Omatietovarantoon liittyneiden hyvinvointisovellusten sertifiointi

Minna Linsamo ja Emilia Varonen

27.8.2021

Terveyden ja hyvinvoinnin laitos

Esityksen sisältö

- Uusi asiakastietolaki
- Keskeisimmät asiakastietolain kohdat hyvinvointisovelluksien näkökulmasta
- Keskeisimmät asiakastietolain kohdat hyvinvointisovellusten olennaisista vaatimuksista
- Määräys omatietovarantoon liitettävien hyvinvointitietoja käsittelevien hyvinvointisovellusten olennaisista vaatimuksista ja sertifioinnista
- Sertifiointiprosessi
- Esimerkkejä olennaisista vaatimuksista: saavutettavuus
- Esimerkkejä olennaisista vaatimuksista: tietoturva

Uusi asiakastietolaki

- Hallituksen esitys eduskunnalle laiksi sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä sekä eräiksi siihen liittyviksi laeiksi HE 212/2020 vp tulee voimaan todennäköisesti 1.11.2021 (jatkossa asiakastietolaki)
- Lain tarkoituksena on edistää ja mahdollistaa sosiaali- ja terveydenhuollon tuottamien asiakastietojen ja asiakkaan itsensä tuottamien hyvinvointitietojen tietoturvallista käsittelyä terveydenhuollon ja sosiaalipalveluiden järjestämisen ja tuottamisen käyttötarkoituksissa.
- Lain tarkoituksena on myös edistää asiakkaan tiedonsaantimahdollisuuksia asiakastietojensa käsittelystä.

Keskeisimmät asiakastietolain kohdat hyvinvointisovelluksien näkökulmasta 1/

Määritelmiä:

- Hyvinvointitieto: henkilön itsensä tuottamia terveyttään ja hyvinvointiaan koskevia tietoja, jotka henkilö on tallentanut omatietovarantoon
- Omatietovaranto: hyvinvointitietojen säilyttämistä ja käsittelemistä varten valtakunnallisiin tietojärjestelmäpalveluihin muodostettua keskitettyä sähköistä tietovarantoa;
- Hyvinvointisovellus: yksityishenkilön käyttämää omatietovarantoon liittyvää sovellusta, jolla käsitellään hyvinvointitietoja, ja johon henkilö voi saada asiakastietonsa arkistointipalvelusta, reseptikeskuksesta ja tiedonhallintapalvelusta;
- Sertifiointi: menettelyä, jolla todennetaan tietojärjestelmän tai hyvinvointisovelluksen täyttävän sitä koskevat tuotantokäyttöä varten vaadittavat olennaiset vaatimukset.

Keskeisimmät asiakastietolain kohdat hyvinvointisovelluksien näkökulmasta 2

13§ Omatietovaranto:

- Henkilö voi tallentaa hyvinvointitietojaan omatietovarantoon hyvinvointisovelluksilla tai kansalaisen käyttöliittymän kautta ja hyödyntää niitä sieltä hyvinvointinsa edistämiseksi.
- Henkilöllä on oikeus päättää tietojensa käytöstä, muuttamisesta ja poistamisesta omatietovarannosta.
- Henkilö voi antaa suostumuksen siihen, että palvelunantajalle voidaan luovuttaa omatietovarannossa olevia hyvinvointitietoja sosiaali- ja terveyspalvelujen toteuttamiseksi.
- Hoitoon tai palveluun vaikuttavien tietojen kirjaamisesta asiakas- tai potilasasiakirjoihin säädetään potilaslaissa, asiakaslaissa ja asiakasasiakirjalaissa.
- Henkilön omatietovarannossa olevat tiedot on säilytettävä, kunnes henkilö on poistanut ne omatietovarannosta tai enintään 5 vuotta henkilön kuolemasta.

