LUONNOS Hyvinvointisovellusten rajapintaa potilastietoihin koskevat toiminnalliset määrittelyt

Tämä dokumentti on keskeneräinen luonnos siitä, millaisia vaatimuksia Kanta-palveluista potilastietoja hakeville hyvinvointisovelluksille on suunniteltu. Vaatimukset julkaistaan keskeneräisinä Kanta PH FHIR -tukiprojektin jäsenille osana tiistain 24.9.2024 kokousta, jossa on käsitellään määrittelyihin tehtyjä muutoksia.

Määrittelyjen työstö on vielä kesken ja vaatimusten sisältö saattaa vielä muuttua. Lopulliset määrittelyt tullaan julkaisemaan myöhemmin.

LUONNOS Hyvinvointisovellusten rajapintaa potilastietoihin koskevat vaatimukset ja toiminnalliset määrittelyt

1. Yleistä

Hyvinvointisovellusten rajapinta potilastietoihin on valtakunnallisiin tietojärjestelmäpalveluihin (Kanta-palvelut) kuuluva toiminnallisuus, jonka avulla kansalainen voi saada Potilastietovarannossa olevat potilastietonsa katseltavaksi tai toimitettavaksi hyvinvointisovellukseen. Palvelusta käytetään myös nimitystä potilastietojen luovuttaminen hyvinvointisovelluksille.

1.1. Määrittelyn noudattaminen ja muut noudatettavat dokumentit

Tämä dokumentti toimii Hyvinvointisovellusten rajapinta potilastietoihin -palveluun liittyvien toiminnallisten vaatimusten kokoavana ja ensisijaisena määrityksenä hyvinvointisovellusten valmistajille. Määrittelyssä olevat vaatimukset perustuvat pääosin lakiin sosiaali- ja terveydenhuollon asiakastietojen käsittelystä (703/2023, asiakastietolaki). Dokumentti kohdistuu toiminnalliseen tasoon ja muut hyvinvointisovellustoimittajia koskevat määräykset ja määrittelyt on myös koostettu tähän dokumenttiin.

Hyvinvointisovelluksen tulee palvelua käyttöönotettaessa täyttää THL:n määräysten 4/2024 Määräys sosiaali- ja terveydenhuollon tietojärjestelmien ja hyvinvointisovellusten luokittelusta ja sertifioinnista ja 5/2024 Määräys sosiaali- ja terveydenhuollon tietojärjestelmien ja hyvinvointisovellusten olennaisista vaatimuksista mukaiset vaatimukset. Määräyksen 5/2024 liitteenä on profiili 3h4 Asiakastietoja käyttävä hyvinvointisovellus, jossa useat vaatimuksista tulevat perustumaan ja viittaamaan tähän määrittelydokumenttiin.

Asiakkaan antaman hyväksynnän osalta hyvinvointisovelluksen tulee noudattaa Kanta-palvelujen auktorisointiopasta hyvinvointisovelluksille (Kanta authorization guide for personal clients).

Tukimateriaalina on mahdollisuus hyödyntää myös Kanta.fi-sivustolle ja Potilastietovarannon määrittelyt -sivustolle koostettuja yleisiä Potilastietovarantoon liittyviä määrittelyjä sekä Potilastietovarantoon liittyvien palvelurajapintojen käyttötapauskuvauksia, joita on kuvattu Kelan julkaisemaan dokumenttiin Potilastiedon arkisto: rajapintakäyttötapaukset arkiston ja liittyvän järjestelmän välillä.

1.2. Keskeiset käsitteet

Auktorisointipalvelu on Kelan Kanta-palvelujen ylläpitämä palvelu, jolla ylläpidetään hyvinvointisovelluksiin liittyviä informointeja ja kansalaisen antamia käyttöoikeuksia. Auktorisointipalvelu on käytössä sekä Omatietovaranto- että Potilastietojen luovutus hyvinvointisovellukseen -palvelut käyttöönottaneille sovelluksille. Kansalaiselle näkyvä osa auktorisointipalvelusta on luvituskäyttöliittymä, jossa kansalainen voi tutustua palveluja koskeviin informointeihin ja antaa hyvinvointisovellukselle käyttöoikeudet hyvinvointisovelluksen käyttötarkoituksen mukaisiin tietoihin. Potilastietojen luovutukseen liittyvistä käyttöoikeuksista käytetään tässä määrittelyssä asiakastietolaissa käytettyä termiä hyväksyntä potilastietojen luovuttamisesta hyvinvointisovelluksille.

