Sosiaali- ja terveydenhuollon digitaalisten palveluiden perusvaatimukset

versio 0.5 kommentoitavaksi

Minna Linsamo, Eve Moilanen, Juha Mykkänen, Taina Kauvo, Niina Palm, Heli Geitlin

17.11.2025

Terveyden ja hyvinvoinnin laitos

Sisällys

Sosiaali- ja terveydenhuollon digitaalisten palveluiden perusvaatimukset 1
Versionhallinta 3
1 Johdanto 4
1.1 Rajaukset 4
1.2 Keskeiset käsitteet 5
2 Lähtökohdat ja lainsäädäntö 9
2.1 Lähtökohdat 9
2.2 Lainsäädäntö 10
3 Sosiaali- ja terveydenhuollon digitaalisten palveluiden yleiskuvaus 12
3.1 Digitaalisten palveluiden palvelukartta 12
3.2 Digitaalisten palveluiden roolit 13
3.3 Toimijat 14
4 Sosiaali- ja terveydenhuollon digitaalisten palveluiden linjaukset 15
5 Sosiaali- ja terveydenhuollon digitaalisten palveluiden vaatimukset 17
5.1 Vaatimusten sitovuus 17
5.2 Kansalaisen informoinnin vaatimukset 18
5.3 Asiakas- ja potilastietojen näyttäminen digitaalisessa palvelussa 19
5.4 Tunnistamisen vaatimukset 20
5.5 Puolesta-asioinnin vaatimukset 20
Taulukko 5.4 Puolesta asioinnin yleiset vaatimukset 20
Taulukko 5.5 Alaikäisen puolesta asioinnin vaatimukset 20
5.6 Digitaalisissa asiointipalveluissa käyttäjän tuottamien tietojen hallinnan vaatimukset 21
5.6.1 Koodistot kansalaisten käyttämissä ja tuottamissa tiedoissa 21
5.7 Tietoturvavaatimukset 22
5.8 Tietosuojavaatimukset 25
5.9 Lokivaatimukset 29
5.10 Saavutettavuusvaatimukset 29
5.11 Muut yleiset vaatimukset 30
Lähteet 31

Versionhallinta

Versio ja julkaisuajankohta	Muutokset
0.5 kommenttikierrosversio	Kommenttikierros

Tämä dokumentti on osin tehty Suomen kestävän kasvun ohjelman (RRP) projektissa ”Itse- ja omahoidon tuki Omatietovarannolla ja asiointipalveluilla”.

Euroopan unionin rahoittama –
NextGenerationEU

Suomen kestävän kasvun ohjelmalla tuetaan ekologisesti, sosiaalisesti ja taloudellisesti kestävää kasvua. THL on saanut rahoitusta Kestävän kasvun ohjelmaan EU:n kertaluonteisesta elpymisvälineestä (Next Generation EU).

Suomen kestävän kasvun ohjelma (RRP)

1 Johdanto

- 1.1 Rajaukset
- 1.2 Keskeiset käsitteet

Tässä dokumentissa kuvataan sosiaali- ja terveydenhuollon digitaalisten palveluiden perusvaatimukset. Dokumenttiin on koottu linjaukset ja keskeiset perusvaatimukset palvelunantajan digitaalisille asiointipalveluille sekä Potilastietoja Kanta-palvelusta käyttävä hyvinvointisovellukselle.

Dokumentin tarvetta taustoittavat useat tekijät. COVID-19 pandemian myötä sosiaali- ja terveydenhuollon digitaaliset palvelut lisääntyivät nopeasti. Uusia etäasiointikanavia ja -palveluita toteutettiin nopealla aikataululla Covid-19-epidemian aikana. Suomen kestävän kasvun ohjelmassa vuosille 2022–2025 yksi keskeinen tavoite on lisätä uusien digitaalisten ratkaisujen käyttöönottoa. Hyvinvointialueilla on käyttöönotettu paljon digitaalisia asiointipalveluita sekä digiklinikoita. Sosiaali- ja terveydenhuollon tiedonhallinnan ja digitalisaation strategia julkaistiin syksyllä 2023. Strategian yksi päätavoitteista on, että digitaalinen asiointi on ensisijaista kaikilla hyvinvointialueilla niissä palveluissa, joihin se sopii tai niille asiakkaille, jotka siihen kykenevät.

Digitaalisten palveluihin liittyvien linjausten ja ohjeistuksen tarve on tunnistettu puutteeksi, ja siksi perusvaatimusten määrittelyt on tarpeen tehdä. Taustamateriaalina on hyödynnetty Sote-ajanvaraus - yleiskuvaus ja terveydenhuollon ajanvarausratkaisujen kansalliset vaatimukset dokumenttia. Käsitemäärittely digitaalisten palveluiden osalta perustuu Sosiaali- ja terveydenhuollon digitaalisten palvelujen sanastoon.

Dokumentin vaatimusten asettamisessa on huomioitu THL:n, Kelan Kanta-palvelujen, STM:n, kansallisten tiedonhallinnan yhteistyöfoorumien (kuten Tiima-foorumi) sekä HL7 Finland Personal Health SIG-ryhmän esiin nostamia tarpeita ja vaatimuksia. Määrittelystä on järjestetty kommentointi- ja lausuntokierros 17.11-16.12.2025. Dokumenttiluonnosta tarkennetaan näistä kuulemisista saatujen kommenttien perusteella.

Dokumentti tukee sosiaali- ja terveydenhuollon asiakkaiden käyttöön suunniteltavien digitaalisten palvelujen kehittäjiä sekä hyvinvointialueita palveluiden hankintojen määrittelyssä.

Dokumenttia työstettäessä EHDS asetus astui voimaan ja sen toimeenpanon myötä tämä dokumentti tulee päivittymään.

Tämä dokumentti on tehty Suomen kestävän kasvun ohjelman (RRP) projektissa Itse- ja omahoidon tuki Omatietovaranolla ja asiointipalveluilla.

1.1 Rajaukset

Tässä dokumentissa keskitytään erityisesti kuvaamaan vaatimukset digitaalisten palvelujen valmistajien ja kansalaiskäyttäjän näkökulmasta. Seuraavat asiat eivät ole tämän dokumentin sisältöä, vaan ne sisältyvät muihin dokumentteihin:

- Dokumentissa ei ota kantaa sote-ammattilaisen toimintaa koskeviin vaatimuksiin. Nämä vaatimukset löytyvät THL:n määräys 5/2024 liitteissä.
- Tässä dokumentissa kuvataan puolesta-asioinnin vaatimukset digitaalisten palvelujen aihepiirissä, mutta puolesta asioinnin tarkempi yleiskuvaus on koottu Puolesta asioinnin yleiskuvaus sosiaali- ja terveydenhuollossa -dokumenttiin.

- Tämä dokumentti on rajattu suhteessa Opas digitaalisen sote-palvelujen kehittämiseen ettei kummassakaan dokumentissa toisteta samoja sisältöjä.
- Tämä dokumentti ei koske sähköisen ajanvarauksen määrittelyjä, jotka on kuvattu erillisessä dokumentissa.
- Tässä dokumentissa ei kuvata vaatimuksia apteekkien verkkopalveluille.

Potilastietoja hakevien hyvinvointisovellusten toiminnalliset määrittelyt on kuvattu Hyvinvointisovellusten rajapintaa potilastietoihin koskevat vaatimukset ja toiminnalliset määrittelyt -dokumentissa. Jatkossa määritykset tullaan tekemään myös reseptitietojen ja sosiaalihuollon asiakastietojen hakemiseen.

Tässä dokumentissa esitellyt puolesta asiointia koskevat linjaukset, vaatimukset ja (suositukset) koskevat vain puolesta asioinnin toiminnallisuudet käyttöön ottavia asiointipalveluja ja hyvinvointisovelluksia. Puolesta asioinnin mahdollistaminen asiointipalvelussa tai hyvinvointisovelluksessa on vapaaehtoista.

1.2 Keskeiset käsitteet

Digitaalisten asiointipalvelujen keskeiset käsitteet on koottu alle. Käsitteet noudattavat Sosiaali- ja terveydenhuollon tiedonhallinnan sanastoa, Sosiaali- ja terveydenhuollon digitaalisten palvelujen sanastoa, Asiakastietolain käsitteistöä (703/2023), THL:n määräys 4/2024 määrittelyjä, Puolesta-asioinnin yleiskuvauksen luvussa 2.2 määriteltyjä Puolesta asioinnin käsitteitä sekä Suomi.fi valtuuksien sanastoa.

Asiakkuus Sosiaalihuollon asiakkuus alkaa, kun henkilö on tehnyt hakemuksen tai muulla tavoin vireille tullutta asiaa aletaan käsitellä tai kun henkilö on aloittanut tietyn sosiaalipalvelun käyttämisen. Määritelmä tarkoittaa myös sellaisia asiakkuussuhteita, joissa asiakas omasta tahdostaan riippumatta tulee sosiaalihuollon piiriin. Sosiaalihuoltolain 34 §:ssä määritellään asiakkuuden alkaminen ja päättyminen. Yleisen neuvonnan ja ohjauksen antaminen ei synnytä lain 3 §:n 2 kohdan mukaista sosiaalihuollon asiakkuutta, joka tulisi kirjata asiakasasiakirjoihin. Esimerkiksi: Lapsesta tehty lastensuojeluilmoitus digitaalisen asiointipalvelun kautta. Kun lomake on lähetetty digitaalisesti sosiaalipalveluun ja vastaanotettu, niin asiakkuus katsotaan alkaneeksi.

Anonyymi asiointi Digitaaliset asiointipalvelut voivat olla tunnisteellisia tai anonyymeja. Anonyymia asiointia voi olla mm. anonyymi chat, anonyymit neuvontapalvelut. Anonyymi asiointi voi tarvittaessa muuttua tunnisteelliseksi asioinniksi eli tällä tarkoitetaan tilannetta, kun siirrytään yleisestä neuvonnasta tilanteeseen, jossa on tarpeen tunnistaa käyttäjä ja tarve tarkastella henkilön asiakas - tai potilastietoja ja tallentaa asiakaskirjoihin asiakkaan palvelun tai potilaan hoidon järjestämisestä.

Digitaalinen asiointi Asiointi käyttämällä digitaalista viestintäkanavaa tai alustaa.

Digitaalinen asiointipalvelu Palvelunantajan tarjoama digitaalinen palvelu, joka mahdollistaa asiakkaan itsenäisen digitaalisen asioinnin. Digitaalisessa asiointipalvelussa voi esimerkiksi hakeutua palveluihin, laittaa asian vireille tai antaa palautetta. Digitaalisia asiointipalveluja ovat muun muassa digitaaliset ajanvaraus- ja neuvontapalvelut, luovutuslupien, suostumusten, kieltojen ja tahdonilmaisujen tekeminen digitaalisesti sekä digitaalinen asiakasohjaus. OmaKanta, Omaolo, OmaKela ja Oma Vero ovat kansallisia tuotteistettuja digitaalisia asiointipalveluja. Myös eri hyvinvointialueilla on käytössä erilaisia digitaalisia asiointipalveluja.

Digitaalinen oirearvio Terveydenhuollon digitaalinen palvelu, jossa tiedot henkilön oireista tai mittaustuloksista syötetään palveluun, jolloin palvelu antaa tietojen perusteella automaattiseen päättelyyn perustuvan tuloksen ja mahdolliset ohjeet jatkotoimenpiteistä.

Digitaalinen palvelu, digipalvelu Digitaalisen viestintäkanavan tai alustan tuella toteutettu palvelu. (Sanasto). Termi kattaa sekä tietojärjestelmät että hyvinvointisovellukset, joissa on suoraan kansalaisen käytettäväksi tarkoitettuja ominaisuuksia. Digipalveluihin voi kuulua sekä digitaalisia asiointipalveluja että Kanta-palveluihin kuten omatietovarantoon liittyviä hyvinvointisovelluksia. On mahdollista myös, että yksi tietojärjestelmä tai digipalvelu täyttää sekä hyvinvointisovelluksen että tietojärjestelmän määritelmän asiakastietolaissa. (M4)

Digitaalinen hoito Hoito, jossa hyödynnetään erilaisia sosiaali- tai terveydenhuollon digitaalisia palveluja asiakkaan terveydentilan ja hyvinvoinnin arvioimiseksi, edistämiseksi ja ylläpitämiseksi asiakkaan ja sosiaali- tai terveydenhuollon työntekijän aktiivisessa vuorovaikutuksessa

Etäasiointi Reaaliaikainen digitaalinen asiointi siten, että vähintään yksi osapuoli on fyysisesti eri paikassa kuin muut.

Etäpalvelu Ihmisten väliseen vuorovaikutukseen perustuva reaaliaikainen digitaalinen palvelu, jossa vähintään yksi osapuoli on fyysisesti eri paikassa kuin muut.

