

Asia: VN/26031/2020-VM-5

## **Luonnos hallituksen esitykseksi eduskunnalle laiksi väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista annetun lain muuttamisesta**

### VTJ-lain muutokset

- Näettekö ehdotetun VTJ-lain muutoksen tehokkaaksi keinoksi vähentää tietoturvaloukkausten uhreille aiheutuvaa vahinkoa? Onko muita tehokkaampia keinoja vähentää uhreille aiheutuvaa vahinkoa?
- Viitaten kappaleeseen 4.1. keskeisistä ehdotuksista, tulisiko selvitysvastuun jakautumisesta säätää henkilötunnuksen muuttamista hakevan ja Digi- ja väestötietoviraston välillä? Tulisiko Digi- ja väestötietovirastolle säätää jokin erityinen tiedonsaantioikeus vireillä olevaan rikosasiaan liittyvistä tiedoista siinä tapauksessa, että selvitysvastuun jakautumisen katsottaisiin edellyttävän nykyistä laajempaa tiedonsaantioikeutta?

Terveyden ja hyvinvoinnin laitoksen lausunto

Alakohta 1:

Yksilöintiin käytettävien tunnisteiden tulisi lähtökohtaisesti olla muuttumattomia. Niiden käyttö esim. tunnistautumiseen, tilaamiseen, lainan nostoon tai palvelujen vireillepanoon ei pitäisi olla mahdollista. Kyseessä ei pitäisi olla salassapidettava tieto, jonka paljastuminen aiheuttaa haittaa. Henkilötunnuksen muuttaminen mahdollisten väärinkäyttömahdollisuuksien vuoksi ei tulisi olla ensisijainen keino tunnisteiden väärinkäyttöön liittyneiden ongelmien korjaamisessa. Jo olemassa olevia tunnistautumisratkaisuja tulee hyödyntää systemaattisemmin ja yksilöintitunnusten väärinkäytön mahdollistavat palvelut tulee muuttaa riittäviä tunnistautumisratkaisuja edellyttäväksi. Vahingon vähentämisen tulisi perustua ensisijaisesti siihen, että palveluissa joissa henkilöllisyyttä ei ole todennettu riittävällä tasolla tehdyt sitoumukset ovat nykyisen käytännön mukaisesti väärinkäytöstapauksissa kiistettävissä ja vastuu on palvelun tarjoajalla.

Kuten materiaalissa todetaan, tunnuksen muuttaminen on lähtökohtaisesti poikkeuksellinen turvaamistoimi ja ongelma ei poistu henkilön henkilötunnusta muuttamalla. On todennäköistä, että monissa palveluissa, joissa tunnistamista ei suoriteta riittävän vahvasti on mahdollista väärinkäyttää jatkossakin sekä passivoituja että muutettuja henkilötunnuksia. Esimerkiksi luottokorttitietojen vuotaminen mahdollistaa väärinkäytökset henkilötunnuksesta riippumatta. Laajamittainen

tunnuksen muuttamisen helpottaminen ei siis materiaalinkaan mukaan ratkaise eikä välttämättä edes merkittävästi vähennä henkilötunnuksen väärinkäyttöön, identiteettivarkauksiin tai tilausväärinkäyttöihin liittyviä ongelmia.

Kuten materiaalissa todetaan, tunnuksen muuttaminen on lähtökohtaisesti poikkeuksellinen turvaamistoimi ja ongelma ei poistu henkilön henkilötunnusta muuttamalla. On todennäköistä, että monissa palveluissa, joissa tunnistamista ei suoriteta riittävän vahvasti on mahdollista väärinkäyttää jatkossakin sekä passivoituja että muutettuja henkilötunnuksia. Esimerkiksi luottokorttitietojen vuotaminen mahdollistaa väärinkäytökset henkilötunnuksesta riippumatta. Laajamittainen tunnuksen muuttamisen helpottaminen ei siis materiaalinkaan mukaan ratkaise eikä välttämättä edes merkittävästi vähennä henkilötunnuksen väärinkäyttöön, identiteettivarkauksiin tai tilausväärinkäyttöihin liittyviä ongelmia.