Hyvinvointisovellus tarkoittaa sovellusta, joka liittyy omatietovarantoon ja jolla käsitellään hyvinvointitietoa sekä sovellusta, johon kansalainen voi saada asiakastietonsa Kanta-palvelujen Potilastietovarannosta. Hyvinvointisovellus voi liittyä sosiaali- ja terveydenhuollon palvelunantajan toimintaan tai olla siitä riippumaton. Hyvinvointisovelluksessa (tai tietojärjestelmässä, jonka osajärjestelmänä hyvinvointisovellus on), on mahdollista olla myös muuta kuin Kanta-palvelujen kautta tapahtuvaa henkilötietojen käsittelyä ja rekisterinpitoa. Näiden tietojen rekisterinpidosta voi vastata hyvinvointisovelluksen valmistaja tai tämän asiakasorganisaatio kuten sote-palvelunantaja.

Digitaalinen asiointipalvelu on palvelunantajan tarjoama digitaalinen palvelu, joka mahdollistaa asiakkaan itsenäisen digitaalisen asioinnin. Se on asiakas- tai henkilötietojen käsittelyyn tarkoitettu tietojärjestelmä tai osajärjestelmä, jonka käyttäjinä voi olla myös ammattihenkilöitä. Digitaalinen asiointipalvelu voi täyttää esimerkiksi vaatimukset profiilista ”3h1 Palvelunantajan digitaalinen asiointipalvelu” (määräys 5/2024, liite 3h). Profiili kokoaa asiointipalvelun vaatimukset siltä osin, kuin palvelu täyttää asiakastietolain mukaisen määritelmän tietojärjestelmästä, jossa käsitellään asiakastietoja.
Tässä dokumentissa olevat toiminnalliset määrittelyt koskevat palvelunantajien tarjoamia digitaalisia palveluita silloin, kun ne täyttävät lain sosiaali- ja terveydenhuollon asiakastietojen käsittelystä (703/2023) ja THL:n määräyksen mukaisen hyvinvointisovelluksen määritelmän. Asiakkaille tarkoitettu digitaalinen palvelu voi olla sekä hyvinvointisovellus että tietojärjestelmä, tai myös osa laajempaa palvelunantajan käyttämää järjestelmää.

Hyvinvointisovelluksen käytön vastuutahona toimii se taho, joka vastaa hyvinvointisovelluksen toiminnasta ja hyvinvointisovelluksessa käsiteltävistä henkilötiedoista. Hyvinvointisovelluksen käytön vastuutahosta tulee sovelluksessa näytettävien ja muutoin käsiteltävien tietojen rekisterinpitäjä. Rekisterinpitäjä määrittelee sovelluksessa tapahtuvan käsittelyn tarkoitukset ja keinot. Rekisterinpitäjyyden määrittely tapahtuu tietosuoja-asetuksen mukaisesti tosiseikkoihin perustuvaan arvioon siitä, mikä taho määrittelee hyvinvointisovelluksessa tapahtuvan henkilötietojen käsittelyn tarkoitukset ja keinot. Kun potilastietoja näytetään hyvinvointisovelluksessa, rekisterinpitäjänä voi toimia esimerkiksi

hyvinvointisovelluksen valmistaja, sosiaali- ja terveydenhuollon palvelunantaja tai hyvinvointi- ja terveyspalveluita tarjoava toimija.

Hyväksyntä potilastietojen luovuttamisesta hyvinvointisovelluksille on asiakastietolain 74 § mukainen kansalaisen antama hyväksyntä tietojen luovuttamisesta. Hyväksyntä voi koskea kaikkia Potilastietovarantoon tallennettuja potilastietoja tai vain tiettyjä tietokokonaisuuksia. Hyvinvointisovellus pyytää lupaa vain niihin tietokokonaisuuksiin, joita se käyttötarkoituksensa mukaisesti hyödyntää. Hyväksyntä tietojen luovutuksesta tehdään hyvinvointisovelluksen kautta Kelan ylläpitämän auktorisointipalvelun luvituskäyttöliittymässä ja hyväksyntä tallennetaan Kanta-palvelujen tahdonilmaisupalveluun.