Hyvinvointisovellus Kanta-palveluihin liitettävä sovellus, jolla kansalainen voi tallentaa tai käsitellä hyvinvointitietojaan tai johon kansalainen voi saada asiakastietonsa valtakunnallisesta asiakastietovarannosta, Reseptikeskuksesta tai Tiedonhallintapalvelusta. Sovellus, joka liittyy omatietovarantoon ja jolla käsitellään hyvinvointitietoa, sekä sovellusta, johon henkilö voi saada asiakastietonsa valtakunnallisesta asiakastietovarannosta, reseptikeskuksesta tai tiedonhallintapalvelusta. (AstL). Hyvinvointisovellus voi liittyä sosiaali- ja terveydenhuollon palvelunantajan toimintaan tai olla siitä riippumaton. ”Hyvinvointisovellus” termiä käytetään myös laajemmassa merkityksessä, joka on kuvattu sotesanastot palvelussa; määräykset 4/2024 ja 5/2024 nojautuvat kuitenkin asiakastietolaissa kuvattuihin määritelmiin ja rajauksiin. Ohjelmisto tai tietojärjestelmä voi olla käyttötarkoitukseltaan sekä asiakastietolain 3 §:n 19 kohdan määritelmän mukainen tietojärjestelmä että 18 kohdan mukainen hyvinvointisovellus. (M4)

Ilmoitus tai heräte on etenkin natiivisovelluksissa tarjolla oleva tapa kertoa reaaliaikaisesti käyttäjälle, jos sovellus on havainnut jonkin uuden käyttäjää koskevan tapahtuman tai tiedon. Ilmoitukset on usein mahdollista saada käyttäjälle näkyville myös silloin kun käyttäjällä ei ole kyseinen sovellus auki tai aktiivisessa käytössä. Ilmoitusasetuksia on yleensä mahdollista hallinnoida sekä laitekohtaisissa että sovelluksen omissa asetuksissa.

Käyttäjän istunto tarkoittaa sitä aikaa, jonka sovelluksen käyttäjä kansalainen on aktiivisena sovelluksessa. Istunnossa, jossa käytetään Kanta-tietoja, tulee kansalaisen olla vahvasti tunnistautuneena.

Istunto alkaa vahvalla tunnistautumisella, jolla käyttäjä kirjautuu sovellukseen sisään ja päättyy joko uloskirjautumiseen sovelluksesta tai sovelluksen tai laitteen sulkemiseen. Sovelluksessa istunto alkaa siitä, kun käyttäjä tunnistautuu vahvasti sovellukseen ja päättyy siihen, kun käyttäjä kirjautuu sovelluksesta ulos tai sulkee selaimen/sovelluksen. Hyvinvointisovellus saa näyttää käyttäjälle Kannasta haettuja asiakastietoja vain silloin kun kansalainen on vahvasti tunnistautuneena sovellukseen ja käyttäjän istunto on voimassa.

Jos sovelluksen on tarkoitus hakea käyttäjän tietoja Kanta-palveluista käyttäjän aktiivisen istunnon ulkopuolella, tulee tämän olla sovelluksen käyttötarkoituksen mukaan perusteltua. Sovelluksen tulee kertoa tästä Kanta-palveluille liittymisen yhteydessä ja se tulee myös kertoa käyttäjälle.

Käyttäjän tunnistaminen

> **Vahva sähköinen tunnistaminen** on henkilöllisyyden varmentamista sähköisesti. Vahvan sähköisen tunnistautumisen avulla käyttäjät voivat turvallisesti vahvistaa henkilöllisyytensä erilaisissa sähköisissä palveluissa ja sähköisten asiointipalveluiden tarjoajat voivat tunnistaa asiakkaansa.
>
> Vahvoja sähköisiä tunnistuspalveluita ovat:

- pankkien verkkopankkitunnukset
- teleyritysten mobiilivarmenteet
- Digi- ja väestötietoviraston kansalaisvarmenne poliisin myöntämällä henkilökortilla ja eräät muut tunnistusvarmenteet
- erilaisilla organisaatiokorteilla rekisteröidyt tunnistusvälityspalvelut

Vahva sähköinen tunnistus voi perustua teknisesti eri menetelmiin.

Yhteistä menetelmille on se, että niissä on käytettävä vähintään kahta seuraavista **todentamistekijöistä ja dynaamista todentamismekanismia**:

- tiedossa oloon perustuva todentamistekijä, jonka henkilön on osoitettava olevan tiedossaan (esim. salasana, PIN-koodi)
- hallussapitoon perustuva todentamistekijä, jonka henkilön on osoitettava olevan hallussaan (esim. tunnuslukulaite, mobiilisovellus, tunnuslukulista)
- luontainen todentamistekijä, joka perustuu johonkin luonnollisen henkilön fyysiseen ominaisuuteen (esim. sormenjälki, iiris)
- Dynaamisella todentamisella tarkoitetaan sähköistä prosessia,
- jossa käytetään salausta tai muita tekniikoita,
- joiden avulla voidaan pyynnöstä luoda sähköinen todiste siitä, että henkilöllä on hallinnassaan tai hallussaan tunnistetiedot, sekä
- muuttaa sitä jokaisessa uudessa henkilön ja hänen henkilöllisyytensä varmentavan järjestelmän välillä tapahtuvassa todentamisessa.

Lähteet: https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/sahkoinen-tunnistaminen

Monivaiheinen tunnistautuminen (Multi-factor authentication, MFA) tarkoittaa sitä, että henkilöllisyys varmistetaan kahta tai useampaa eri tunnistautumistapaa käyttämällä. Henkilön identiteetti varmistetaan useampaa eri tunnistautumistapaa käyttämällä. Kaksivaiheinen tunnistautuminen (Two-factor Authentication, 2FA) on yleisin monivaiheisen tunnistautumisen muoto.

Natiivi- tai mobiilisovellus on ohjelmisto, joka on suunniteltu toimimaan tietyssä käyttöjärjestelmässä tai laitteessa. Mobiilisovellukset on yleensä tehty tietyssä laitteessa käytettäväksi, kuten älypuhelimessa, tabletissa tai älykellossa ja ne asennetaan käyttäjän laitteelle. Natiivisovellusta käytetään henkilökohtaisessa käytössä olevalla laitteella. Esimerkiksi Android-laitteelle tehdyt sovellukset ovat ladattavissa Googlen sovelluskaupasta ja Applen iOS-käyttöjärjestelmää hyödyntäville laitteille tehdyt sovellukset ovat ladattavissa Applen sovelluskaupasta.

- Katso myös verkkosovelluksen määritelmä.

Puolesta-asiointi on toimintaa, jossa henkilö hoitaa toisen henkilön tai yrityksen puolesta tämän asioita. Henkilön puolesta-asiointi sosiaali- ja terveydenhuollossa perustuu huoltajuuteen, tiedonsaantioikeuteen, digitaaliseen valtuuteen tai edunvalvontaan.

Puolesta asioiva on luonnollinen henkilö, jolla on oikeus hoitaa asioita toisen henkilön puolesta.

Valtuus tarkoittaa oikeutta asioida toisen henkilön puolesta valitussa asiassa). Valtuus luodaan valtuutuksella. Suomi.fi-valtuuksissa annettu valtuus on digitaalinen valtakirja asioiden hoitamista varten.

Valtuutettu eli asiamies on luonnollinen henkilö, oikeushenkilö, yritys tai yhteisö, joka on saanut valtuuden asioida toisen henkilön, yrityksen tai yhteisön (valtuuttajan) puolesta (Suomi.fi, valtuuksien sanasto).

Valtuuttaja eli päämies on luonnollinen henkilö, oikeushenkilö, yritys tai yhteisö, joka antaa toiselle henkilölle, yritykselle tai yhteisölle valtuuden asioida puolestaan (Suomi.fi, valtuuksien sanasto).

Valtuuttaminen tarkoittaa menettelyä, jossa valtuuttaja valtuuttaa valtuutetun asioimaan puolestaan tietyssä asiassa.

Verkko- tai websovellus on ohjelmisto, jota käytetään verkkoselaimen kautta esimerkiksi älypuhelimella tai tietokoneella. Verkkosovelluksen käyttö edellyttää toimivaa internet-yhteyttä, mutta se ei ole riippuvainen tietystä laitteesta. Verkkosovellusta ei asenneta käytettävälle laitteelle.

- Katso myös mobiilisovelluksen määritelmä.

Rekisterinpitäjä, luonnollinen henkilö tai oikeushenkilö, viranomainen, virasto tai muu elin, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot; jos tällaisen käsittelyn tarkoitukset ja keinot määritellään unionin tai jäsenvaltioiden lainsäädännössä, rekisterinpitäjä tai tämän nimittämistä koskevat erityiset kriteerit voidaan vahvistaa unionin oikeuden tai jäsenvaltion lainsäädännön mukaisesti (GDPR artikla 4).

2 Lähtökohdat ja lainsäädäntö

- 2.1 Lähtökohdat
- 2.2 Lainsäädäntö

2.1 Lähtökohdat

Digitaalisten palveluiden nykytilaa ja on kuvattu useissa eri dokumenteissa. Strategiatasolla kokonaisuus kytkeytyy sosiaali- ja terveysministeriön kansallisiin strategioihin: Sote-tieto hyötykäyttöön (2014–2020) ja Digitaalisuus sosiaali- ja terveydenhuollon kivijalaksi. Molemmissa strategioissa keskiössä on kansalaisten aktiivisen roolin vahvistaminen ja palveluiden tarpeenmukaisuus. Niiden tavoitteena on, että kansalaiset käyttävät digitaalisia palveluita, kun se on suhteessa hoidon tarpeeseen sopivaa. Tällä tavalla digitaalisiin palveluihin ohjautuvat kevyemmillä palveluilla pärjäävät kansalaiset ja huolenpitoa tarvitsevien asiakkaiden hoitoon vapautuu enemmän palvelujärjestelmän resursseja (Steps 3.0). Digitaalisen asioinnin kokonaisuutta kuvataan lisäksi Digitaalisten sote-palveluiden kehittämisen oppaassa joka on suunnattu kaikille digitaalisten palveluiden kehittämiseen ja yhteistyöhön osallistuvien tahojen sekä digitaalisten palvelujen toteuttajien tueksi. Oppaassa tarkastellaan digitaalista asiointia laajasti kattaen mm. ajanvarauspalvelut, neuvontapalvelut, asiakas- ja palveluohjauksen palvelut sekä myös erilaiset etävastaanotot ja etätapaamiset osaan sosiaali- ja terveyspalveluja.

Tässä luvussa kuvatut lähtökohdat ovat pohja tarkennetuille konkreettisille vaatimuksille, joita kuvataan tämän dokumentin myöhemmissä luvuissa. Keskeisinä dokumentteina lähtökohtien kuvaukselle ovat olleet Sosiaali- ja terveydenhuollon tiedonhallinnan viitearkkitehtuuri, Sosiaali- ja terveydenhuollon valtakunnalliset tavoitteet vuosille 2023–2026 ja Digitaalisuus sosiaali- ja terveydenhuollon kivijalaksi strategia.

Sosiaali- ja terveydenhuollon digitaalisten palveluiden perusvaatimusten tavoitetilan ratkaisuihin liittyviä keskeisiä toiminnallisia ja laadullisia tavoitteita ovat:

- asiakkaille mahdollistetaan oman tilanteen laajempi ymmärtäminen ja parempien itseä koskevien päätösten tekeminen terveyttä ja hyvinvointia koskevia tietojen ja itseään koskevien asiakas- tai potilastietojen avulla, tarjotaan digitaalisten palveluiden hyötyjä
- kansalaisen asiointipalveluissa tuotettu tieto tarjotaan sote-ammattilaisen hyödynnettäväksi, vähennetään työtaakkaa kansalaiselta saatujen tietojen kirjaamisessa mahdollistamalla kansalaisen tuottaman tiedon saaminen suoraan palveluissa käytettäväksi tarjoten kattavamman kuva kansalaisen hyvinvoinnista ja terveydestä,
- määrittely on hyvinvointialueiden, tietojärjestelmätoimittajien ja hyvinvointisovellustoimittajien käytettävissä ja tukee näin digitaalisten palveluiden kehittämistä
- kehitettävien ja käyttöönotettavien palveluiden tulee olla tietoturvallisia ja huomioida tietosuoja

Sosiaali- ja terveydenhuollon linjauksissa on periaatteita, jotka linkittyvät myös digitaalisiin palveluihin. Linjaukset on tarkoitettu erityisesti sosiaali- ja terveydenhuollon palvelunjärjestäjille ja palveluntuottajille, kansallisille toimijoille ja tietojärjestelmä- toimittajille, mutta niissä on pyritty huomioimaan myös asiakkaan näkökulmaa. Linjauksissa on myös itse- ja omahoidon linjaukset, jotka sovellettavissa myös digitaalisiin palveluihin.