29§ Tietojärjestelmien ja hyvinvointisovellusten käyttötarkoitus ja luokittelu

- Hyvinvointisovelluksen valmistajan on laadittava kuvaus hyvinvointisovelluksensa käyttötarkoituksesta ja siitä, kuinka se täyttää sitä koskevat olennaiset vaatimukset.
- Hyvinvointisovellukset kuluvat luokkaan A.

Keskeisimmät asiakastietolain kohdat hyvinvointisovelluksien näkökulmasta 3

30§ Tietojärjestelmien ja hyvinvointisovellusten rekisteröinti

- Hyvinvointisovelluksen valmistajan on ilmoitettava hyvinvointisovelluksesta Sosiaali- ja terveysalan lupa ja valvontavirastolle ennen hyvinvointisovelluksen ottamista tuotantokäyttöön.
- Sosiaali- ja terveysalan lupa- ja valvontavirasto ylläpitää julkista rekisteriä sille ilmoitetuista sosiaali- ja terveydenhuollon hyvinvointisovelluksista. Rekisterissä on oltava tieto:
  1. tuotantokäyttöön tarkoitetuista hyvinvointisovelluksista, niiden käyttötarkoituksista sekä niiden täyttämistä olennaisista vaatimuksista;
  2. luokkaan A kuuluvien tuotantokäyttöön hyväksyttyjen hyvinvointisovellusten yhteentoimivuuden testauksen tuloksista;
  3. luokkaan A kuuluvien tuotantokäyttöön hyväksyttyjen hyvinvointisovellusten tietoturvallisuuden arvioinnista saadun tietoturvallisuuden arviointia koskevan todistuksen voimassaolosta; sekä
  4. tuotantokäytössä olevan luokkaan A kuuluvan hyvinvointisovelluksen merkittävästä poikkeamasta poikkeaman keston ajan.

Keskeisimmät asiakastietolain kohdat hyvinvointisovelluksien näkökulmasta 4

31§ Tietojärjestelmän ja hyvinvointisovelluksen ottaminen tuotantokäyttöön

- Luokkaan A kuuluvan hyvinvointisovelluksen saa ottaa tuotantokäyttöön ja liittää valtakunnallisiin tietojärjestelmäpalveluihin sen jälkeen, kun tietojärjestelmä tai hyvinvointisovellus on sertifioitu 35 §:n mukaisesti.
- Hyvinvointisovellusta ei saa ottaa tuotantokäyttöön, ellei siitä ole voimassa olevia tietoja 30 §:n 2 momentissa tarkoitetussa rekisterissä tai luokkaan A kuuluvan hyvinvointisovelluksen tietoturvallisuuden arviointia koskeva todistus on vanhentunut.

Keskeisimmät asiakastietolain kohdat hyvinvointisovelluksien näkökulmasta 5

32§ Tietojärjestelmän ja hyvinvointisovelluksen käyttöönoton jälkeinen seuranta

- Hyvinvointisovelluksen valmistajan on seurattava ja arvioitava ajantasaisella järjestelmällisellä menettelyllä hyvinvointisovelluksesta sen tuotantokäytön aikana saatavia kokemuksia.
- Hyvinvointisovelluksen merkittävistä poikkeamista on ilmoitettava kaikille hyvinvointisovelluksen käyttäjille.
- Hyvinvointisovelluksen valmistajanon ilmoitettava hyvinvointisovellusten merkittävistä poikkeamista Kansaneläkelaitokselle ja Sosiaali- ja terveysalan lupa- ja valvontavirastolle.
- Luokkaan A kuuluvan hyvinvointisovelluksen olennaisista muutoksista on ilmoitettava tietoturvallisuuden arviointilaitokselle ja Kansaneläkelaitokselle.
- Hyvinvointisovelluksen valmistajan on seurattava hyvinvointisovellusten olennaisten vaatimusten muutoksia ja tehtävä muutosten edellyttämät korjaukset
- Tietoturvallisuuden arviointia koskeva todistus tai yhteentoimivuuden testaus on uudistettava, jos hyvinvointisovellukseen tehdään merkittäviä muutoksia, tai olennaisia vaatimuksia on muutettu tavalla, joka edellyttää uutta sertifiointia.