#### Alakohta 2:

Muutoskriteerien kohdan 3 mukainen käytäntö on epäselvä ja tulkinnanvarainen. Palvelujen osalta, joissa ei huolehdita riittävästä henkilön identiteetin todentamisesta, tulisi selkeästi todeta, että palveluissa tehdyt sitoumukset voidaan kiistää jälkikäteisesti ja vahingosta vastaa palvelun tuottaja, jos tunnistautuminen ei ole riittävällä tasolla. Tunnuksen ennakoiva muuttaminen pelkän väärinkäyttömahdollisuuden pohjalta tai tapauskohtaisen selvitystaakan tai tiedonsaantioikeuksien lisääminen muille kuin selvästi jo tapahtunutta väärinkäyttöä tutkiville viranomaisille ei paranna yksilön oikeusturvaa eikä ole julkisen hallinnon resurssien järkevää käyttöä. Kohdan 4 mukainen käytäntö tulisi tulkita siten, että muutokset tehdään vain välttämättömissä tapauksissa, joissa on näyttöä siitä, että muuttamisella ehkäistään merkittäviä haitallisia seuraamuksia tunnuksen haltijalle. Näyttöä tunnuksen väärinkäytöstä ja vahingosta tulisi edellyttää hakijalta tai väärinkäyttöä tutkivalta viranomaiselta. Muutosmahdollisuutta on mahdollista myös pyrkiä väärinkäyttämään usein eri tavoin, joita materiaalissa ei ole eritelty tai kuvattu. Erityisen suuri riski on, jos oletuksena on luvun 4.2.1 mukainen käytäntö "hakijalta ei edellytetä näyttöä jo tapahtuneen vahingon määrästä ja väärinkäytösten toistuvuudesta".

## Vaikutusten arviointi

- **Keskeiset kehitys- ja tarkennuskohteet esityksen vaikutusten arvioinnin osalta (esimerkiksi vaikutukset tietoja käsittelevien tiedonhallintaan ja tietoaaineistojen muodostamiseen tai vaikutukset asiakkaisiin, mikäli asiakas ei ole toteuttanut hänen vastuullaan olevia toimenpiteitä).**

Luonnos ei sisällä riittävää vaikutusarviota ehdotuksen vaikutuksista yhteiskunnan kaikkien henkilötunnusta käyttävien toimijoiden tietojen käsittelyyn ja tietoaaineistojen muodostamiseen.

Tilasto- ja rekisteritoiminta:

THL:n rekisteriseurannan ja tilastotoiminnan näkökulmasta henkilötunnuksen muutoksessa on huomioitava rekisteriseurannan ja tilastotoiminnan tarpeet, joissa on seurattava ajassa henkilöstä

kerättyjä tietoja. Henkilötunnuksen vaihtuessa on taattava mahdollisuus liittää henkilön eri tunnukset yhteen ja turvattu tiedonvälitys ja tunnusten hallinta sekä DVV:ltä että eri lähdejärjestelmissä ja aineistoissa. THL:n tilasto- ja rekisteritoiminnan järjestelmissä on pääsääntöisesti jo aiemmin huomioitu henkilötunnusten muuttamismahdollisuudet, mutta rekisteriaineistoissa muutoksella voi olla lisätyötä aiheuttavia vaikutuksia. DVV:n ja THL:n välistä aineistosiirtoprosessia kehitetään edelleen myös vuonna 2021.