Taulukko 1. Itse- ja omahoidon linjaukset (Sosiaali- ja terveydenhuollon tiedonhallinnan viitearkkitehtuuri)

Itse- ja omahoidon linjaukset	
Henkilö voi ylläpitää omatoimisesti hyvinvointiaan, terveyttään ja toimintakykyään tietoon perustuen ennakoinnin ja digitaalisten palvelujen tuella.	Omatoimisuuden merkitys tulee kasvamaan tulevaisuudessa. Toimijoiden tulee kehittää tai käyttöönottaa ratkaisuja, joiden avulla henkilöt voivat ennakoida omaa tilannettaan ja hoitaa asioitaan mahdollisimman sujuvasti digitaalisten palvelujen avulla. Sekä julkiset että yksityiset palveluntuottajat voivat tukea omatoimisuutta älykkäiden digitaalisten palvelujen avulla.
Kansallisia ja alueellisia asiointipalveluita kehitetään siten, että ne muodostavat asiakkaalle yhteentoimivan kokonaisuuden.	Kansalliset ja alueelliset asiointipalvelut ja alueelliset itse- ja omahoidon ratkaisut pitää kehittää siten, että ne tukevat tarvittavaa integraatiota eivätkä kansalliset ratkaisut estä alueellisten ja paikallisten erityistarpeiden huomioimista ja innovointia. Asiointipalvelut muodostavat kansalaisen näkökulmasta yhteentoimivan kokonaisuuden, jotta siirtymät kansallisten, alueellisten ja yksityisten palveluiden välillä ovat sujuvia. Semanttisen yhteentoimivuuden tasolla tämä tarkoittaisi kansallisesti sovittujen tietorakenteiden, luokitusten ja terminologioiden käyttöä.
Henkilön omassa käytössä olevat terveys- ja hyvinvointisovellukset ovat tietoturvallisia ja helppokäyttöisiä.	Henkilön käytössä olevat terveys- ja hyvinvointisovellukset ovat saavutettavia, helppokäyttöisiä ja muokattavissa omiin tarpeisiin. Sovellusten tietosuoja ja -turva tulee varmistaa. Henkilön on helppo siirtää tietoa sovelluksista haluamiinsa käyttötarkoituksiin (esim. sosiaali- ja terveyspalvelujen käyttöön).
Henkilön osallistumista omaan hoitoonsa ja palveluunsa vahvistetaan yhteisillä toimintamalleilla ja käyttöönotetuilla ratkaisuilla.	Henkilön osallistamista ja sitoutumista omaan hoitoonsa ja palveluihinsa edistetään varmistamalla pääsy omiin tietoihin. Henkilön itsetuottamia tietoja voidaan hyödyntää henkilön palveluiden järjestämisessä ja tuottamisessa. Henkilöllä on oikeus jakaa tietojaan eri hyvinvointipalveluihin ja hän ymmärtää riittävästi tietojen jakamisen periaatteet.

2.2 Lainsäädäntö

Sosiaali- ja terveydenhuollon tiedonhallintaa ohjaava yleinen lainsäädäntö on kuvattu kattavasti julkaisussa Sosiaali- ja terveydenhuollon viitearkkitehtuuri luvussa 2.2. Itsehoidon, sähköisen asioinnin ja omahoidon kokonaisuutta säädellään edellä mainitun lisäksi muulla lainsäädännöllä, jota on tarkennettu alla keskeisimpien säädösten osalta ja tiedonhallinnan näkökulmasta. Keskeisimmät asiointi- ja omahoitopalveluihin vaikuttavat lainsäädännöt on kuvattu Yleisoppaassa digitaalisten sote-palvelujen kehittämiseen.

Keskeisimpiä digitaalista asiointia ohjaavia lakeja:

- EU:n yleinen tietosuoja-asetus (679/2016)
- Tietosuojalaki (1050/2018)
- Laki sähköisestä asioinnista viranomaistoiminnassa (13/2003)
- Laki digitaalisten palvelujen tarjoamisesta (saavutettavuuslaki) (306/2019)
- Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (asiakastietolaki) (703/2023)
- Sosiaali- ja terveysministeriön asetus sosiaali- ja terveydenhuollon asiakastietojen käsittelystä (457/2024)
- Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (617/2009)
- Laki lääkinnällisistä laitteista (719/2021)
- Laki sosiaali- ja terveystietojen toissijaisesta käytöstä (toisiolaki) (552/2019)
- Sosiaalihuoltolaki (1301/2014)
- Laki sosiaalihuollon asiakkaan asemasta ja oikeuksista (asiakaslaki) (812/2000)

- Terveydenhuoltolaki (1326/2010)
- Laki potilaan asemasta ja oikeuksista (potilaslaki) (785/1992)
- Laki julkisen hallinnon tiedonhallinnasta (tiedonhallintalaki) (906/2019)
- Asetus eurooppalaisesta terveystietoalueesta (2025/327)

Ajantasainen lainsäädäntö löytyy muun muassa Finlex-palvelusta. Palvelusta löytyvät muun muassa alkuperäiset säädökset, ajantasainen lainsäädäntö, hallituksen esitykset vuodesta 1992 lähtien, tuomioistuinten ratkaisut sekä tietosuojavaltuutetun päätöksiä lain tulkinnasta.

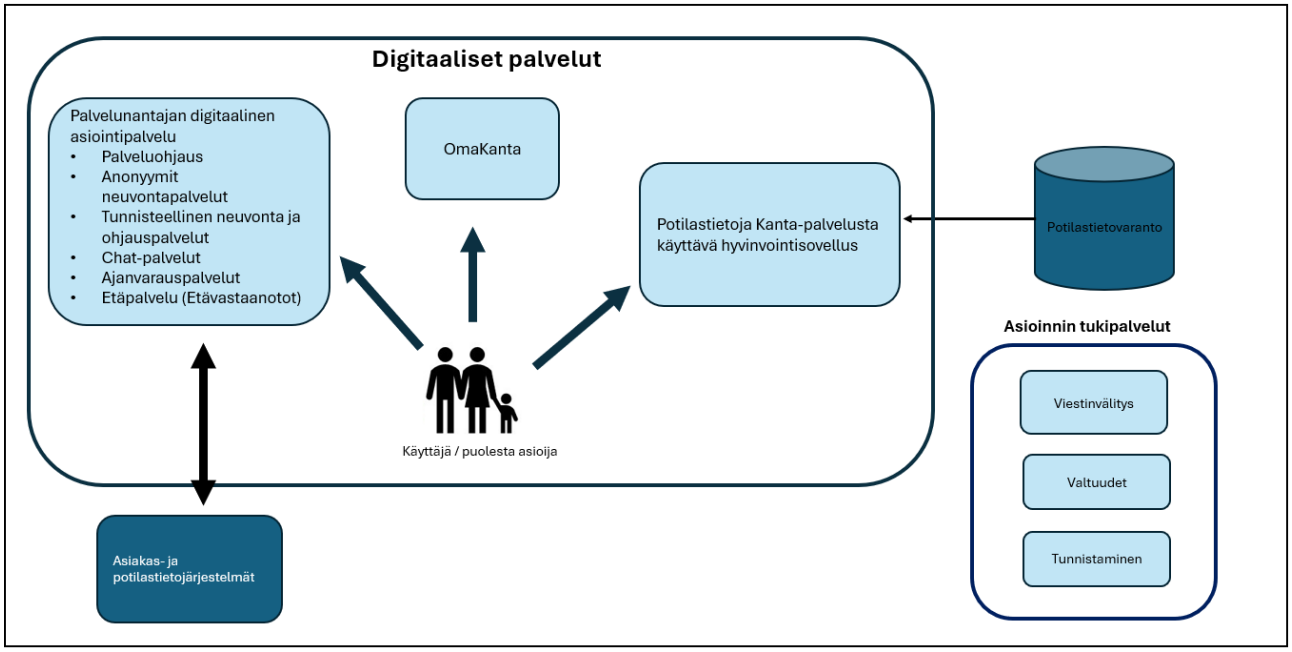
EU:n esteettömyysdirektiivi (2019/882) vaatii, että viranomaiset ja yksityinen sektori tekevät tietyt tuotteet ja palvelut esteettömiksi. Direktiivi tuli laittaa kansallisesti toimeen jokaisessa EU-maassa 28.6.2022 mennessä. Tämä tarkoittaa muutoksia myös Suomen lainsäädäntöön. Esteettömyysvaatimusten soveltaminen alkaa 28.6.2025. Tämän jälkeen markkinoille tulevien tuotteiden ja palvelujen tulee olla esteettömyysvaatimusten mukaisia. Direktiivi sallii kuitenkin muutamia siirtymäaikoja esimerkiksi hätäviestin, itsepalvelupäätteiden ja ennen 28.6.2025 solmittujen palvelusopimusten tai palvelujen tarjoamiseen tarkoitettujen tuotteiden osalta.

Euroopan unionin alueella yhdenmukaistetaan potilastietojen käsittelyä ja potilastietojärjestelmien vaatimuksia säätämällä eurooppalaisesta terveystietoalueesta (European Health Data Space, EHDS). Eurooppalainen terveystietoalueen (EHDS) säädöspohja vaikuttaa laaja-alaisesti erityisesti terveydenhuollon tiedonhallintaan. EHDS tuli voimaan maaliskuussa 2025. EHDS:n täytäntöönpanoa valmistellaan ja kansalliseen lainsäädäntöön on tulossa muutoksia mm. sosiaali- ja terveydenhuollon asiakastietojen käsittelystä annettuun lakiin (703/2023, asiakastietolaki). Eurooppalaisen terveystietoalueen avulla vastataan sähköisten terveystietojen saatavuuden ja jakamisen haasteisiin. Käsittelyn ja vaatimusten yhdenmukaistamisella on vaikutuksia potilastietojärjestelmien lisäksi myös kansalaisten ja ammattihenkilöiden oikeuksiin. Asetuksessa säädetään muun muassa potilastietojen vaihdosta EU:n jäsenvaltioiden välillä, potilaan oikeuksista omiin potilastietoihin ja terveydenhuollon ammattihenkilöiden oikeuksista ja velvollisuuksista potilastietojen käsittelyssä. Asetuksella edistetään sähköisten terveystietojen saatavuutta ensi- ja toissijaista käyttöä varten. Ensisijaisen käytön osalta EHDS vaikuttaa mm. potilaan oikeuksiin, kuten oikeus saada pääsy sähköisiin terveystietoihin sähköisten terveystietojen käyttöpalvelussa, lisätä tietoja sähköiseen potilaskertomukseensa, luovuttaa tai pyytää välittämään tiedot toiselle palveluntarjoajalle tai rajoittaa omiin tietoihin pääsyä. Merkittävä uudistus on artikla 5 luonnollisen henkilön oikeus lisätä tietoa sähköiseen potilaskertomukseen.

3 Sosiaali- ja terveydenhuollon digitaalisten palveluiden yleiskuvaus

- 3.1 Digitaalisten palveluiden palvelukartta
- 3.2 Digitaalisten palveluiden roolit
- 3.3 Toimijat

Tässä luvussa kuvataan digitaalisten palveluiden yleiskuvaus. Tavoitteena on tunnistaa ja kuvata palvelut.



Kuva 3.1 Yleiskuvaus digitaalisista palveluista. Jatkossa hyvinvointisovellukset voivat hakea tietoja myös Reseptikeskuksesta ja asiakastietovarannosta.

3.1 Digitaalisten palveluiden palvelukartta

Digitaalisten palveluiden kuvaukset on koottu alla olevaan taulukoihin Sosiaali- ja terveydenhuollon tiedonhallinnan viitearkkitehtuuria mukaillen (ks. Palvelukartta 3.1.2). Palvelukartan avulla on tarkoitus kuvata palvelut, joihin dokumentin vaatimukset kohdistuvat.