Keskeisimmät asiakastietolain kohdat hyvinvointisovellusten olennaisista vaatimuksista 1

33§ Tietojärjestelmäpalvelun tuottajan ja valmistajan sekä hyvinvointisovelluksen valmistajan yleiset velvollisuudet

- Hyvinvointisovelluksen valmistaja on vastuussa sovelluksen suunnittelusta ja valmistuksesta.
- Hyvinvointisovelluksen valmistajan on laadittava kuvaus hyvinvointisovelluksensa käyttötarkoituksesta ja annettava sen yhteydessä järjestelmän käyttäjälle yhteentoimivuuden, tietoturvallisuuden ja tietosuojan sekä toiminnallisuuden kannalta tarpeelliset tiedot ja ohjeet järjestelmän käyttöönotosta, tuotantokäytöstä ja ylläpidosta.

Keskeisimmät asiakastietolain kohdat hyvinvointisovellusten olennaisista vaatimuksista 2

34§ Tietojärjestelmälle ja hyvinvointisovellukselle asetettavat olennaiset vaatimukset

- Asiakastietojen käsittelyssä käytettävän tietojärjestelmän ja hyvinvointisovelluksen tulee täyttää yhteentoimivuutta, tietoturvaa ja tietosuojaa sekä toiminnallisuutta koskevat olennaiset vaatimukset.
- Hyvinvointisovelluksen tulee täyttää saavutettavuusvaatimukset.
- Terveyden ja hyvinvoinnin laitos antaa tarkempia määräyksiä olennaisten vaatimusten sisällöstä ja siitä, mitkä olennaiset vaatimukset on täytettävä eri palveluissa käytettävissä tietojärjestelmissä ja hyvinvointisovelluksissa.

35§ Vaatimustenmukaisuuden osoittaminen

- Luokkaan A kuuluvan hyvinvointisovelluksen vaatimustenmukaisuus on osoitettava sertifioinnilla eli hyvinvointisovelluksen valmistajan antamalla selvityksellä siitä, että hyvinvointisovellus täyttää käyttötarkoituksensa mukaiset toiminnallisuutta koskevat vaatimukset, hyväksytyllä yhteentoimivuuden testauksella ja 37 §:n mukaisella tietoturvallisuuden arviointilaitoksen antamalla tietoturvallisuuden arviointia koskevalla todistuksella.
- Hyvinvointisovelluksen valmistaja vastaa siitä, että tietojärjestelmä tai hyvinvointisovellus on sertifioitu.
- Terveyden ja hyvinvoinnin laitos voi antaa määräyksiä vaatimustenmukaisuuden osoittamisessa noudatettavista menettelyistä ja annettavan selvityksen sisällöstä.

Keskeisimmät asiakastietolain kohdat hyvinvointisovellusten olennaisista vaatimuksista 3

36§ Yhteentoimivuuden testaaminen

- Luokkaan A kuuluvan tietojärjestelmän ja hyvinvointisovelluksen on oltava yhteentoimiva valtakunnallisten tietojärjestelmäpalvelujen ja siihen liitettyjen muiden tietojärjestelmien kanssa.
- Yhteentoimivuus on osoitettava Kansaneläkelaitoksen järjestämässä yhteentoimivuuden testauksessa.
- Ennen yhteentoimivuuden testausta tietojärjestelmäpalvelun tuottajan ja hyvinvointisovelluksen valmistajan on annettava Kansaneläkelaitokselle selvitys siitä, miten tietojärjestelmän tai hyvinvointisovelluksen toiminnallisuutta koskevat vaatimukset on toteutettu ja testattu.
- Yhteentoimivuuden testauksen ajankohdasta ja toteuttamisesta on sovittava Kansaneläkelaitoksen kanssa.