Potilastietojen luovuttamista hyvinvointisovelluksille koskeva informointi on OmaKannassa tai Kannan auktorisointipalvelussa kansalaiselle annettava tiedonanto potilastietojen luovuttamisesta hyvinvointisovelluksille. Informoinnilla pyritään selvittämään kansalaiselle toiminnallisuuden käyttöön liittyviä vastuita ja velvollisuuksia.

Suostumus tietojen hyödyntämiseen on hyvinvointisovelluksen käyttäjän antama EU:n yleisen tietosuoja-asetuksen (GDPR, 2016/679) mukainen suostumus, joka antaa hyvinvointisovelluksen rekisterinpitäjälle luvan käsitellä luovutettuja potilastietoja laajemmin kuin asiakastietolain 74 § 2 momentissa on säädetty. Hyvinvointisovelluksen vastuutaho vastaa tämän suostumuksen pyytämisestä ja se tallennetaan sen rekisterinpitoon.

Tahdonilmaisupalvelu on Kanta-palveluihin kuuluva tietojärjestelmäpalvelu, jonne tallennetaan tieto kansalaiselle annetusta Kanta-informoinnista sekä ylläpidetään hänen luovutuslupiaan, suostumuksiaan, kieltojaan ja muita tahdonilmaisujaan. Tahdonilmaisupalveluun tallennetaan tieto potilastietojen luovutukseen liittyvästä informoinnista sekä hyväksyntä potilastietojen luovutuksesta hyvinvointisovellukseen.
Lisää aiheeseen liittyvien termien määrittelyjä on luettavissa Sosiaali- ja terveydenhuollon digitaalisten palvelujen sanastosta.

1.3. Potilastietojen luovuttaminen ja palvelun käyttö

Potilastietovarannossa olevien potilastietojen näyttämisestä ja toimittamisesta hyvinvointisovelluksen välityksellä säädetään asiakastietolain 74 §:ssä. Hyvinvointisovelluksen tulee liittyä Kanta-palveluihin ja olla sertifioitu (kuuluu luokkaan A), jotta se voi tuotantokäytössä hakea Potilastietovarannon tietoja. Sertifiointi tapahtuu asiakastietolain ja THL:n määräysten 4/2024 ja 5/2024 mukaisesti. Hyvinvointisovellusten tulee täyttää saavutettavuusvaatimukset ja toiminnallisuutta koskevien vaatimusten

täyttymisen edellytyksenä on, että sovellus edistää kansalaisen terveyttä ja hyvinvointia (asiakastietolaki 84 §).

Saadakseen tiedot Potilastietovarannosta hyvinvointisovellukseen kansalaisen tulee ottaa hyvinvointisovellus käyttöön ja hyväksyä tietojen luovutus. Kanta-palvelut luovuttaa Potilastietovarannosta kansalaiselle hyvinvointisovellukseen ne tietokokonaisuudet, joihin kansalainen on antanut hyväksynnän. Sellaista tietoa ei luovuteta, jota julkisuuslain 11 §:n 2 momentin, tietosuojalain 34 §:n tai muun lainsäädännön mukaan kansalaisella ei ole oikeutta saada. Kansalaiselle ei luovuteta hyvinvointisovellukseen mitätöityjä tai viivästettyjä asiakirjoja, eikä riskitietoihin kirjattuja käyttäytymiseen liittyviä riskejä. Kansalaisen mahdollisesti asettamat kiellot Kanta-palveluissa potilastietojensa luovuttamiseen esimerkiksi toiselta hyvinvointialueelta toiselle tai julkisen ja yksityisen terveydenhuollon välillä eivät vaikuta tietojen luovuttamiseen kansalaiselle hyvinvointisovelluksen kautta. Hyvinvointisovellus voi hakea kerralla vain yhden henkilön potilastietoja.