Taulukko 3.1 Digitaaliset palvelut ja niiden kuvaukset

Digitaaliset asiointipalvelut	Kuvaus
Palveluohjaus	Palveluohjaus tarkoittaa kahdenlaista palvelua. Yleinen palveluohjaus kattaa asiakkaalle annettavaa yleistä neuvontaa ja ohjausta, mikä ei edellytä tunnistautumista. Henkilökohtainen palveluohjaus kattaa asiakaskohtaisen palvelutarpeen arvioinnin ja sen perusteella tehtävää palveluohjausta. Yleistä neuvontaa ja ohjausta annetaan myös sosiaali- ja terveydenhuollon asiakkaalle osana julkista tehtävää. Se on yleisluontoista ja sitä voidaan tehdä kysymättä asiakkaalta henkilötietoja.
Anonyymit neuvontapalvelut	Neuvontapalvelussa henkilöt voivat hakea tietoja mm. sosiaali- ja terveydenhuollosta, terveyden ja hyvinvoinnin edistämisestä, saatavilla olevista palveluista, niihin saatavista tuista ja etuuksista. Tietoa voi hakea myös liittyen esim. tietoon terveellisestä syömisestä tai liikunnasta, eri sairauksista tai vaivoista ja niiden hoidosta sekä yksityisistä ja julkisen sektorin sosiaalihuollon ja terveydenhoidon palveluista. Anonyymi neuvontapalvelu voi hyödyntää myös vastaustietokantaa ja palvelun toteuttamista palvelubottina.
Tunnisteellinen neuvonta ja ohjauspalvelut	Neuvontapalvelussa henkilöt voivat hakea tietoja mm. sosiaali- ja terveydenhuollosta, terveyden ja hyvinvoinnin edistämisestä, saatavilla olevista palveluista, niihin saatavista tuista ja etuuksista. Tietoa voi hakea myös liittyen esim. tietoon terveellisestä syömisestä tai liikunnasta, eri sairauksista tai vaivoista ja niiden hoidosta sekä yksityisistä ja julkisen sektorin sosiaalihuollon ja terveydenhoidon palveluista. Neuvontapalvelua voidaan toteuttaa tunnisteellisena neuvonta- ja usein palveluohjauksen palveluna, jolloin henkilö asioi sote-ammattihenkilön kanssa.
Chat-palvelu	Chat-palvelut ovat osa neuvonnan ja ohjauksen palveluja. Niissä henkilö voi keskustella anonyymisti chat-robotin tai sosiaali- ja terveydenhuollon ammattihenkilön kanssa.
Ajanvarauspalvelut	Ajanvarauspalvelussa henkilö voi varata aikoja suoraan tai esimerkiksi oirearvioinnin tuloksen tai hänelle laaditun suunnitelman pohjalta tarvitsemiinsa palveluihin. Ajanvarauspalvelussa henkilö voi peruuttaa ja siirtää aikojaan.
Etävastaanotot	Etävastaanotto on tietylle aikavälille sovittu reaaliaikainen etäkontakti, jossa sosiaali- tai terveydenhuollon ammattihenkilö tai muu työntekijä käsittelee tietyn asiakkaan asiaa tai antaa tälle hoitoa tai palvelua. Etävastaanotto voi tapahtua esimerkiksi ääni- tai videoyhteyden tai chatin kautta.

Taulukko 3.2 Potilastietoja käyttävä hyvinvointisovellus

Digitaalinen palvelu	Kuvaus
Potilastietoja käyttävä hyvinvointisovellus	Kanta-palveluihin liittyvä hyvinvointisovellus, jolla kansalainen voi saada käyttöönsä potilastietovarannosta potilastietojaan.

Taulukko 3.3 Asioinnin tukipalvelut

Tukipalvelu	Kuvaus
Tunnistautuminen	Palvelut henkilöllisyyden todentaminen sähköisesti. Sähköisessä tunnistamisessa voidaan käyttää esimerkiksi käyttäjätunnuksia, salasanoja, varmenteita ja henkilön biometrisiä ominaisuuksia. Julkishallinnossa käytetään lähtökohtaisesti Suomi.fi-tunnistautumista.
Viestinvälitys	Palvelut turvalliseen viestinvälitykseen asiakkaan ja/tai sote-organisaatioiden tai -ammattihenkilöiden välillä.
Valtuudet	Palvelu toteuttaa sähköisen valtakirjan, jolla henkilö, yritys ja yhdistys voi valtuuttaa henkilön, yrityksen tai yhteisön hoitamaan asioita puolestaan. Lisäksi palvelu toteuttaa mm. huoltajuussuhteen tarkistuksen alaikäisen puolesta-asioinnissa.

3.2 Digitaalisten palveluiden roolit

Vaatimukset kohdistetaan ao. roolien mukaisesti. Vaatimus kohdistetaan ko. roolin mukaisesti. Mikäli vaatimus kohdistuu kaikkiin sovelluksiin, niin käytetään termiä "kaikki."

Taulukko 3.4 Digitaalisten palveluiden roolit ja niiden kuvaus

Rooli	Kuvaus
Potilastietoja Kanta-palvelusta käyttävä hyvinvointisovellus	Kanta-palveluihin liittyvä hyvinvointisovellus, jolla kansalainen voi saada käyttöönsä potilastietovarannosta potilastietojaan.

Rooli	Kuvaus
Palvelunantajan digitaalinen asiointipalvelu	Asiakastietojen käsittelyyn tarkoitetun tietojärjestelmän määritelmän täyttävä järjestelmä / digitaalinen asiointipalvelu, jolla tarjotaan digitaalista palvelua kansalaisille. Lisäksi järjestelmää käyttää suoraan tai siitä välitetään tietoja sote-palvelunantajalle ja/tai palvelunantajan palveluksessa oleville ammattihenkilöille (vaatimusten roolien kohdalla luvussa 5 käytetään termiä "asiointipalvelu").

3.3 Toimijat

Alla olevassa taulukossa on kuvattuna määrittelyn kannalta oleelliset toimijat.

Taulukko 3.5 Toimijat

Hyvinvointisovelluksen valmistaja	Itse- ja omahoitoon tai hyvinvoinnin ylläpitoon tarkoitettuja laitteita, sovelluksia ja tallennuspalveluja tuottavat, kehittävät ja ylläpitävät toimijat ja yritykset. Itsehoidossa henkilö ottaa näitä laitteita ja palveluja omaehtoisesti käyttöönsä, mutta ohjatussa omahoidossa laite tai sovellus voi olla myös palvelunantajan asiakkaalle käyttöön lainaama tai suosittelema laite tai sovellus, tai käyttöön annettu lääkinnällinen laite.
Asiakas- ja potilastietojärjestelmän toimittaja	Tahoa, joka tarjoaa tai toteuttaa palvelunantajalle tietojärjestelmän ja joka vastaa tietojärjestelmän valmistajana, valmistajan lukuun tai yhden tai useamman valmistajan puolesta tietojärjestelmälle asetetuista vaatimuksista (Asiakastietolaki 703/2023 3 §)
Sote-palvelunantaja	Asiakastietolain määritelmän mukaan *palvelunantajalla* tarkoitetaan sosiaali- ja terveyspalvelujen järjestäjää ja sosiaali- ja terveyspalveluntuottajaa. (asiakastietolaki 3 §:n 1 mom. 11 kohta)
Puolesta-asioija	Luonnollinen henkilö, jolla on oikeus hoitaa asioita toisen henkilön puolesta.
Palvelun käyttäjä	Digipalvelua käyttävä luonnollinen henkilö tai hänen puolestaan asioiva henkilö.

4 Sosiaali- ja terveydenhuollon digitaalisten palveluiden linjaukset

Tässä luvussa kuvataan digitaalisia palveluita koskevia linjauksia. Linjaukset, joita tässä esitetään ovat sitovia palveluita kehitettäessä ja käyttöönotettaessa.

Käyttäjän tunnistaminen digitaalisissa palvelussa

Vahva tunnistaminen

- Sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetun lain eli asiakastietolain (703/2023) 8 §:n 1momentin mukaan asiakas on asiakastietojen sähköisessä käsittelyssä tunnistettava luotettavasti.
- Jos viranomaisen digitaalisesta palvelusta on mahdollista saada salassa pidettäviä tietosisältöjä nähtäväksi ja käytettäväksi, palvelun käyttäjä on tunnistettava vahvaa sähköistä tunnistamista tai painavasta perustellusta syystä muuta vastaavaa tietoturvallista tunnistuspalvelua käyttämällä (laki digitaalisten palvelujen tarjoamisesta (306/2019, digipalvelulaki) 6 § 2 momentti).
    - Digitaalisissa palveluissa asiakastietojen käsittelyssä käyttäjä ja puolesta asioija tulee tunnistaa vahvalla sähköisellä tunnistuspalvelulla.
        - Vahvoja sähköisiä tunnistuspalveluita ovat
            - pankkien verkkopankkitunnukset
            - teleyritysten mobiilivarmenteet
            - Digi- ja väestötietoviraston kansalaisvarmenne poliisin myöntämällä henkilökortilla ja eräät muut tunnistusvarmenteet
            - (erilaisilla organisaatiokorteilla rekisteröidyt tunnistusvälityspalvelut
- Testien / lomakkeiden tallentaminen / lähettäminen / välittäminen ammattilaiselle edellyttää vahvaa tunnistautumista. Huomioitava, että viranomainen voi vaatia digitaalisessa palvelussa käyttäjältä sähköistä tunnistamista vain, jos se on tarpeen palvelun tai sen tietosisältöön liittyvien käyttöoikeuksien varmistamiseksi tai palvelussa tehtävään toimeen liittyvien oikeusvaikutusten vuoksi (digipalvelulaki 6 § 1 mom).

Ei tunnistamista

- Voidaan käyttää, kun ei käsitellä henkilötietoja, asiakas- tai potilastietoja.
    - Esim. anonyymi chat.
    - Käyttäjän suostumuksella tai luvalla käyttäjälle voidaan lähettää tekstiviestitse tai muuta viestikanavaa käyttäen viestejä. Viestissä ei saa paljastua erityisiin henkilötietoryhmiin kuuluvia tietoja eikä henkilötunnusta (yleisen tietosuoja-asetus 9 artikla (Apulaistietosuojavaltuutetun päätös TSV/29/2020).

Puolesta-asiointi

- Sosiaali- ja terveydenhuollon digitaalisen puolesta-asioinnin toteutuksissa tulee noudattaa linjauksia ja ohjeistuksia, jotka on kuvattu Puolesta-asioinnin yleiskuvauksessa ja Kanta-palvelujen käsikirjassa sosiaalihuollon toimijoille (luku 5). Yksityiskohtaiset vaatimukset tietojen näyttämisestä digitaalisissa palveluissa on kuvattu tässä dokumentissa luvussa 5.3. ja puolesta-asioinnin vaatimukset luvussa 5.5.
- Puolesta-asiointi on mahdollista seuraavin tavoin:
    - Täysi-ikäinen valtuuttaa toisen henkilön asioimaan puolestaan Suomi.fi-valtuuksissa.
    - Asiointi alaikäisen puolesta perustuu huoltajuuteen. Huoltajuuden perusteella puolesta-asiointiin oikeutetut ja asiointiin liittyvät tarkistukset Suomi.fi-valtuuksissa on kuvattu Puolesta-asioinnin yleiskuvauksen luvussa 3
    - Asiointi alaikäisen puolesta voi perustua myös tiedonsaantioikeuteen, kun tiedonsaantioikeus on määritelty huollonjakosopimuksessa tai -määräyksessä. Tällöin henkilölle on erikseen sovittu tai määrätty tiedonsaantioikeus alaikäisen henkilön sosiaalihuollon ja/tai terveydenhuollon tietoihin, ja tieto on kirjattu lapsen huollosta tehtyyn sopimukseen tai päätökseen. Tiedonsaantioikeus on myös huoltajalla, jonka päätösoikeuksia huollettavansa sosiaalihuollon tai terveydenhuollon asioihin on rajoitettu.
- Hyvinvointialueen ja hyvinvointiyhtymän viranomaiset ovat velvollisia käyttämään asiointivaltuuspalvelusta saatavaa tietoa puolesta-asioinnin valtuuksien tarkastamisessa DVV:n Suomi.fi-valtuuksia mikäli palvelun tarjoaa hyvinvointialue tai hyvinvointiyhtymän viranomaiset tai kunnallinen viranomainen niiden hoitaessa laissa niille säädettyjä tehtäviä ellei 5 § 1 momentissa mainituista syistä ole välttämätöntä syytä käyttää muuta palvelua. (Laki hallinnon yhteisistä sähköisen asioinnin tukipalveluista (571/2016) § 5).
- Yksityiset sosiaali- ja terveydenhuollon palvelunantajat *voivat* viranomaisten lisäksi hyödyntää digitaalisissa palveluissaan Suomi.fi-valtuuksia. Digipalvelun tarjoajan tulee varmistaa, että puolesta-asioijalla on oikeus asioida henkilön puolesta (asiakastietolaki 8 §). Suositellaan, että puolesta asioinnin oikeutuksessa tulisi käyttää Suomi.fi-valtuuksia.
- Valtuuttajalla tulee olla oikeus kohdentaa puolesta-asioinnin valtuutus:
    - vain terveydenhuollon asioihin tai
    - vain sosiaalihuollon asioihin
    - tai molempiin. Terveydenhuollon ja sosiaalihuollon valtuusasiat on kuvattu tarkemmin Puolesta-asioinnin yleiskuvauksen luvussa 4.