37§ Tietoturvallisuuden arviointi

- Luokkaan A kuuluvan hyvinvointisovelluksen olennaisten tietoturvallisuusvaatimustenmukaisuuden arviointi suoritetaan tämän lain ja tietoturvallisuuden arviointilaitoksista annetun lain mukaisesti.
- Tietoturvallisuuden arviointi tehdään hyvinvointisovelluksen valmistajan hakemuksesta.
- Tietoturvallisuuden arviointilaitoksen on annettava suorittamastaan tietoturvallisuuden arvioinnista tietojärjestelmäpalvelun tuottajalle ja hyvinvointisovelluksen valmistajalle todistus sekä siihen liittyvä tarkastusraportti.
- Arviointi on suoritettava tietojärjestelmän ja hyvinvointisovelluksen käyttötarkoitusta koskevien olennaisten vaatimusten tai järjestelmään tehtyjen muutosten laajuuden mukaisesti.
- Tietoturvallisuuden arviointi on voimassa kolme vuotta.

Keskeisimmät asiakastietolain kohdat hyvinvointisovellusten olennaisista vaatimuksista 4

38 Tietoturvallisuuden arviointilaitoksen ilmoittamisvelvollisuus

- Tietoturvallisuuden arviointilaitoksen on ilmoitettava Sosiaali- ja terveysalan lupa- ja valvontavirastolle, Kansaneläkelaitokselle ja Terveyden ja hyvinvoinnin laitokselle tiedot kaikista myönnetyistä, muutetuista, täydennetyistä ja evätyistä todistuksista.
- Tietoturvallisuuden arviointilaitoksen on pyydettäessä annettava Sosiaali- ja terveysalan lupa ja valvontavirastolle kaikki tarvittavat lisätiedot tietojärjestelmistä ja hyvinvointisovelluksista, joille arviointilaitos on myöntänyt tietoturvallisuuden arviointia koskevan todistuksen.

Uuden asiakastietolain siirtymäsäännökset

- Henkilö voi antaa suostumuksen siihen, että palvelunantajalle voidaan luovuttaa omatietovarannossa olevia hyvinvointitietoja sosiaali- ja terveyspalvelujen toteuttamiseksi => siirtymäsäännöksen mukaan sovelletaan viimeistään 1.1.2024.
- Potilastiedot voidaan luovuttaa asiakkaalle hyvinvointisovelluksen tai kansalaisen käyttöliittymän kautta. Saadakseen tiedot hyvinvointisovellukseen potilaan tulee ottaa hyvinvointisovellus käyttöön ja hyväksyä tietojen luovutus => siirtymäsäännöksen mukaan sovelletaan viimeistään 1.12.2023.
- Sosiaalihuollon asiakastiedot voidaan luovuttaa asiakkaalle hyvinvointisovelluksen tai kansalaisen käyttöliittymän kautta. Saadakseen tiedot hyvinvointisovellukseen asiakkaan tulee ottaa hyvinvointisovellus käyttöön ja hyväksyä tietojen luovutus => siirtymäsäännöksen mukaan sovelletaan viimeistään 1.5.2025.
- Reseptitietojen luovutus hyvinvointisovelluksille 1.12.2022.

Määräys omatietovarantoon liitettävien hyvinvointitietoja käsittelevien hyvinvointisovellusten olennaisista vaatimuksista ja sertifioinnista

- Määräys on työn alla THL:ssä. Työstetään yhdessä sidosryhmien kanssa.
- Lausuntokierrokselle todennäköisesti syyskuun alussa.
- Koostuu itse Määräysdokumentista ja Olennaiset vaatimukset excelistä.