Sovelluksen on pyydettävä kansalaiselta erillinen suostumus terveystietojen käsittelyyn, mikäli tietoja käsitellään laajemmin kuin asiakastietolain 74 § 2 momentissa on säädetty, ellei sovelluksessa tapahtuvalle käsittelylle ole muuta käsittelyperustetta. Pääsääntöisesti pelkkä tietojen näyttäminen tai toimittaminen kansalaiselle ei edellytä suostumusta. Muuta tietojen käsittelyä varten pyydetty suostumus tulee olla yksilöity ja suostumuksen antajan tulee yksiselitteisesti ymmärtää mihin käyttötarkoitukseen suostumuksen antaa. Tämä suostumus annetaan hyvinvointisovelluksessa ja se tallennetaan hyvinvointisovelluksen rekisterinpitäjän rekisteriin. Hyvinvointisovelluksen käyttäjille on annettava tieto siitä, mihin tarkoitukseen kutakin tietoa käytetään.

Hyväksyntä potilastietojen luovutuksesta ja suostumus luovutettujen potilastietojen käsittelyyn annetaan erikseen. Kela vastaa Kanta-palvelujen kautta tapahtuvien potilastietojen luovutusten lainmukaisuudesta, jonka takia hyväksyntä tallennetaan tahdonilmaisupalveluun. Muutoin Kelalla ei ole toimivaltaa sovelluksessa tapahtuvaan tietojen käsittelyyn eikä sovellusten tallentamien käsittelyyn oikeuttavien suostumusten keräämiseen. Hyvinvointisovelluksen käytön vastuutaho sen sijaan tekee arvion siitä, edellyttääkö sovelluksessa tapahtuva tietojen käsittely erillisen suostumuksen pyytämistä käyttäjältä tai onko sovelluksessa tapahtuvalle käsittelylle jokin muu tietosuoja-asetuksen mukainen käsittelyperuste.

Puolesta-asiointi potilastietojen luovuttamisessa hyvinvointisovellukseen on mahdollista syyskuussa 2025 ja siitä julkaistaan erilliset toiminnalliset määrittelyt.

1.4. Rajapinnan avulla hyvinvointisovellukselle luovutettavat tietokokonaisuudet

Rajapintapintapalvelu mahdollistaa potilastietojen luovuttamisen kansalaiselle itselleen silloin, kun kansalainen on antanut siihen hyväksynnän. Hyväksyntä tietojen luovutuksesta tehdään hyvinvointisovelluksen kautta Kannan auktorisointipalvelun luvituskäyttöliittymässä ja hyväksyntä tallennetaan tahdonilmaisupalveluun. Auktorisointipalvelun luvituskäyttöliittymässä kansalaiselta pyydetään hyväksyntää niiden tietokokonaisuuksien luovuttamiseen, joita hyvinvointisovelluksen on tarkoitus hyödyntää ja jotka ovat hyvinvointisovelluksen käyttötarkoituksen mukaisia. Sovelluksen käyttötarkoitus ja tietosisällöt, joita hyvinvointisovellus haluaa hyödyntää, tulee ilmoittaa Kelalle palvelua käyttöönotettaessa. Tieto ilmoitetaan järjestelmälomakkeella yhteistestaukseen ilmoittautumisen yhteydessä.

Rajapinnan avulla luovutettavia tietokokonaisuuksia ovat potilaskertomukset, diagnoosit, riskitiedot, toimenpiteet, fysiologiset mittaukset, rokotustiedot, laboratoriotutkimukset, kuvantamistutkimukset, ajanvaraustiedot, sekä terveys- ja hoitosuunnitelmat. Tietokokonaisuuksien sisällöt on kuvattu Simplifier.net -sivustolta löytyvään Implementointioppaaseen.

Kanta-auktorisointipalvelu vastaa hyvinvointisovelluksille kansalaisen hyväksynnällä annettujen käyttöoikeuksien hallinnoinnista. Auktorisoinnin toteutuksessa käytetään OAuth2.0 auktorisointiprotokollaa. Käytetyt auktorisointiprofiilit ja - mallit on kuvattu Kanta-auktorisointioppaassa hyvinvointisovelluksille.