Asiakastietojen näyttäminen digitaalisissa palveluissa

- Digitaalisissa palveluissa noudatetaan samaa käytäntöä potilas- ja asiakastietojen näyttämisen rajoituksista kuin OmaKannassa. Yksityiskohtaiset vaatimukset tietojen näyttämisen rajoituksista on kuvattu tässä dokumentissa luvussa 5.3.
- Sosiaalihuollon osalta yleiset ja tilannekohtaiset rajoitukset asiakastietojen näyttämisessä on kuvattu dokumentin Kanta-palvelujen käsikirja sosiaalihuollon toimijoille luvussa 5.
    - Poikkeuksena linjaukset asiakaskertomusmerkintöjen näyttämisestä OmaKannassa, jotka ovat vielä ratkaisematta. Asiointipalvelukohtaisesti voidaan ratkaista näytetäänkö asiointipalvelussa asiakaskertomusmerkintöjä ennen kuin niitä näytetään OmaKannassa.
- Terveydenhuollon osalta potilastietojen näyttämisen rajoitukset OmaKannassa on kuvattu tarkemmin Potilastietovarannon toimintamallien luvussa 8. Reseptikeskukseen tallennettujen lääkemääräysten näyttämisen rajauksista OmaKannassa on kuvaus Sähköisen lääkemääräyksen toimintamallien luvussa 7.

5 Sosiaali- ja terveydenhuollon digitaalisten palveluiden vaatimukset

- 5.1 Vaatimusten sitovuus
- 5.2 Kansalaisen informoinnin vaatimukset
- 5.3 Asiakas- ja potilastietojen näyttäminen digitaalisessa palvelussa
- 5.4 Tunnistamisen vaatimukset
- 5.5 Puolesta-asioinnin vaatimukset
    - Taulukko 5.4 Puolesta asioinnin yleiset vaatimukset
    - Taulukko 5.5 Alaikäisen puolesta asioinnin vaatimukset
- 5.6 Digitaalisissa asiointipalveluissa käyttäjän tuottamien tietojen hallinnan vaatimukset
    - 5.6.1 Koodistot kansalaisten käyttämissä ja tuottamissa tiedoissa
- 5.7 Tietoturvavaatimukset
- 5.8 Tietosuojavaatimukset
- 5.9 Lokivaatimukset
- 5.10 Saavutettavuusvaatimukset
- 5.11 Muut yleiset vaatimukset

5.1 Vaatimusten sitovuus

Tämän dokumentin vaatimukset kohdistuvat luvun 3.2 rooleihin ja yksilöidyissä vaatimuksissa käytetään seuraavia ilmaisuja pakollisuuksiin:

- "tulee tehdä", "on tehtävä" tai preesens "tekee": vaatimus on pakollinen toteutettava kyseisen roolin / loogisen tietojärjestelmäpalvelun toteuttavassa tietojärjestelmässä
- "tulisi tehdä" (konditionaali): vaatimus on vahvasti suositeltava toteutettavaksi kyseisen roolin / loogisen tietojärjestelmäpalvelun toteuttavassa tietojärjestelmässä, mutta siitä on mahdollista poiketa perustellusta syystä; on mahdollista, että kaikissa tai tarkemmin määritellyissä tilanteissa vaatimus muuttuu jatkossa pakolliseksi
- "voi tehdä": vaatimus on vapaaehtoinen, mutta useissa tilanteissa tarpeellinen ja suositeltava toteutettavaksi kyseisen roolin / loogisen tietojärjestelmäpalvelun toteuttavassa tietojärjestelmässä.

5.2 Kansalaisen informoinnin vaatimukset

Taulukko 5.1 Kansalaisen informoinnin vaatimukset

Vaatimuksen ID	Vaatimus	Rooli
TO01	Digitaalisen palvelun käyttötarkoitus tai käyttötarkoitukset tulee kuvata tiiviisti. Kuvauksessa tulee pyrkiä siihen, että käyttötarkoitus on kuvattu selkeästi ja käyttäjän ymmärtämässä muodossa. Digitaalisen palvelun käyttötarkoitus tulee kuvata tiiviisti, selkeästi ja käyttäjien ymmärtämässä muodossa. Asiakastietolain (703/2023) 3 §:n määritelmän mukaisten hyvinvointisovellusten tulee täyttää terveyden ja hyvinvoinnin edistämisen käyttötarkoitus.	Kaikki
TO02	Käyttäjälle tulee kertoa, onko digitaalinen palvelu tarkoitettu sairauden hoitoon tai diagnosointiin vaiko ei. Käyttäjälle tulee kertoa, jos digitaalinen palvelu on tarkoitettu sairauden hoitoon tai diagnosointiin. Lääkinnällisistä laitteista on mainittava, että kyseessä on lääkinnällinen laite, jolla on CE-MDR-merkintä.	Kaikki
TO03	Digitaalisen palvelun tulee informoida käyttäjää siitä, mitä tietoja se kerää ja mitä tarkoitusta varten. Digitaalisen palvelussa tulee kertoa myös datan mahdollisista kaupallisista käyttökohteista. Jos tietoja tallennetaan sovelluksen omaan tietovarantoon, myös näiden tietojen käyttötarkoitus on kerrottava.	Kaikki
TO04	Digitaalisen palvelun on kuvattava käyttäjälle, minne hänen tuottamiaan tietoja tallennetaan ja kuka toimii rekisterinpitäjänä.	Kaikki
TO05	Digitaalisen palvelun käyttöehdot on kuvattava tiiviisti ja ymmärrettävästi.	Kaikki
T006	Käyttäjälle tulee kuvata mistä lähteistä hänelle näytettävät itseensä liittyvät asiakastiedot tulevat. • Lisätietoa: Asiointipalvelu voi sisältää asiakastietoja palvelunantajan rekistereistä ja potilastietoja käyttävä hyvinvointisovellus voi sisältää potilastietovarannosta sikäli kuin kansalainen on antanut luvan tällaisten tietojen viemiseen sovellukseen.	Kaikki
TO07	Käyttäjälle tulee tarjota digitaalisen palvelun käyttöohjeet, joiden tarkoitus on tiedottaa käyttäjää riittävästi palvelun käytöstä.	Kaikki
TO08	Viranomaisen tarjoaman digitaalisen asiointipalvelun tulee julkaista palvelussa tai palveluun liittyvällä verkkosivustolla yhteistieto, josta käyttäjällä on mahdollisuus saada neuvoja digitaalisen asiointipalvelun käyttämiseksi (laki digitaalisten palveluiden tarjoamisesta 5§).	Asiointipalvelu
TO09	On kuvattava millaista tukea digitaalisen palvelun valmistaja tai digipalvelu tarjoaa käyttäjälle. Tukipalvelujen tarjoaminen on suositeltavaa, mutta ei ole pakollista, ks. myös vaatimus TO8.	Kaikki
TO10	Digitaalisen asiointipalvelun käyttäjälle on ilmaistava selkeästi, että digipalvelussa ei voi laatia ja lähettää palvelunantajalle lastensuojeluilmoitusta tai ilmoitusta sosiaalihuollon tarpeesta (huoli-ilmoitusta) anonyymisti, jos käyttäjä on tunnistautunut vahvasti digipalveluun.	Asiointipalvelu

5.3 Asiakas- ja potilastietojen näyttäminen digitaalisessa palvelussa

Taulukko 5.2 Asiakas- ja potilastietojen näyttäminen digitaalisessa palvelussa vaatimukset

Vaatimuksen ID	Vaatimus	Rooli
RE01	Digitaalisen palvelun rekisterinpitäjän on määriteltävä henkilötietojen säilytysaika. Henkilötietoja saa säilyttää vain niin kauan, kuin ne ovat tarpeen henkilötietojen käyttötarkoituksen kannalta. Rekisterinpitäjän on esimerkiksi arvioitava ja pystyttävä perustelemaan, kuinka kauan tietojen säilyttäminen on tarpeen sen jälkeen, kun käyttäjä ei enää käytä palvelua. • Sosiaalihuollon asiakasasiakirjojen säilytyksessä tulee noudattaa asiakastietolaki 703/2023 23§, • Potilasasiakastietojen säilytyksessä tulee noudattaa asiakastietolaki 703/2023 23§ • Hyvinvointisovelluksen rekisterinpitäjä on kuvattava käyttäjälle tietojen säilytysaika. ○ Lisätietoja: Rekisterinpitäjän on suunniteltava ja pystyttävä perustelemaan henkilötietojen säilytysaika. Henkilötietojen säilytysajat on myös dokumentoitava. Tietosuoja-asetuksessa ei ole määritelty tarkkoja henkilötietojen säilytysaikoja. Rekisterinpitäjän on arvioitava henkilötietojen säilytysaikaa ja tarpeellisuutta kysymyksessä olevaa käyttötarkoitusta vasten. Henkilötietoja saa säilyttää vain niin kauan, kun ne ovat tarpeen henkilötietojen käyttötarkoituksen kannalta. Rekisterinpitäjän on esimerkiksi arvioitava ja pystyttävä perustelemaan, kuinka kauan asiakastietojen säilyttäminen on tarpeen sen jälkeen, kun asiakassuhde on päättynyt. Säilytysaikaan voi vaikuttaa esimerkiksi asiakkaan reklamaatiomahdollisuus. Rekisterinpitäjän on itse huomioitava laista tulevat säilytysajat (https://tietosuoja.fi/sailytyksen-rajoittaminen).	Kaikki
RE02	Palvelunantajalle Kanta-palvelusta luovutuksella haettuja asiakastietoja ei saa näyttää digitaalisissa asiointipalvelussa käyttäjälle eikä hänen puolestaan asioivalle henkilölle.	Asiointipalvelu
RE03	Asiakas- ja potilastietoja ei näytetä digitaalisessa palvelussa käyttäjälle itselleen eikä hänen puolestaan asioivalle henkilölle, jos asiakirja tai tutkimuspyyntö tai -lausunto on viivästetty tai se on merkitty erityissisältöiseksi asiakasasiakirjaksi sosiaali- ja terveydenhuollon ammattilaisen toimesta. Sosiaalihuollon asiakastietojen näyttämisessä toimitaan kuten Kanta-palvelujen käsikirjan luvuissa 5.3.1 ja 5.3.2 on kuvattu.	Kaikki
RE06	Digitaalisissa palveluissa ei näytetä seuraavia potilastietoja: • Jos riskitiedon tyyppi on käyttäytymiseen liittyvä kriittinen riskitieto tai hoidossa huomioitavat riskitiedot, niin tietoja ei tule näyttää kansalaiselle eikä puolesta asioijalle. • Jos asiakirja on ERAS, niin sen sisältöä ei näytetä kansalaiselle eikä puolesta asioijalle. Lisätieto: Potilasasiakirjat, jotka sisältävät tietoja toisesta osapuolesta (esim. toisesta vanhemmasta) on erikseen merkitty asiakirjan kuvailutietoihin (erillisasiakirja ERAS). • Jos asiakirja on VLÄÄ, niin sen sisältöä ei näytetä alaikäisen puolesta asioijalle. • Jos asiakirja on LÄÄ, niin asiakirjaa ei näytetä digipalvelussa käyttäjälle eikä puolesta asioijalle. • Jos asiakirja on osastohoitojaksolla kirjattu Päivittäismerkintä -otsikon alle, niin tietoja ei näytetä käyttäjälle eikä puolesta asioijalle.	Kaikki
RE07	Digitaalisissa palveluissa ei näytetä seuraavia sosiaalihuollon asiakastietoja: • Asiakirjat, joita ei näytetä OmaKannassa. Pysyvästi OmaKannasta rajattavat asiakirjat on kuvattu Kanta-palvelujen käsikirjassa luvussa 5.2.2. • Asiakirjat, joiden näyttämistä on viivästetty OmaKannassa • Asiakirjat, jotka on merkitty erityissisältöisiksi • Huoltajille ja muille tiedonsaantiin oikeutetuille henkilöille ei näytetä niitä asiakirjoja, joihin on kirjattu näitä henkilöitä koskeva luovutuskielto (ks. APA05)	Kaikki
RE08	Digitaalisen palvelun tulee kuvata minne käyttäjän tietoja luovutetaan ja mihin tietoja käytetään.	Kaikki
RE09	Digitaalisissa asiointipalveluissa tulee näyttää asiakastiedot viivytyksettä, kun asiakirja on valmistunut.	Asiointipalvelu
RE10	Jos digitaalisessa asiointipalvelussa käytetään eri rekistereitä (esim. terveydenhuolto, sosiaalihuollon asiakas- ja ilmoitusrekisteri, työterveyshuolto), tulee eri palveluissa syntyvät rekisterit voida erotella toisistaan.	Asiointipalvelu

