjeen käyttötaso organisaatiossa	Koko Vankiterveydenhuollon yksikkö

VANKITERVEYDENHUOLLON TIETOSUOJAPOLITIikka

1. JOHDANTO

Tämä tietosuojapolitiikka määrittelee vastuut, velvollisuudet ja tietosuojaperiaatteet VTH:n henkilötietojen käsittelyssä. Tietosuojan toteutumista VTH:ssa ohjaa lainsäädäntö, kuten EU:n yleinen tietosuoja-asetus, tietosuojalaki, julkisuuslaki, tiedonhallintalaki, tiedonhallinta-asetus, laki Vankiterveydenhuollon yksiköstä, vankeuslaki, tutkintavankeuslaki, potilaslaki, asiakastietolaki, mielenterveyslaki.

THL voi antaa määräyksiä, kuinka vankien terveydenhuolto tulee VTH:ssa järjestää (Vankeuslaki 10:11 §, Tutkintavankeuslaki 6:8 §).

2. TIETOSUOJAPERIAATTEET

Tietosuojaperiaatteet toteutuvat VTH:ssa seuraavasti

Lainmukaisuus, asianmukaisuus ja läpinäkyvyys: Henkilötietoja käsitellään aina lain edellyttämällä tavalla, oikeudenmukaisesti ja avoimesti. Potilaille ja työntekijöille tiedotetaan selkeästi, mihin tarkoituksiin heidän tietojaan kerätään ja miten niitä käsitellään.

Käyttötarkoitussidonnaisuus: Henkilötietoja käsitellään ainoastaan ennalta määriteltyihin, selkeisiin ja laillisiin käyttötarkoituksiin. Tietoja ei käytetä muuhun kuin siihen tarkoitukseen, johon ne on alun perin kerätty.

Tietojen minimointi: Keräämme ja käsittelemme vain sellaisia henkilötietoja, jotka ovat välttämättömiä kyseisen käyttötarkoituksen kannalta. Emme kerää tarpeettomia tai ylimääräisiä tietoja.

Säilytyksen rajoittaminen: Henkilötietoja säilytetään vain niin kauan kuin se on tarpeen käyttötarkoituksen toteuttamiseksi tai lain edellyttämien säilytysaikojen mukaisesti. Tiedot poistetaan tai arkistoidaan, kun niitä ei enää tarvita.

Eheys ja luottamuksellisuus: Henkilötietojen käsittelyssä varmistetaan tietojen eheys, luottamuksellisuus ja turvallisuus teknisin ja organisatorisin toimenpitein. Pääsy tietoihin on rajattu vain niille henkilöille, joilla on siihen työtehtäviensä perusteella oikeus.

Vankiterveydenhuolto rekisterinpitäjänä arvioi henkilötietojen käsittelyyn liittyvät riskit ja valitsee

arvioidun riskitason mukaan tarvittavat hallintatoimenpiteet. Tietosuojariskien hallinta on osa Vankiterveydenhuollon riskienhallintaprosessia, jolloin erityisesti merkittävän tason riskit raportoidaan johdolle saakka.

Lain edellyttämässä tilanteissa, kuten käsiteltäessä laajamittaisesti erityisiin henkilötietoryhmiin kuuluvia henkilötietoja, VTH laatii ennen henkilötietojen käsittelyn aloittamista tietosuojaa koskevan vaikutustenarvioinnin (DPIA) ja ylläpitää arviota säännöllisesti. Vaikutustenarvioinnin tuloksia käytetään niiden hallintakeinojen määrittämisessä, joilla pyritään pienentämään henkilötietojen käsittelyn riskitasoa hyväksyttävälle tasolle.

3. TIETOSUOJAN ORGANISOINTI JA VASTUUT

Tietosuojapolitiikan hyväksyy Vankiterveydenhuollon yksikön johtoryhmä. Kokonaisvastuu tietosuojan toteuttamisessa ja sen johtamisessa on Vankiterveydenhuollon johtajalla. Vankiterveydenhuollon johtaja päättää rekisterinpidon ja tietosuojan kokonaisuudesta antamalla tietosuojaa ja rekisterinpitoa koskevat periaateohjeet sekä nimeämällä tietosuojavastaavan.

Vankiterveydenhuollon tietosuojavastaava on organisaation sisäinen asiantuntija, joka seuraa henkilötietojen käsittelyä ja auttaa tietosuojasäännösten noudattamisessa sekä valvoo tietosuojalainsäädännön noudattamista. Tietosuojavastaava raportoi organisaation johdolle tietosuojan toteutumisesta. Tietosuojavastaava ei vastaa henkilökohtaisesti tietosuojan toteutumisesta VTH:ssa.

Esihenkilö vastaa siitä, että hänen alaisensa noudattavat VTH:n tietosuojakäytäntöjä ja annettuja ohjeita henkilötietojen käsittelyssä. Tämä vastuu kattaa myös sen varmistamisen, että henkilöstö on tietoinen tietosuojavelvoitteista ja saa tarvittavaa koulutusta. Esihenkilön tehtävänä on valvoa, että henkilötietoja käsitellään lainmukaisesti, turvallisesti ja käyttötarkoituksen mukaisesti.

4. TIETOSUOJAN TOTEUTTAMINEN

Tietosuoja toteutetaan VTH:ssa osana päivittäistä toimintaa, ja se perustuu lainsäädännön, viranomaisohjeiden sekä sisäisten käytäntöjen ja ohjeistusten noudattamiseen.