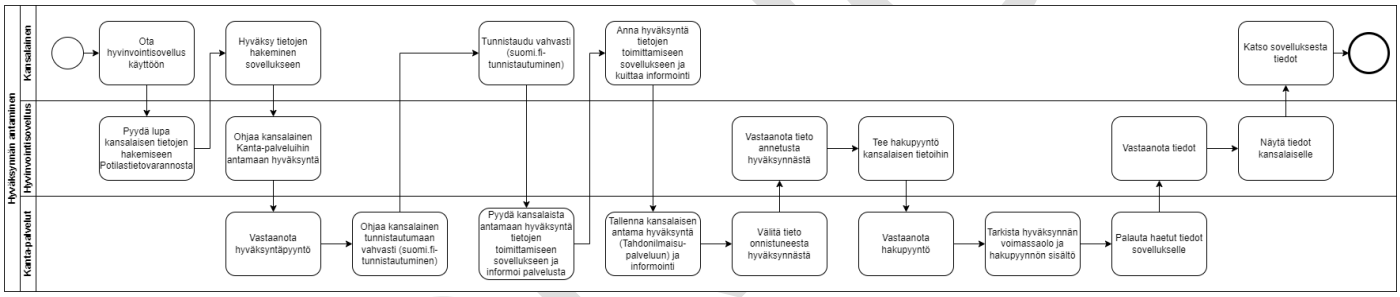
1.5. Hyvinvointisovelluksen käytön vastuutahon velvollisuudet ja lokitietojen kerääminen

Hyvinvointisovelluksen käytön vastuutahon tulee huomioida tietosuoja-asetuksesta tulevat rekisteripitäjän velvollisuudet Potilastietovarannosta luovutettujen tietojen käsittelyn suhteen. Näitä vastuita ovat muun ohella esimerkiksi rekisterinpitäjän osoitusvelvollisuus ja vastuut henkilötietojen turvaloukkauksista ilmoittamisesta.
Hyvinvointisovelluksen käytön vastuutahon tulee kerätä lokia hyvinvointisovelluksessa tapahtuvasta potilastietojen käsittelystä. Suositeltavaa on kerätä lokia myös Potilastietovarannosta tehdyistä hauista. Hyvinvointisovelluksessa on oltava lokien keräämistä varten tarvittavat ominaisuudet. Hyvinvointisovelluksen käytön vastuutahon tulee huomioida myös muut tietosuoja-asetuksesta tulevat rekisteripitäjän velvollisuudet Potilastietovarannosta luovutettujen tietojen käsittelyn suhteen.
Kanta-palvelut keräävät lokitietoja Kansalaiselle hyvinvointisovelluksen kautta luovutetuista tiedoista Kanta-palvelujen luovutuslokiin, ja kansalainen voi seurata näitä luovutuksia Omakanta-palvelusta.

2. Prosessikuvaus potilastietovarannon tietojen luovuttamisesta hyvinvointisovellukseen

Tämän luvun prosessikuvaus havainnollistaa, miten Potilastietovarannon tietojen luovuttaminen hyvinvointisovellukseen tapahtuu ja mitkä ovat eri toimijoiden (kansalainen, hyvinvointisovellus ja Kanta-palvelut) rooli prosessissa. Prosessissa kuvataan hyvinvointisovelluksen käyttöönotto, potilastietojen luovutusta koskevan hyväksynnän ja informoinnin käsittely sekä potilastietojen luovutus hyvinvointisovellukselle.

Prosessikuvaan ei ole kuvattu hyvinvointisovelluksen pyytämää suostumusta luovutettujen tietojen käsittelyyn. Hyvinvointisovelluksella on oltava voimassaoleva kansalaisen suostumus tai muu käsittelyperuste ennen luovutettujen tietojen käsittelyä.



Kuva 1: Hyvinvointisovelluksen käyttöönotto, Potilastietovarannon tietojen luovuttamisen hyväksyminen ja niiden luovuttaminen hyvinvointisovellukseen