5.4 Tunnistamisen vaatimukset

Taulukko tunnistautumisen vaatimukset käyttäjälle ja puolesta asioijalle

5.3 Tunnistautumisen vaatimukset

Vaatimuksen ID	Vaatimus	Rooli
TU01	Käyttäjän tai puolesta asioijan tunnistamisessa tulee käyttää palvelussa vahvaa tunnistamismenetelmää, mikäli käyttäjä tai puolesta asioija pääsee katselemaan tai muokkaamaan asiakastietoja tai viestimään ammattilaisen kanssa.	Kaikki
TU02	Digitaalisessa palvelussa, joka on verkkosovellus, tulee käyttäjän tai puolesta asioijan tulee kirjautua verkkosovellukseen vahvalla sähköisellä tunnistautumisella joka kerta, ennen kuin sovelluksella pääsee näkemään Kannasta luovutettuja potilastietoja. Käyttäjän tulee olla tunnistautuneena hyvinvointisovellukseen koko istunnon ajan. Kannasta ei saa näyttää kansalaisen tietoa silloin kun käyttäjä ei ole tunnistautuneena hyvinvointisovellukseen.	Kaikki
TU03	Digitaalisessa palvelussa, joka on mobiilisovellus, tulee vahvaa sähköistä tunnistautumista käyttää vähintään siinä tilanteessa, kun käyttäjä tai puolesta asioija ottaa sovelluksen käyttöön. Käyttäjän henkilökohtaisessa käytössä olevalla laitteella, esimerkiksi älypuhelimella, voidaan ensimmäisen vahvan tunnistautumisen jälkeen käyttää esimerkiksi pin-koodia tai biometristä tunnistetta. Tunnistautuminen on laitekohtainen.	Kaikki

5.5 Puolesta-asioinnin vaatimukset

Taulukko 5.4 Puolesta asioinnin yleiset vaatimukset

Vaatimuksen ID	Vaatimus	Rooli
PU01	Jos puolesta-asiointi on mahdollista digipalvelussa, niin palvelussa täytyy olla toiminnallisuus, jolla käyttäjä valitsee, että haluaa asioida toisen henkilön puolesta. Palvelussa tulee olla selkeästi eroteltuna puolesta-asiointi ja oma asiointi.	Kaikki
PU02	Puolesta-asioija asioi pääsääntöisesti kuin päämiehensä, huomioiden vaatimukset kohdassa 5.3.	Kaikki
PU03	Puolesta-asiointi tulee estää, jos huollettava tai valtuuttaja on kuollut.	Kaikki
PU04	Jos digitaalisen palvelun sisällä siirrytään toiseen sovellukseen tai palveluun, niin puolesta-asioinnin oikeus tulee tarkastaa uudelleen (Puolesta asioinnin yleiskuvaus luku 5).	Kaikki
PU05	Puolesta-asioinnin oikeus tulee tarkistaa aina, kun digipalvelussa asioidaan toisen henkilön puolesta.	Kaikki

Taulukko 5.5 Alaikäisen puolesta asioinnin vaatimukset

Vaatimuksen ID	Vaatimus	Rooli
APA01	Puolesta-asioijalle ei näytetä digipalvelussa alaikäisen henkilön potilastietoja, jos alaikäinen on kieltänyt tietojen luovuttamisen ja terveydenhuollon ammattihenkilö on merkinnyt tiedon palvelutapahtumaan.	Kaikki
APA02	Puolesta-asioijalle ei näytetä digipalvelussa alaikäisen henkilön potilastietoja, jos alaikäisen päätöskykyä ei ole selvitetty terveydenhuollossa.	Kaikki
APA03	Alaikäistä koskevia potilastietoja, jotka ovat syntyneet ennen 1.8.2016 ei näytetä alaikäisille itselleen eikä hänen puolestaan asioijalle. **Lisätieto**: Alaikäisellä potilaalla, joka ikäänsä ja kehitystasoonsa nähden kykenee päättämään hoidostaan, on oikeus kieltää potilastietojensa antaminen huoltajalleen, muulle lailliselle edustajalleen tai muulle tiedonsaantiin oikeutetulle henkilölle (Asiakastietolaki (703/2023) § 51).	Kaikki

Vaatimuksen ID	Vaatimus	Rooli
APA04	Digitaalisen puolesta-asioinnin erityistilanteissa, kuten silloin, kun lapsen huollosta on tehty huollonjakosopimus, tai asiakkaalla tai puolesta-asioijalla on turvakielto, tulee noudattaa Puolesta asioinnin yleiskuvauksen luvun 5 linjauksia.	Kaikki
APA05	Puolesta-asioijalle ei näytetä digitaalisessa asiointipalvelussa alaikäisen asiakastietoja, jos alaikäinen asiakas on kieltänyt tietojen luovuttamisen ja sosiaalihuollon ammattihenkilö on hyväksynyt kiellon. Digitaalisessa asiointipalvelussa hyödynnetään samoja metatietoja, kuin OmaKannassa vastaavassa rajaamisessa käytetään. • Rajaamisessa käytetään alaikäisen asiakkaan asiakirjojen metatietokenttää "Luovutuskielto huoltajalle". Kun kenttään on kirjattu arvo 2 tai 4, asiakirjaa ei voi näyttää digitaalisessa asiointipalvelussa alaikäisen asiakkaan puolesta asioivalle henkilölle. • Digitaalisissa asiointipalveluissa noudatetaan Kanta-palvelujen käsikirjan luvun 5.4 kuvausta. **Lisätieto**: Vaatimus perustuu asiakastietolain 51.2 §:ään, jonka mukaan alaikäinen voi painavasta syystä kieltää antamasta itseään koskevia tietoja huoltajalleen, muulle lailliselle edustajalleen tai muulle tiedonsaantiin oikeutetulle henkilölle, jollei se ole selvästi alaikäisen edun vastaista, ja ottaen huomioon hänen ikänsä ja kehitystasonsa sekä asian laatu.	Asiointipalvelu
APA06	Digitaalinen asiointipalvelu voi mahdollistaa myös muun henkilön kuin huoltajan asioimaan alaikäisen puolesta. Muu kuin huoltaja voi asioida alaikäisen puolesta silloin kun asiointipalvelu sen sallii ja kaikki lapsen huoltajat, myös mahdolliset sijais- ja oheishuoltajat, ovat vahvistaneet lapsen puolesta annettavan valtuuden. **Lisätieto**: Muun kuin huoltajan puolesta asioimisen mahdollistamisessa digitaalisessa asiointipalvelussa tulee huomioida lapsen etu kokonaisuutena (YK:n yleissopimus lapsen oikeuksista, SopS 60/1991). Esimerkiksi OmaKannassa muiden kuin huoltajien asiointi on estetty sääntömoottorin säännöllä, ja vastaavaa sääntöä suositellaan käytettävän muissakin sote-asiointipalveluissa sosiaalihuollon ja terveydenhuollon asioissa. (Puolesta asioinnin yleiskuvaus luku 5).	Kaikki

5.6 Digitaalisissa asiointipalveluissa käyttäjän tuottamien tietojen hallinnan vaatimukset

Tässä luvussa kuvataan vaatimuksia tilanteeseen, jossa digitaalisen asiointipalvelun käyttäjän tietyn palveluntuottajan asiointipalveluissa tuottamat tiedot voidaan ottaa käsiteltäväksi palvelunantajan tietojärjestelmiin ja sisällyttää palvelunantajan vastuulla olevaan henkilörekisteriin, kun käyttäjä on palvelunantajan tarjoamien palvelujen piirissä. Asiointipalvelun käyttäjältä kysyttävät tai saatavat tiedot selvästi kuuluvat palvelunantajan rekisterinpitoon ja esimerkiksi tietojen poistaminen käyttäjän toimesta ei tulisi olla mahdollista.

Taulukko 5.6 Digitaalisissa asiointipalveluissa käyttäjän tuottamien tietojen hallinnan vaatimukset

Vaatimuksen ID	Vaatimus	Rooli
TH01	Käyttäjän asiointipalveluissa tuottama tieto voidaan sisällyttää palvelunantajan tuottamiin ja palvelunantajan rekisteriin kuuluviin asiakastietoihin ja asiakasasiakirjoihin ammattilaisen harkinnan mukaan. Näiden tietojen osalta on merkittävä, että tiedot ovat asiakkaalta saatuja	Asiointipalvelu
TH02	Käyttäjän tuottamien tietojen rekisterinpitäjänä toimii palvelunantaja joka tiedot on pyytänyt.	Asiointipalvelu

5.6.1 Koodistot kansalaisten käyttämissä ja tuottamissa tiedoissa

Kansallisena tavoitteena on yhteentoimivuus sote-palveluissa ja kansalaisten käyttämissä digitaalisissa palveluissa ja laitteissa tuotettavien tietojen välillä. Kansalaisten käyttämät digitaaliset palvelut voivat osin nojautua sote-palveluissa käytettäviin tietosisältöihin ja koodistoihin. Kansalaiset käyttävät ja hyödyntävät itseään tai läheisiään koskevia terveystietoja ja tietoja käyttämistään sosiaalipalveluista. Kansalaiset ja heidän käyttämänsä laitteet ja

sovellukset myös tuottavat yhä enemmän tietoa, josta osa on hyödynnettävissä sekä kansalaisen itsehoidossa että sote-palveluissa. Kansalainen on tärkeä tietolähde ja tietojen hyödyntäjä sote-palvelujen tuottamisessa sekä sote-palvelujen kautta omahoidossa. Myös henkilön itsehoito sekä oman terveyden ja hyvinvoinnin ylläpito ovat keskeisiä kansallisia tavoitteita, joilla pyritään vähentämään sote-palvelujen kuormitusta. Asiakastietolaissa on myös määritelty kansalaisen tuottama ja hallinnoima hyvinvointitieto erikseen sote-palveluissa syntyvistä asiakastiedoista.

Kansalaisen käyttämien ja tuottamien tietojen koodistojen yhteensopivuus on keskeistä asioinnissa ja omahoidossa, jossa sote-ammattihenkilöt ja kansalaiset toimivat yhdessä. Itsehoidossa ja omaehtoisessa terveyden ja hyvinvoinnin ylläpidossa tietosisältöjä ja mahdollisia koodistoja ohjaa ensisijaisesti ymmärrettävyys ja helppokäyttöisyys yksilön näkökulmasta. Nämä ovat kuitenkin tärkeitä näkökulmia myös, kun sote-palveluissa käytettäviä koodistoja sovitetaan toimimaan yhdessä kansalaisten käyttämien digipalvelujen kanssa. Sote-luokitusstrategiassa 2025-2030 on luotu tavoitetila koodistoille kansalaisen käyttämissä ja tuottamissa tiedoissa. Alla esitetyt suositellut vaatimukset ovat linjassa luokitusstrategian tavoitteiden kanssa.

Taulukko 5.6 Koodistojen ja asiakirjarakenteiden käyttö kansalaisen tuottamissa tiedoissa

Vaatimuksen ID	Vaatimus	Rooli
KK01	Digitaalisissa palveluissa käyttäjän tuottaessa tietoa asioinnissa tulisi käyttää samoja tai yhteensopivia koodistoja kuin sote-toiminnoissa muutenkin käytetään.	Asiointipalvelu
KK02	Jos käyttäjä tuottaa tietoa palvelussa, tulisi palvelussa käyttää kansalaistermejä ammattilaisten erikoistuneiden termien sijaan, mikäli termistöissä on "kansalaistermejä" käytettävissä. Lisätietoja: Esimerkiksi SNOMED CT –Terveysongelmat ja kontaktien syyt https://koodistopalvelu.kanta.fi/codeserver/pages/publication-view-page.xhtml.	Asiointipalvelu
KK03	Digitaalisissa palveluissa tulisi toteuttaa koodistoihin nojautuvia ominaisuuksia ja linkityksiä lisätietoihin tai lisäpalveluihin, esimerkiksi käyntisyy-, laboratorio- tai muiden sellaisten tietojen osalta, joissa ammattilaisten käyttämät termit ja selitteet ovat käyttäjälle vaikeaselkoisia.	Asiointipalvelu
KK04	Digipalveluun toteutettavien, asiakkaan laadittavaksi tarkoitettujen asiakirjojen tulee noudattaa Sosmeta-palvelussa julkaistuja asiakasasiakirjarakenteita.	Asiointipalvelu

5.7 Tietoturvavaatimukset

Alla olevaan taulukkoon on koottu digitaalisten palveluiden tietoturvavaatimukset. Digitaalisten palveluiden tulee huomioida myös 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 tietoturvavaatimukset.