Tietosuojan toteuttaminen varmistetaan seuraavin keinoin:

Ohjeistus ja koulutus: Henkilöstö perehdytetään tietosuojavelvoitteisiin ja saa säännöllistä koulutusta henkilötietojen käsittelystä. Esihenkilöt vastaavat ohjeiden noudattamisen valvonnasta ja tukevat henkilöstöä tietosuojaan liittyvissä kysymyksissä.

Tietojärjestelmien hallinta: Käytössä olevat tietojärjestelmät on suojattu teknisin ja organisatorisin toimenpitein. Käyttöoikeudet myönnetään roolipohjaisesti ja vain niille henkilöille, joilla on työtehtäviensä perusteella oikeus käsitellä kyseisiä tietoja.

Tietojen käsittelyn seuranta: Henkilötietojen käsittelyä valvotaan lokitietojen ja muiden valvontakeinojen avulla. Mahdollisiin poikkeamiin puututaan viipymättä, ja niistä raportoidaan tietoturva- ja tietosuojavastaavalle.

Riskienhallinta ja vaikutustenarvioinnit: Uusien palveluiden ja järjestelmien käyttöönotossa arvioidaan henkilötietojen käsittelyyn liittyvät riskit ja tarvittaessa tehdään tietosuojaa koskeva vaikutustenarviointi (DPIA).

Yhteistyö tietosuojavastaavan kanssa: Tietosuojavastaava on otettava mukaan riittävän ajoissa suunniteltaessa henkilötietojen käsittelyä, otettassa käyttöön uusia järjestelmiä tai suunniteltaessa käsittelyn oleellisia muutoksia.

5. TOIMINTA TIETOTURVA- JA TIETOSUOJAPOIKKEAMATILANTEISSA SEKÄ ILMOITUSVELVOLLISUUS

Poikkeamatilanteilla tarkoitetaan esimerkiksi henkilötietojen luvattomia paljastumisia, katoamisia, muuttumisia tai pääsyä tietoihin ilman asianmukaista valtuutusta.

Poikkeamatilanteissa toimitaan seuraavasti:

Havaitseminen ja ilmoittaminen: Jokaisen työntekijän velvollisuus on ilmoittaa viipymättä havaitsemastaan tietoturva- tai tietosuojapojikkeamasta esihenkilölle sekä tietoturvavastaavalle tai tietosuojavastaavalle. Ilmoitus tehdään VTH:n sisäisen ohjeistuksen mukaisesti.

Arviointi ja dokumentointi: Rekisterinpitäjä arvioi tietosuojavastaavan tuella poikkeaman vakavuuden ja sen mahdolliset vaikutukset rekisteröityjen oikeuksiin ja vapauksiin. Kaikki poikkeamat dokumentoidaan, riippumatta siitä, aiheutuuko niistä ilmoitusvelvollisuutta viranomaiselle tai rekisteröidyille.

Ilmoitus viranomaiselle: Mikäli poikkeama todennäköisesti aiheuttaa riskin luonnollisten henkilöiden oikeuksille ja vapauksille, rekisterinpitäjän on ilmoitettava tietoturvaloukkauksesta tietosuojavaltuutetun toimistolle ilman aiheutonta viivytystä ja mahdollisuuksien mukaan 72 tunnin kuluessa siitä, kun loukkaus on tullut tietoon.

Ilmoitus rekisteröidylle: Jos poikkeama aiheuttaa korkean riskin rekisteröidyn oikeuksille ja vapauksille, rekisteröidylle on ilmoitettava tapahtuneesta selkeällä ja ymmärrettävällä tavalla ilman aiheetonta viivytystä.

Korjaavat toimenpiteet: Poikkeamatilanteen jälkeen toteutetaan tarvittavat tekniset ja organisatoriset toimenpiteet, joilla estetään vastaavien tilanteiden toistuminen.

NIS2: Jos poikkeama liittyy myös kyberturvallisuuteen tai sillä on merkittäviä vaikutuksia VTH:n tietojärjestelmiin, tehdään tapahtuneesta myös NIS2-ilmoitus viranomaisille erillisen ohjeistuksen mukaisesti.

6. RIKKOMUKSET JA SEURAAMUKSET

Jokainen Vankiterveydenhuollon tietojärjestelmien käyttäjä on sitoutunut noudattamaan organisaation tietosuoja- ja tietoturvaperiaatteita allekirjoittamalla salassapitositoumuksen.

VTH:ssa tietosuojarikkomuksiin suhtaudutaan vakavasti. Henkilötietojen käsittelyä koskevien ohjeiden ja lainsäädännön rikkominen voi johtaa hallinnollisiin seuraamuksiin, kuten huomautuksiin, määräyksiin tai rikosoikeudelliseen prosessiin. Jokaisella työntekijällä on velvollisuus noudattaa tietosuojaperiaatteita ja ilmoittaa havaitsemistaan poikkeamista viipymättä esihenkilölle tai tietosuojavastaavalle.

Ohjeen laatija(t)	Mari Pekkanen	14.07.2022
Tarkastanut	Jarkko Reittu Anna-Maija Strömberg Lucia Jakobsson	15.08.2022 05.08.2022 01.08.2022
Hyväksynyt	Johtoryhmä	21.09.2022
Voimassa alkaen	21.09.2022	
Päivittänyt	Mari Pekkanen, Tietosuojavastaava VTH Jarkko Reittu, Tietosuojavastaava THL	15.7.2025
Seuraava päivitys	Mari Pekkanen, Tietosuojavastaava	7/2026
Lisätietoja antaa	Mari Pekkanen, Tietosuojavastaava	0295245663