Asiakas- ja potilastietojen hallinta:

Henkilötunnuksen muuttuminen on sosiaali- ja terveydenhuollon palveluissa poikkeustilanne, jonka hoitaminen vaatii nykyisin erityistoimia, manuaalista työtä ja erityistä huolellisuutta, jotta potilas- ja asiakastietojen eheys voidaan varmistaa. Henkilötunnusmuutosten lisääntyminen muodostaa riskejä asiakkaalle mm. potilas- ja reseptitietojen osalta sekä hankaloittaa sosiaali- ja terveyspalvelujen ja niitä tuottavien ammattilaisten toimintaa.

Mikäli vanhoihin tietoihin ei tarvittaessa päästä käsiksi tai tietojen eheys vaarantuu, syntyy mm. asiakkaan tietojen katoamiseen ja potilasturvallisuuteen liittyviä riskejä, jotka voivat aiheuttaa esimerkiksi potilasvahinkoja. Vähintään vanhan henkilötunnuksen takana olevat kriittiset tiedot, kuten pitkäaikaissairaudet, pysyvä lääkitystieto, allergiat ja riskitiedot sekä muut hoidossa huomioitavat tiedot tulisi siis viedä myös uuden henkilötunnuksen alle.

Olemassa olevissa tiedonhallintaratkaisuisissa tai järjestelmissä ei ole kattavasti tehokkaita välineitä tai toimintoja suuren määrän tunnuksia muuttamiseen automatisoidusti eikä kaikkien tunnuksella yksilöityjen tietojen linkittämiseen uuteen tunnukseen. Henkilötunnusmuutoksia tehdään suurelta osin rekisterinpitäjittäin, manuaalisesti ja asiakirja tai asiakas kerrallaan tehtävillä korjauksilla, jotka ovat virhealttiita ja edellyttävät usein myös asiakkaan omia toimenpiteitä. Vanhoilla tai käytöstä poistuneilla tietojärjestelmillä luotujen asiakirjojen korjaaminen tai linkittäminen uusiin tunnisteisiin on vaikeaa.

Vanhalla tunnuksella luotuja tietoja jouduttaisiin todennäköisesti siirtämään uuden henkilötunnuksen alle, jotta tietoa ei tarvitse kirjata uudelleen järjestelmiin. Todennäköisesti myös vanhan henkilötunnuksen rinnakkaiskäyttö tietojen hakuun olisi mahdollistettava monissa palveluissa ja organisaatioissa, vaikka tavoitteena olisi kaikkien keskeisten terveydenhuollon ja sosiaalihuollon tietojen hyödyntäminen voimassa olevan henkilötunnuksen kautta. Valtakunnallisesti tulisi varmistaa että myös vanhoja tunnuksia vastaavat uudet tunnisteet pystytään saamaan palveluntuottajien käyttöön vanhan tunnuksen kautta.

Nykyisten menettelyjen mukainen henkilötunnuksen muuttaminen suurelle joukolle kansalaisia aiheuttaa todennäköisesti suuren työmäärän useimmille sote-palveluja tuottaville ja järjestäville organisaatioille. Sosiaali- ja terveydenhuollon ammattilaisille uusien ja vanhojen tunnisteiden hallinnasta ja muutoksista voi koitua merkittävää lisätyötä, koska käytössä olevissa tiedonhallintaratkaisuisissa ei kattavasti ole automatisoituja keinoja välittää tietoa siitä, että tunnus on muuttunut tai että asiakkaan tietoja löytyy useilla eri henkilötunnuksilla. Mikäli suuri määrä henkilötunnuksia on tarpeen muuttaa, on todennäköistä että yksittäisen henkilön tietojen muutoksia ei saada tehtyä synkronoidusti kaikille sosiaali- ja terveydenhuollon toimijoille eikä

kaikkiin heidän käyttämiinsä tietojärjestelmiin, joista kaikki eivät ole yhteydessä esimerkiksi DVV:n tietopalveluihin tai Kanta-palveluihin. Tunnuksen muuttaminen voi edellyttää esimerkiksi kaikkien reseptien mitätöintiä ja uudelleen kirjoittamista, rekisterinpitäjä- ja asiakaskohtaista asiakirjojen korjaamista tai asiakkaan tekemien tahdonilmaisujen uudelleen tekemistä.