Taulukko 5.8 Digipalvelujen tietoturvavaatimukset

Vaatimuksen ID	Vaatimus	Rooli
DTT01	Tietoturvauhkien ja -riskien tunnistaminen: Digipalvelun valmistajan tulee tunnistaa ja kontrolloida hyvinvointisovellukseen kohdistuvat tietoturvauhat ja -riskit. Riskien tunnistamiseen tulee sisällyttää vähintään tähän määräykseen liittyvien olennaisten vaatimusten tietoturva- ja tietosuoja-aiheisiin liittyvät riskit. Uhkien ja riskien tunnistaminen, kontrollointi ja riskiarvio ja sen johdosta tehtävät toimenpiteet on dokumentoitava sekä palvelun suunnittelun että muutostenhallinnan näkökulmasta (vastaa osittain ISO/TS 82304-2:2021 kohtaa 5.4.2.2.).	Kaikki

Vaatimuksen ID	Vaatimus	Rooli
DTT02	Tietoturvariskien arvio: Hyvinvointisovelluksen relevantit tietoturvariskit on arvioitava. Tietoturvariskien arvioinnissa tulee: a) huomioida sisäiset ja ulkoiset sovelluksen käyttötarkoituksen, oikeudellisten, sääntely- ja sopimusvaatimusten sekä rajapintojen ja sovellusten valmistajien ja muiden organisaatioiden välisten riippuvuuksien kysymykset; b) tunnistaa riskit ja mahdolliset seuraukset, jotka liittyvät tietojen luottamuksellisuuden, loukkaamattomuuden ja saatavuuden menettämiseen sekä riskien todennäköisyyteen; c) arvioida valvontatavoitteiden ja valvonnan sovellettavuutta sekä tietoturvaan liittyvien riskien että henkilötietojen käsittelyyn liittyvien riskien yhteydessä, erityisesti riskit henkilölle jota tiedot koskevat; d) määriteltävä, mihin riskiin on puututtava ohjelmistokoodauksella, laitteistomuutoksilla tai muilla tietoturvallisuuskäytännöillä; e) varmistettava ja dokumentoitava, sisältyykö riskeihin vastaamiseen varmuuskopiointi- ja palautusmenettelyitä; f) dokumentoitava, minkä jäännösriskin sovelluksen valmistaja hyväksyy. Valmistajan on suoritettava arviointi tarkoituksenmukaisessa laajuudessa, kehikkona on mahdollista käyttää useita erilaisia tietoturvallisuuden arviointiin soveltuvia standardeja (vastaa osittain myös ISO/TS 82304-2:2021[10] kohtaa 5.4.2.2). Lisätietoja: Palvelunantajan digitaaliselle asiointipalvelulle vastaava käytäntö on suositeltava sekä osana tietojärjestelmän riskiarviointia että palvelunantajan tietoturvasuunnitelmaa.	Kaikki, huom. asiointipalvelu suositeltava, ks. lisätieto
DTT03	Tietoturvariskien arvio / digipalvelun hyödyntämät alustat ja liittyvät sovellukset: Hyvinvointisovelluksen käyttämistä alustoista ja hyvinvointisovellukseen liittyvistä muista sovelluksista on pyrittävä varmistamaan riittävien tietoturvallisuuskäytäntöjen täyttyminen ja riskien arviointi. Esimerkiksi voidaan kuvata, onko hyvinvointisovelluksen valmistaja ja kaikki siihen liittyviä palveluja tarjoavat organisaatiot toteuttaneet ISO/IEC 27001 -standardin tai sitä vastaavan. Liittyviä palveluja ja alustoja voivat olla muut mobiili- tai web-sovellukset, pilvipalvelut, tallennuspalvelut, kolmannen osapuolen API-rajapinnat, ja muut ratkaisut, joita voidaan käyttää hyvinvointisovelluksen toteuttamiseen tai sen toimintojen tarjoamiseen. Liittyvien sovellusten ja alustojen tietoturvariskien arviossa on a) kuvattava keskeiset alustat ja liittyvät sovellukset, joihin hyvinvointisovellus nojautuu tai joihin se liittyy; b) nostettava esiin erityisesti, mikäli joidenkin tietosuojaan tai tietoturvallisuuteen liittyvien olennaisten vaatimusten täyttymisestä tietyn alustan tai liittyvän sovelluksen osalta ei voida varmistua (vastaa osin ISO/TS 82304-2:2021 kohtaa 5.4.2.1). Lisätietoja: Palvelunantajan digitaaliselle asiointipalvelulle vastaava käytäntö on suositeltava sekä osana tietojärjestelmän riskiarviointia että palvelunantajan tietoturvasuunnitelmaa.	Kaikki, huom. asiointipalvelu suositeltava, ks. lisätieto
DTT04	Tietoturvan haavoittavuuksien seuranta ja ratkaiseminen: Sovelluksen valmistajalla on oltava käytäntö, jolla seurataan, arvioidaan ja kirjataan hyvinvointisovellusta tai sen alustaa tai liittyviä palveluja koskevia tietoturvahaavoittuvuuksia sekä menettelyt haavoittuvuuksien ratkaisemiseen. Tietoturvahaavoittuvuuksia koskevia tietolähteitä voivat olla julkisesti saatavilla olevat raportit viranomaisilta sekä julkaisut toimittajilta kuten esimerkiksi käyttöjärjestelmätoimittajilta ja kolmansien osapuolten ohjelmistoilta. Seurantaprosessiin on sisällyttävä vähintään: a) sovelluksen käyttäjien ja asiakkaiden tiedottaminen tietoturvahaavoittuvuuksista, joista valmistaja on tullut tietoiseksi; b) sovelluksen käyttäjien ja asiakkaiden tiedottaminen lainsäädäntöjohdannaisista riskeistä, jotka vaikuttavat sovelluksen käyttöön; c) haavoittuvuusilmoitusten ja -raporttien koordinoidun seurannan ja ilmoittamisen käytännöt; d) ilmoituskäytännöt käyttäjille, viranomaisille ja muille sidosryhmille haavoittuvuuksista ja niiden aiheuttamista poikkeamista; e) ohjelmistokirjastojen ja ohjelmistokomponenttien päivitysten seuranta ja niiden käytön suunnittelu; f) haavoittuvuuksien seuranta sovellukseen liittyvissä palveluissa, esim. haavoittuvuudet pilvipohjaisten todentamis- ja tallennuspalvelujen tarjoajien palveluissa (vastaa osin ISO/TS 82304-2:2021 kohtaa 5.4.2.9.). Lisätietoja: Digitaaliselle asiointipalvelulle vastaava käytäntö on suositeltava sekä osana tietojärjestelmän riskiarviointia että palvelunantajan tietoturvasuunnitelmaa	Kaikki, huom. asiointipalvelu suositeltava, ks. lisätieto

Vaatimuksen ID	Vaatimus	Rooli
DTT05	Tietoturvan organisatoriset toimenpiteet: Sovelluksen valmistajalla on oltava käytössä organisatoriset toimenpiteet sen varmistamiseksi, että henkilötietojen käsittely (ks. myös Tietosuojavaatimukset) suoritetaan säädösten mukaisella ja tietojen sekä hyvinvointisovelluksen käyttötarkoituksen mukaisella tavalla. Toimenpiteisiin voi kuulua tietoturvan hallintajärjestelmän vaatimusten integrointi valmistajan prosesseihin ja sopimuksiin, tietoturvan hallintaan tarvittavien resurssien varmistaminen, sisäinen ja ulkoinen tiedottaminen tietoturva- ja tietosuojavaatimuksista ja niiden merkityksestä, käytännön toimenpiteet tietoturvan hallintajärjestelmän tavoitteista ja tuloksista, henkilöiden ohjaus ja tukeminen ja jatkuvat kehittämistoimenpiteet (Vastaa osin ISO/TS 82304-2:2021 kohtaa 5.4.2.6.). Lisätietoja: Digitaalisessa asiointipalvelussa tämä vaatimus tulee toteutetuksi palvelunantajan tietoturvasuunnitelmassa.	Kaikki, huom. asiointipalvelu suositeltava, ks. lisätieto
DTT06	Toimenpiteet lähdekoodin suojaamiseksi: Digipalvelun valmistajan on dokumentoitava toimenpiteet, joilla estetään digipalvelun lähdekoodin luvaton käyttö ja muutokset. Prosessiin voi sisältyä esimerkiksi seuraavia toimenpiteitä erityisesti mobiilisovelluksissa (joista kaikkien täyttäminen ei ole ehdoton vaatimus kaikissa eri tyyppisissä digipalveluissa): a) tarkista sovelluksen eheys ja sovelluksen ja sen resurssien muuttumattomuus; b)alustapalvelujen ja sovelluskauppojen varmistusten käyttö mobiilisovellusten varmentamiseen; c) muistin sisäisten koodin eheystarkastusten käyttö koodin muuttumiselta tai ohjelmistokutsuihin kohdistuvilta hyökkäyksiltä suojautumiseksi; d) käänteisen suunnittelun vaikeuttaminen ja koodin hämärtäminen (obfuskointi); e) merkkijonojen salaaminen sovelluslogiikan hämärtämiseksi; f) kehittäjien ominaisuuksien käytöstä poistaminen; g) virheenkorjauksen poistaminen käytöstä sovellusasetuksissa ja kehittäjätilan käytön tarkistaminen. Digipalvelun lähdekoodi on suojattava suunnittelun, kehityksen ja käyttöönoton aikana, jos lähdekoodi sisältyy jaettavaan digipalveluun (Vastaa ISO/TS 82304-2:2021 kohtaa 5.4.2.5). Lisätietoja: Digitaaliselle asiointipalvelulle vastaava käytäntö on suositeltava.	Kaikki, huom. asiointipalvelu suositeltava, ks. lisätieto
DTT07	Muutos- ja ylläpitotestaus: Digipalvelun valmistajan on dokumentoitava toimenpiteet, joilla digipalvelun ja siihen liittyvien palveluiden turvallisuus testataan säännöllisesti ja suurten muutosten yhteydessä. Testauksessa on arvioitava teknisten ja organisatoristen toimenpiteiden tehokkuutta luottamuksellisuuden, eheyden ja saatavuuden varmistamiseksi. Testauksen sisällön ja laajuuden tulisi määräytyä riskiarvion pohjalta. Testaukseen voi sisältyä automaattisia staattisen koodin haavoittuvuuden skannausratkaisuja, tunkeutumistestausta tai muita testauskäytäntöjä haavoittuvuuksien löytämiseksi (Vastaa ISO/TS 82304-2:2021 kohtaa 5.4.2.10). Lisätietoja: Digitaaliselle asiointipalvelulle vastaava käytäntö on suositeltava.	Kaikki, huom. asiointipalvelu suositeltava, ks. lisätieto
DTT08	Kansalaiskäyttäjän istunnon katkaisu: Digipalveluissa, joissa edellytetään sisäänkirjautumista tai tunnistautumista, on huolehdittava kansalaisen istunnon katkaisemisesta tai käyttöliittymän lukkiutumisesta ja/tai henkilötiedon piilottamisesta aikarajan jälkeen (Vastaa ISO/TS 82304-2:2021 [10] kohtaa 5.4.2.7). Lisätietoja: Digitaaliselle palvelunantajan asiointipalvelulle vaatimus on suositeltava heti, voimassa 1.1.2027.	Kaikki, huom. asiointipalvelu suositeltava, ks. lisätieto