Sertifiointiprosessi

Luonnos

1. Yhteistestaus

Ennen yhteistestausta toimita Kelalle Olennaiset vaatimukset Excel

Ilmoittaudu Kelan Kanta-palvelujen kanssa suoritettavaan yhteistestaukseen

Sovi yhteistestauksen testauksen ajankohdasta ja toteuttamisesta Kelan kanssa

Hyväksytysti suoritetun yhteistestauksen jälkeen Kela antaa yhteistestauslausunnon

Yhteistestauslausunto on edellytys tietoturvalaitoksen myöntämälle auditointitodistukselle

2. Tietoturva-auditointi

Ilmoittaudu tietoturvallisuuden arviointilaitoksen kanssa suoritettavaan tietoturvallisuuden auditointiin

Toimita arviointilaitokselle etukäteen Olennaiset vaatimukset Excel (liite 1) ja yhteistestauslausunto

Auditoinnin hyväksytysti läpäissyt hyvinvointisovellus saa todistuksen sekä siihen liittyvän tarkastusraportin arviointilaitokselta

Arviointi on suoritettava hyvinvointisovelluksen käyttötarkoitusta koskevien olennaisten vaatimusten tai sovellukseen tehtyjen muutosten laajuuden mukaisesti

Todistus on voimassa enintään kolme vuotta. Todistuksen voimassaoloa voidaan jatkaa enintään kolmeksi vuodeksi kerrallaan

Tietoturvallisuuden auditointi on maksullinen

3. Ilmoitus Valviralle

Ilmoita hyvinvointisovelluksesta Valviralle ennen sovelluksen ottamista tuotantokäyttöön

Toimita Valviralle ilmoitus sekä siihen liittyvät kuvaukset, joilla vakuutat sovelluksen asianmukaisesti asennettuna ja käyttötarkoituksen ja ohjeiden mukaan käytettynä täyttävän olennaiset vaatimukset

Sovelluksen käyttöönotto voidaan aloittaa sen jälkeen, kun sovellus on hyväksytty Valviran rekisteriin

4. Käyttöönotto

Hyvinvointisovelluksen voi liittää osaksi valtakunnallisia tietojärjestelmäpalveluja, kun se on läpäissyt sertifioinnin aiemmat kolme vaihetta.

5. Seuranta

Seuraa järjestelmällisesti käyttöönoton jälkeen saatavia kokemuksia

Ilmoita merkittävistä poikkeamista kaikille hyvinvointisovelluksen käyttäjille

Ilmoita merkittävistä poikkeamista Kelalle ja Valviralle

Ilmoittaudu tarvittaessa olennaisten muutosten takia tehtävään Kelan yhteistestaustarpeen arviointiin sekä tietoturvallisuuden uudelleenauditointitarpeen arviointiin

Esimerkkejä olennaisista vaatimuksista: saavutettavuus

Kriteeri	Kuvaus	Vastaus
Saavutettavuusvaatimusten täyttäminen	Hyvinvointisovelluksen tulee täyttää saavutettavuusvaatimukset.fi sivustolla esitetyt ajankohtaiset saavutettavuuskriteerit. Hyvinvointisovelluksen saavutettavuus tulee testata itse toteutetun tai ulkopuolisen toimijan toteuttaman saavutettavuuden auditoinnin avulla. Saavutettavuusvaatimukset ja sovelluksen saavutettavuus tulee tarkistaa vähintään kerran vuodessa.	[Kyllä]
Saavutettavuusselosteen tekeminen	Hyvinvointisovelluksen tulee tehdä käyttäjille saavutettavuusseloste. Selosteen sisältö on määrätty EU tasolla ja sen tulee kertoa käyttäjälle palvelun saavutettavuuden taso. Saavutettavuusselosteen tekemiseen voi hyödyntää saavutettavuusvaatimukset.fi sivulta löytyvää saavutettavuusselostetyökalua tai selosteen voi muotoilla itse KOMISSION TÄYTÄNTÖÖNPANOPÄÄTÖS (EU) 2018/1523, perusteella. Saavutettavuuden tarkistamisen yhteydessä saavutettavuusseloste tulee tarpeen vaatiessa päivittää.	[Kyllä]
Saavutettavuuspalaute	Sovellustoimittajalla tulee olla valmius ottaa vastaan saavutettavuuspalautetta sähköiseen yhteystietoon. Vastaus saavutettavuuspalautteeseen tulee antaa 14 päivän kuluessa palautteen saamisesta.	[Kyllä]