Henkilötunnuksen muuttaminen voi heikentää tietosuojan ja tietoturvallisuuden toteutumista, koska asiakkaan tietojen käsittelyn seurannan lokijärjestelmissä käytetään henkilötunnusta yksilöimään se, kenen asiakkaan tietoja organisaation työntekijät käsittelevät. Tunnuksen muuttuessa asiakastietojen käytön jälkikäteisseuranta sekä siirtymäaikana myös hoitosuhteen todentaminen, joka on edellytyksenä potilastietojen luovutukselle voivat vaikeutua tai estyä.

Mikäli sosiaali- ja terveydenhuollon toimijoiden kehittämiin ja käyttämiin järjestelmiin mukaan lukien kansalliset tietojärjestelmäpalvelut joudutaan toteuttamaan mittavia tunnusten muutosten automatisointiin tai rinnakkaisten henkilötunnusten hallintaan liittyviä ratkaisuja, vaatii tämä säädösten lisäksi mittavaa suunnittelua a) kansallisesti yli toimialarajojen, b) kansallisesti toimialoittain (kuten sosiaali- ja terveyspalvelut, kansalliset tietojärjestelmäpalvelut kuten Kanta-palvelut), c) kaikissa tunnusta hyödyntävissä organisaatioissa sekä d) kaikkien tai useimpien tunnusta käsittelevien tietojärjestelmätuotteiden tuotekehityksessä. Muutosten määrittely, toteutus, käyttöönotto, kansallisten ja paikallisten järjestelmien sekä prosessien muutokset ja niiden käyttöönotto tulisi vaatimaan runsaasti aikaa ja resursseja. Eri tasojen valtakunnallinen koordinointi nopealla aikataululla olisi erittäin haastavaa ja muutokset koskisivat suurta toimijajoukkoa. Esimerkiksi sosiaali- ja terveydenhuollossa muutos koskettaisi satoja julkisia ja tuhansia yksityisiä palvelunantajia sekä useita satoja tietojärjestelmiä, sekä kansallisia ja paikallisia tietojärjestelmäratkaisuja, joista useat sisältävät satoja miljoonia potilas- ja asiakasasiakirjoja. Kehittämisen kustannukset olisivat mahdollisesti lähellä aiempia henkilötunnuksen pitkän aikavälin uudistamiseen liittyneitä kustannusarvioita, vaikka tunnuksen muoto ei muuttuisikaan.

Riskinä on myös se, että muut merkittävästi ja aidosti potilas- ja tietoturvallisuutta sekä asiakkaiden parempia palveluja kehittävät hankkeet ja uudistukset vaarantuvat tai viivästyvät, jos tunnusten muuttamiseen liittyvien ratkaisujen kehitys edellyttäisi kehitysresurssien uudelleenkohdistamista sekä kansallisesti että paikallisesti tasolla. Asiakas- ja potilastietojen sekä tietoturvallisuuden uudistuvien säädösten toimeenpano, sote-uudistukseen sekä pandemian hallintaan ja seurantaan liittyvät tiedonhallinnan kehityskohteet voivat vaarantua, mikäli kehittämisresurssit ohjataan henkilötunnusten käsittelyn ja muuttamisen uudistuksiin.