3. Potilastietovarannon tietojen hakemista koskevat linjaukset ja vaatimukset hyvinvointisovelluksille

Tässä luvussa kuvataan hyvinvointisovelluksia koskevia linjauksia ja toiminnallisia vaatimuksia. Palvelun käyttöönotto lähtee liikkeelle siitä, että kansalainen ottaa sertifioidun hyvinvointisovelluksen käyttöönsä. Kansalaisen on tunnistauduttava hyvinvointisovellukseen vahvasti, jos sovelluksella pääsee hakemaan tai näkemään Kannasta luovutettuja potilastietoja. Vahvaa tunnistautumista tulee käyttää vähintään siinä tilanteessa, kun hän ottaa sovelluksen käyttöön ensimmäisen kerran. Kansalaisen tulee tutustua Potilastietovarannon tietojen luovutusta koskevaan informointiin ja antaa hyväksyntä tietojen luovutuksesta potilastietoja näyttävälle hyvinvointisovellukselle. Jos kansalainen ei hyväksy informointia tai tietojen luovutusta hyvinvointisovellukselle, kansalainen ei voi ottaa sovellusta käyttöön tai käyttää sitä.

Taulukko 1: Potilastietovarannon tietojen hakemista ja näyttämistä koskevat linjaukset

Linjauksen ID	Linjaus
PHKL 1	Hyvinvointisovelluksen ei tule hakea kansalaisen potilastietoja sen jälkeen, kun kansalainen on peruuttanut hyväksynnän tietojen luovuttamisesta OmaKannassa. Hyvinvointisovelluksella tulee olla kansalaisen suostumus tai muu käsittelyperuste, mikäli hyvinvointisovelluksen on tarkoitus näyttää, toimittaa tai käsitellä kansalaisen potilastietoja hyväksynnän poistamisen jälkeen.
PHLK 2	Hyvinvointisovelluksen valmistajalla on oltava käytäntö sovelluksen käytön lopettamiseen ja sovelluksessa olevien tietojen poistamiseen. Hyvinvointisovelluksen käytön lopettamisen yhteydessä kansalaisen sovellus ja tiedot on pystyttävä poistamaan turvallisesti.

Taulukko 2: Potilastietovarannon tietojen hakemista ja näyttämistä koskevat vaatimukset

Vaatimuksen ID	Vaatimus
PHKV 1	Asiakkaan tunnistautumisessa tulee käyttää vahvaa tunnistautumista vähintään hyvinvointisovelluksen käyttöönoton yhteydessä, jos kansalainen pääsee hakemaan tai näkemään Kanta-palveluista luovutettuja asiakastietoja. Omalla laitteella riittää, että vahva tunnistautuminen on tehty kerran ja myöhemmin voi käyttää esimerkiksi pin-koodia tai sormenjälkitunnistetta.

Vaatimuksen ID	Vaatimus
PHKV 2	Hyvinvointisovelluksen tulee ohjata kansalainen Kanta-palvelujen Auktorisointipalvelun luvituskäyttöliittymään, jossa kansalainen voi hyväksyä informoinnin sisällön ja potilastietojen luovutuksen. Luvitustuskäyttöliittymään ohjaaminen tehdään seuraavissa tilanteissa: • Kansalainen haluaa aloittaa palvelun käytön • Hyvinvointisovellukselle luovutettavien tietosisältöjen kokonaisuus on muuttunut • Kansalaisen antama hyväksyntä on vanhentunut • Potilastietojen luovutukseen liittyvän informoinnin sisältö on muuttunut
PHKV 3	Hyvinvointisovelluksen tulee kyetä hallitsemaan kansalaisen Auktorisointipalvelun luvituskäyttöliittymässä antamat hyväksynnät ja tilanteet, joissa kansalainen ei anna hyväksyntää. Hyvinvointisovellus voi käyttötarkoituksestaan riippuen pyytää samalla kertaa kansalaiselta käyttöoikeuksia Potilastietojen luovuttamisen lisäksi myös Omatietovarannon hyvinvointitietoihin. Hyvinvointisovelluksen tulee tässä tilanteessa huomioida, että kansalainen voi antaa käyttöoikeudet Potilastietovarannon tietoihin, Omatietovarannon hyvinvointitietoihin tai molempiin.
PHKV 4	Hyvinvointisovelluksen tulee hakea Potilastietovarannosta sovelluksen käyttötarkoituksen mukaiset tietosisällöt, joiden luovutukseen kansalainen on antanut hyväksynnän Auktorisointipalvelun luvituskäyttöliittymässä.
PHKV 5	Potilastietojen hakemisessa käytetään FHIR-rajapintaa ja hyvinvointisovelluksen tulee käyttää potilastietojen hakemisessa erikseen määriteltyjä hakuparametreja. Käytettävät hakuparametrit on kuvattu Simplifierissa julkaistuun implementointioppaaseen.
PHKV 6	Kanta-palvelut palauttaa hakutuloksen sivutettuna. Koko hakutuloksen saamiseksi hyvinvointisovelluksen tulee kyetä tekemään jatkohakuja, kunnes koko tulosjoukko on palautunut. Hakuihin liittyvät toiminnallisuudet on kuvattu Simplifierissa julkaistuun implementointioppaaseen.
PHKV 7	Hyvinvointisovelluksen käytön vastuutaho vastaa kaikista tiedon käsittelystä aiheutuvista rekisterinpitäjän velvoitteista ja sen tulee informoida kansalaista tietojen käsittelystä.
PHKV 8	Hyvinvointisovelluksen käytön vastuutahon tulee kerätä lokia hyvinvointisovelluksessa tapahtuvasta potilastietojen käsittelystä.