Esimerkkejä olennaisista vaatimuksista: tietoturva

Kriteeri	Kuvaus	Vastaus
5.4.2.5 Onko käytössä prosessi, jolla estetään hyvinvointisovelluksen lähdekoodin luvaton käyttö ja muutokset?	Prosessi voi sisältää seuraavat: - Tarkista sovelluksen eheys, tarkista, että sovellus ja sen resurssit eivät ole muuttuneet: - käytä alustapalvelua (esim. AndroidTM SafetyNet -varmennus, iOS® App Storen kuitti); -suorita muistin sisäisten koodien eheystarkastukset suojautuaksesi koodin muuttumiselta ja/tai ajon aikaiselta koukkaamiselta. - Tee käänteisestä suunnittelusta vaikeampaa: - Hämärrä (obfuscate) koodi; - Salaa tiedot (esim. merkkijonot) hämärtääksesi sovelluslogiikkaa lisää. - Poista kehittäjien ominaisuudet käytöstä: - Poista debuggaus käytöstä sovellusasetuksissa; - Tarkista, onko laite kehittäjätilassa, jos se tukee alustaa, esimerkiksi AndroidTM; - Tarkista, onko debugger liitetty ja/tai jäljitetäänkö prosessia. Alustoilla, joissa on hallittu koodin tarkistus tarkista hallitun ja natiivikoodin debuggerit. Tarkista laitteen/alustan eheys varmistaaksesi, että sitä ei ole muunneltu. Suosi alustapalveluja, jos saatavilla, esimerkiksi AndroidTM SafetyNet -varmennusta. Impelementoi kustomoitu tai käytä kolmannen osapuolen juuren/jailbreak-tunnistusta ainoastaan, jos alusta ei tarjoa sisäänrakennettua ratkaisua [38] Terveyssovelluksen lähdekoodi on suojattava suunnittelun, kehityksen ja käyttöönoton aikana, jos lähdekoodi sisältyy jaettuun hyvinvointisovellukseen.	Todisteet: Asianmukainen vakiokäytäntö, vaihtoehtoisesti raportti tai muuta näyttöä CRESTin [37] tai vastaavan asianomaisen elimen suorittamasta kooditason turvallisuusarvioinnista.
5.4.2.9 raportoidaanko, tunnistetaanko, arvioidaanko, kirjataanko, vastataanko, tuodaanko esille ja ratkaistaanko tietoturva haavoittuvuudet nopeasti ja tehokkaasti?	Tietoturvahaavoittuvuuksia koskevia tietolähteitä voivat olla julkisesti viranomaisilta saatavilla olevat raportit sekä julkaisut, joita tarjoavat esimerkiksi käyttöjärjestelmien ja kolmansien osapuolien ohjelmistojen toimittajat (IEC 82304-1: 2016, 4.1). Seurantaprosessiin on sisällyttävä vähintään: - hyvinvointisovelluksen käyttäjien ja asiakkaiden tiedotus havaituista tietoturvahaavoittuvaisuuksista sekä muutoksista hyvinvointisovelluksen käyttöön vaikuttavissa sääntelyvaatimuksissa (IEC 82304-1: 2016, 8.4); - Koordinoitu haavoittuvuusilmoitus (CVD), vastuullisuuspolitiikka ja aktiivinen sitoutuminen sidosryhmien ja vertaisten kanssa rikkomuksen sattuessa - ohjelmistokirjastojen ja muiden ohjelmistokomponenttien päivitysten seuranta ja niiden käytön suunnittelu; - haavoittuvuuksien seuranta liitännäispalveluissa, esim. hiljattain löydetyt haavoittuvuudet pilvipohjaisten todentamis- ja tallennuspalvelujen tarjoajilla.	Todisteet: Asianmukainen vakiokäytäntö, koordinoitu haavoittuvuusilmoitus (CVD) tai Vastuullinen paljastaminen, haavoittuvuusraportti

Kiitos! Kysymyksiä?