Aikataulullisesti laajamittaisen henkilötunnusten muuttamiseen liittyvän automatisoinnin ja tietojen eheyden varmistamisen kyvykkyyksien kehittäminen muutaman kuukauden aikana ei ole realistista, koska on pystyttävä varmistamaan, että vanhan henkilötunnuksen kautta syntyneet sosiaalihuollon ja terveydenhuollon tiedot ja asiakirjat saadaan tarvittaessa myös jatkossa käyttöön vaivatta ja turvallisesti. Mikäli uusia tietojärjestelmäkyvykkyyksiä tarvitaan laajasti, siirtymäajan olisi oltava useiden vuosien mittainen, ja siitä huolimatta olisi käytännössä mahdotonta varmistaa sitä, että esimerkiksi pienillä ja suurilla palveluntuottajilla olisi yhtäaikaaisesti käytössä esimerkiksi rinnakkaisten tunnusten hallinnan kyvykkyyksiä. Muutokset eivät rajoitu keskitettyihin kansallisiin

tietojärjestelmäpalveluihin. THL on lausunut vastaavasta asiasta ja siirtymäaikatatarpeesta aiempien hetu-uudistukseen liittyvien lausuntojen yhteydessä.

## Yleiset kommentit

- **Yleiset kommentit hallituksen esityksen luonnoksesta**

Henkilötunnus on keskeisin asiakas- ja potilastiedot kansalaiseen linkittävä tunniste sosiaali- ja terveydenhuollossa. Tunnistetta on pitkän ajan kuluessa käytetty sekä paperi- että sähköisissä järjestelmissä tietojen linkittämiseen ja löytämiseen, käyttäjäorganisaatioita on erittäin suuri määrä esimerkiksi sosiaali- ja terveydenhuollossa, ja kaikissa tietoa käsittelevissä järjestelmissä muutosten yhtäaikainen tekeminen tai vanhojen ja uusien tunnusten välisten vastaavuuksien hallinta ei ole mahdollista. Tunnusten muuttamiseen liittyy nykyisin runsaasti manuaalista ja erityistä huolellisuutta vaativaa työtä muun muassa sosiaali- ja terveydenhuollon organisaatioissa.

Tunnuksen muuttamisen merkittävästä laajentamisesta aiheutuisi laajenevia eheys- ja saatavuusriskejä, kustannuksia ja lisätyötä laajasti yhteiskunnan julkisiin ja yksityisiin palveluihin. On olemassa riski siihen, että yksilön tarvitsemat palvelut ja esimerkiksi sosiaali- ja terveydenhuollon potilas- ja asiakastietojen eheys ja potilasturvallisuus häiriintyvät tunnuksen muuttamisen yhteydessä useissa sellaisissakin palveluissa, joita yksilö jatkuvasti tarvitsee ja haluaa säilyttää ja joissa henkilötunnuksen väärinkäytöstä syntyneet haitat ovat nykyisin olleet tietyvästi suhteellisen vähäisiä.

Tunnuksen muuttamisen automatisointiratkaisuja tai rinnakkaisten tunnusten hallinnan ratkaisuja ei käytännössä ole mahdollista kehittää kaikkiin sosiaali- ja terveyspalveluissa käytettäviin järjestelmiin kustannustehokkaasti tai yhtäaikaisesti ehdotetulla voimaantuloaikataululla. Laajan tunnusten vaihtamisen automatisoinnin tai rinnakkaisten tunnusten hallinnan edellyttämiä järjestelmäkehitystoimenpiteitä kaikilta toimijoilta ja tietojärjestelmiltä nopealla aikataululla ei ole realistista edellyttää.

THL pitää tärkeänä, että henkilötunnuksen muuttamisen kynnyks asetetaan uudessakin lainsäädännössä korkealle siten, että tunnusten muuttaminen ei ole ensisijainen vaan poikkeuksellinen ja viimekätinen toimenpide tapauksissa, joissa rikollista väärinkäyttöä on tapahtunut. Yksin sivullisten haltuunsa saama henkilötunnustieto ei pitäisi olla peruste tunnuksen muuttamiselle vaan muuttamista tarvitaan viimeisenä keinona tilanteissa, joissa tietoa on käytetty väärin ja tunnuksen muuttamisella voidaan aidosti estää lisävahinkoja.

Mykkänen Juha  
Terveysten ja hyvinvoinnin laitos