Vaatimuksen ID	Vaatimus
PHKV 9	Mikäli sovelluksessa tapahtuu muuta kuin asiakastietolain 74 § 2 momentissa tarkoitettua käsittelyä (Potilastietovarantoon tallennettujen tietojen näyttäminen tai toimittaminen), tulee hyvinvointisovelluksen pyytää tätä käsittelyä varten kansalaiselta suostumus.
PHKV 10	Hyvinvointisovellus voi säilyttää paikallisia kopioita, kun se täyttää seuraavat vaatimukset: • Mikäli tietojen näyttäminen tai asiakkaalle toimittaminen edellyttää tietojen säilyttämistä paikallisesti, tulee säilytysaika ja muut käsittelytoimet rajata vain välttämättömään mainittuun käyttötarkoitukseen nähden. • Hyvinvointisovelluksen tulee ilmoittaa kansalaiselle milloin tieto on haettu Potilastiedon arkistosta. • Mikäli hyvinvointisovelluksessa on toiminnallisuus, joka mahdollistaa tietojen välittämisen eteenpäin kolmansille osapuolille joko kansalaisen itsensä tai sovelluksen toimesta, tulee hyvinvointisovelluksen informoida tästä toiminnallisuudesta kansalaista. Tietojen edelleen välittäminen edellyttää kansalaiselta tietosuoja-asetuksen mukaista suostumusta tai muuta tiedon välittämiseen oikeuttavaa käsittelyperustetta. • Hyvinvointisovelluksen tulee mahdollistaa, että kansalainen voi poistaa paikallisesti tallennetut tiedot.
PHKV 11	Hyvinvointisovelluksen tulee ilmoittaa kansalaiselle virhetilanteista, kuten siitä, jos tietojen haku Kanta-palveluista ei onnistu. Kansalaiselle ei tarvitse näyttää virhekoodeja. Auktorisointipalvelin palauttaa sovellukselle virheviestin, jota sovellus pystyy halutessaan hyödyntämään. Jos potilastietojen haku Potilastiedon arkistosta epäonnistuu, sovellukselle palautetaan seuraavat virheviestit, jotka löytyvät THL:n kansallisesta Koodistopalvelimesta koodistosta "KanTa-palvelut - Prosessivirheet ja huomautukset" (HUOM. Lista on vielä keskeneräinen): 2T02001 Sisäinen tekninen virhe. 4Y00007 Virhe sanoman eheydessä. 5A00012 Hae asiakirjoja - Potilaan tiedot puuttuvat. 5A00054 Kyselyssä oli useita henkilötunnuksia.

Vaatimuksen ID	Vaatimus
	5Y00009 Käyttöoikeusvirhe.

Taulukko 3: Potilastietovarannon tietojen hakemista ja näyttämistä koskevat suositukset

Suosituksen ID	Suositus
PHKS 1	Suostumus tietojen käsittelyyn on suositeltavaa pyytää sovelluksen käyttöönoton yhteydessä, jos sovelluksessa käsitellään tietoja laajemmin kuin asiakastietolaki mahdollistaa.
PHKS 2	Hyvinvointisovelluksen vastuutahon on suositeltavaa kerätä lokia Potilastietovarannosta tehdyistä hauista.