Vaatimuksen ID	Vaatimus	Rooli
DTT09	Kansalaiskäyttäjän tunnistautumisen ja todentamisen toteutuskuvaukset: Digipalvelun valmistajan on kuvattava, millä toimenpiteillä: a) käyttäjän henkilöllisyys todennetaan ennen pääsyä henkilötietojen käyttöön; b) todennustapa ilmoitetaan käyttäjälle ennen sovelluksen käyttöönottoa; c) vähintään käyttäjän mahdolliset toimenpiteet, joilla digipalvelu on vuorovaikutuksessa sote-palvelujen tuottajiin tai joilla on taloudellisia vaikutuksia edellyttävät henkilön tunnistamista ja todentamista; d) mahdollisia salasanoja ei jätetä näkyviin pelkkänä tekstinä; e) jos pääsy digipalveluun paljastaa henkilötietoja, käyttäjä saa mahdollisuuden asettaa vahvan todennuksen menetelmiä (esim. monivaiheinen todennus ja/tai biometriikka) salasanojen lisäksi. Todennuksen tulisi koskea myös mahdollisten liitettyjen palvelujen käyttöä taustajärjestelmiä. Lisätieto: Digitaaliselle asiointipalvelulle vastaava käytäntö on suositeltava heti, voimassa 1.1.2027.	Kaikki, huom. asiointipalvelu suositeltava, ks. lisätieto
DTT10	Palvelunsovellusten suojaus: Palvelinsovelluksista on kuvattava, kuinka ne on suojattu tietoliikenteen, palvelinsovellusten, alustan sekä rajapintojen osalta. Hyvinvointisovellusten palvelinsovelluksille on suoritettava tietoturvatestaus. Sovelluksen käyttämän palvelinympäristön ja siinä toimivan hyvinvointisovellukseen liittyvän ohjelmiston suojaus on suunniteltava, toteutettava, dokumentoitava ja testattava (Vastaa ISO/TS 82304-2:2021 kohtaa 5.4.2.3). Lisätietoja: Digitaalisessa asiointipalvelussa suositeltava, täytetään pääosin tietojärjestelmän muiden vaatimusten kautta.	Kaikki, huom. asiointipalvelu suositeltava, ks. lisätieto
DTT11	Asiakas- ja kirjautumistietojen salaaminen tallennuksessa: Digipalvelu ei saa säilyttää kansalaisen laitteella salaamattomana kansalaisen asiakastietoja tai salasana- tai kirjautumistietoja. On kuvattava, kuinka tämäntyyppiset tiedot on suojattu, kun niitä käsitellään tai säilytetään sovelluksessa tai laitteessa, jossa sovellus toimii, ja testattava, että tietoihin ei pääse esim. yleiskäyttöisillä välineillä. Lisätietoja: käyttäjän tekemillä toimenpiteillä sovelluksesta tietojen kopiointi, tulostaminen tai paikallinen tallentaminen ovat sallittuja toimintoja, ja näin saaduista tiedoista vastaa käyttäjä itse (Vastaa ISO/TS 82304-2:2021 kohtaa 5.4.2.8). Lisätietoja: Palvelunantajan digitaalisessa asiointipalvelussa voimassa soveltuvin osin; todennus luokassa A ennen 1.1.2027	Kaikki, huom. lisätieto
DTT12	Välimuisti: Sovelluksessa, johon liittyy selainkäyttöä, on pyrittävä estämään kansalaisen sovelluksen käyttöön liittyvän salaamattoman henkilötiedon (sisältäen arkaluonteisen terveys- tai hyvinvointidatan) tallentuminen selaimen välimuistiin. Todentamisessa on kuvattava, kuinka tämä on toteutettu ja testattu, tai testattava, että tietoihin ei pääse esim. yleiskäyttöisillä välineillä. Valmistaja ei voi kuitenkaan vastata esim. yleiskäyttöisten selainten oikeellisesta toiminnasta. Lisätietoja: Palvelunantajan digitaalisessa asiointipalvelussa voimassa soveltuvin osin; todennus luokassa A ennen 1.1.2027	Kaikki, huom. lisätieto
DTT13	Käyttäjän huomiointi virhetilanteissa: Digipalvelun on kerrottava käyttäjälle virhetilanteista ymmärrettävästi niiden tapahtuessa. Digipalvelun on annettava selkeä virheilmoitus ja toimittava loogisesti yleisimpien tai todennäköisimpien virhetilanteiden sattuessa (esim. verkko-ongelmat, toimimaton yhteys taustapalveluun). Lisätietoja: Palvelunantajan digitaalisessa asiointipalvelussa voimassa soveltuvin osin; todennus luokassa A ennen 1.1.2027	Kaikki, huom. lisätieto

5.8 Tietosuojavaatimukset

Alla olevaan taulukkoon on koottu digitaalisten palveluiden tietosuojavaatimukset. Digitaalisten palveluiden tulee huomioida 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 tietosuojavaatimukset.

Taulukko 5.9 Digipalvelujen tietosuojavaatimukset

Vaatimus ID	Vaatimus	Rooli
DTS01	Henkilötietojen käsittelyn vastuuhenkilö ja tietosuojavastaava: Vaatimus on täytettävä, jos hyvinvointisovelluksen valmistaja toimii rekisterinpitäjänä tai sillä on tai voi olla pääsy hyvinvointi- tai asiakastietoihin. Jos hyvinvointisovelluksen valmistaja toimii rekisterinpitäjänä tai sillä on tai voi olla pääsy hyvinvointi- tai asiakastietoihin, hyvinvointisovelluksen valmistajan on nimettävä organisaation johtoon kuuluva henkilö, joka vastaa siitä, että valmistaja toteuttaa, ylläpitää ja valvoo henkilötietojen käsittelyn asianmukaisuutta ja henkilötietojen yksityisyyden suojaa sekä säädösten mukaisuutta. Lisäksi valmistajan on tarvittaessa (vähintään tietosuoja-asetuksen edellytysten täyttyessä) nimettävä erikseen tietosuojavastaava. (GDPR artikla 39, mukautettu ISO/IEC 27701: 2019, 6.3.1.1). Vastaava vaatimus täyttyy palvelunantajan käytössä olevissa digipalveluissa palvelunantajan tietoturvasuunnitelman kautta.	Potilastietoja käyttävä hyvinvointisovellus
DTS02	Kuvaus terveyteen liittyvien henkilötietojen suojauksesta: Vaatimus on täytettävä samoilla ehdoilla kuin vaatimus TS01. Hyvinvointisovelluksessa on huomioitava terveyteen liittyvien henkilötietojen käytön suojaus. Terveystietoihin kuuluvien henkilötietojen luokittelu ja suojausvaatimukset voivat vaihdella lainkäyttöalueelta toiseen, joten hyvinvointisovelluksen valmistajan on erityisesti huomioitava mm. erityisten henkilötietoryhmien suojaaminen, jota voidaan myös valvoa tiukemmin. (mukautettu ISO/IEC 27701: 2019, 7.2.2; Laki digitaalisten palvelujen tarjoamisesta 306/2019 4 §) Vastaava vaatimus täyttyy palvelunantajan käytössä olevissa digipalveluissa palvelunantajan tietoturvasuunnitelman ja muiden vaatimusten kautta.	Potilastietoja käyttävä hyvinvointisovellus
DTS03	Tietojen minimointi: Prosessit ja järjestelmät on suunniteltava siten, että tietojen keräys ja käsittely (mukaan lukien säilyttäminen, siirto ja hävittäminen) rajoittuvat siihen, mikä on tarpeen tietojen käsittelyn tarkoituksen kannalta. Jos henkilötietojen keräämisessä ja käsittelyssä on valinnaisuuta sen suhteen, mitä tietoja kerätään, jokainen vaihtoehto on oletusarvoisesti poistettava käytöstä ja otettava käyttöön vain rekisteröidyn nimenomaisella valinnalla. Tietojen minimointiin kuuluu sen varmistaminen, että (ISO/IEC 27701: 2019, 7.4.4; Yleinen tietosuoja-asetus (EU 679/2016), artikla 5;): - tietoja ei käsitellä tarkemmalla tasolla kuin tarpeen; - ei välitetä tarpeetonta käyttäjän identiteetin paljastavaa tietoa eri laitteiden tai palvelujen välillä; - käyttöä ja mahdollista tilin luomista ja varten kerätään vähimmäismäärä käyttäjän henkilötietoja - käytetään vain niitä alustan tai laitteiden toimintoja ja tietolähteitä, jotka ovat välttämättömiä, oletusarvoisesti ei esim. laitteen sijainti-, kamera-, mikrofoni-, kiihtyvyysanturi- ja muut anturit, yhteystietoluettelo- tai kalenteriominaisuuksia; - käytön aikana lähetetty laitteen numero tai IP- tai muita verkko-osoitteita tallennetaan vain tarvittavissa määrin digipalvelun tarkoituksen täyttämiseksi - tietoja joiden välittäminen tunnisteellisena ei ole välttämätöntä ei välitetä tai anonymisoidaan mahdollisuuksien mukaan.	Kaikki
DTS04	Henkilötietojen poistamisen ja tarkistamisen käytäntö Hyvinvointisovelluksen valmistajalla on oltava käytäntö sovelluksen käytön lopettamiseen ja siihen liittyvien tietojen poistamiseen. Hyvinvointisovelluksen käytön lopettamisen yhteydessä käyttäjän sovellus ja tiedot on pystyttävä poistamaan turvallisesti. Jos käyttäjä lopettaa sovelluksen käytön, on informoitava tietojen säilymisestä ja mahdollisuudesta poistaa tiedot sovelluksesta. Passiivisten käyttäjien kohdalla on oltava määriteltynä sovelluksessa sijaitsevien henkilötietojen säilyttämiskäytäntö. Valmistajan on määriteltävä säilyttämisajat huomioiden vaatimus säilyttää henkilötietoja vain niin kauan kuin se on tarpeen. Säilyttämiseen liittyen on tarvittaessa tehtävä dokumentoitu riskiarvio. Menettelyjen, joilla tietoja säilytetään ja käytetään edelleen sovelluksen käytön lopettamisen jälkeen, on oltava selkeitä ja ymmärrettävää ja niiden on annettava käyttäjälle mahdollisuus saada kopio tiedoistaan.	Potilastietoja käyttävä hyvinvointisovellus

Vaatimus ID	Vaatimus	Rooli
DTS05	Henkilötietojen käsittelyn kuvausten saatavuus käyttäjälle: Digipalvelun valmistajan on täytettävä lakisääteiset vaatimukset siitä, mitä tietoja henkilötietojen käsittelystä annetaan käyttäjille esimerkiksi ennen digipalvelun käyttöönottoa ja tietopyyntöjen yhteydessä. Tiedot voivat ainakin osin perustua selosteeseen henkilötietojen käsittelytoimista. (osa alakohdista: ISO/IEC 27701: 2019, 7.3.2, 8.5.8, 7.3.4; Yleinen tietosuoja-asetus (EU 679/2016), artikla 30;, artikla 12). Esimerkkejä tiedoista, joita informointiin voi kuulua (esimerkki kohdistettu hyvinvointisovelluksiin): a) henkilötietojen käsittelyn tarkoitus Kanta-palveluihin liittyvien ja muiden kerättävien tietojen osalta; b) hyvinvointisovelluksen valmistajan tai sen edustajan yhteystiedot; c) käsittelyn laillinen perusta, d) mistä henkilötiedot on saatu, ellei niitä ole saatu suoraan henkilötietojen kohteelta; d) onko henkilötietojen antaminen lakisääteinen tai sopimusperusteinen vaatimus, ja tarvittaessa mahdolliset seuraukset henkilötietojen toimittamatta jättämisestä; e) asiakkaan oikeudet ja velvoitteet, erityisesti pääsy tietoihin, tietojen muuttamisen, oikaiseminen, pyytäminen, poistaminen ja käsittelyn vastustaminen; f) miten asiakas voi peruuttaa suostumuksensa; g) henkilötietojen mahdolliset siirrot; h) henkilötietojen vastaanottajat tai vastaanottajaryhmät; i) henkilötietojen säilytysaika; j) mahdollisen henkilötietoihin perustuvan automaattisen päätöksenteon käyttö; k) asiakkaan tietopyyntöihin vastaaminen; l) asiakkaan informointitapa ja -käytäntö, jos henkilötietojen käsittelyn tarkoituksia muutetaan tai laajennetaan; m) asiakkaan informointitapa ja -käytäntö sekä asiakkaan luvan pyytäminen, jos henkilötietoja käsittelevien toimijoiden tai alihankkijoiden joukko laajenee tai muuttuu; n) mekanismit, joilla käyttäjä voi muuttaa tai peruuttaa suostumuksiaan; o) kuvaus siitä, kuinka käyttäjältä pyydetään lupa liittyen kuhunkin I) hyvinvointisovellukseen liittyvään tietolähteeseen; II) mahdollisiin ominaisuuksiin, joihin liittyy käyttäjän seurantaa III) käyttäjän laitteella suojattavan ominaisuuden tai resurssin, kuten kameran, mikrofonin, yhteystietojen, kalenterin tai puhelujen, käyttöön Vastaava vaatimus täyttyy palvelunantajan käytössä olevissa digipalveluissa palvelunantajan tietoturvasuunnitelman ja muiden henkilötietojen käsittelyn velvoitteiden kautta.	Kaikki
DTS06	Henkilötietojen käsittelyn tiivistelmä käyttäjälle: Enintään 150 sanan yleiskatsaukseen on sisällytettävä kuvaus käsitellyistä henkilötiedoista, tarkoituksesta ja säilyttämiskäytännöstä. Sovelluksen valmistajan on toimitettava keskeisimmät henkilötietojen käsittelyä koskevat tiedot käyttäjälle yksinkertaisesti, ytimekkäästi, läpinäkyvästi sekä ymmärrettävässä ja helposti saatavilla olevassa muodossa. Tiivistelmässä on käytettävä selkeää ja pelkistettyä kieltä kohdeyleisölle soveltuvalla tavalla. Tavoitteena on mahdollistaa riittävä ymmärryksen taso (tietosuojalukutaito) sekä tietoon perustuvat päätökset sovelluksen käyttäjille ja potentiaalisille käyttäjille. Esimerkiksi sosiaalisen median sovellusten tietosuojakäytäntöjen lukukäyttäytymistä koskevat tutkimukset viittaavat siihen, että kolme neljästä käyttäjästä ei lue tietosuojakäytäntöä, ja lukijoiden keskimääräinen lukuaika on 73 sekuntia. (ISO/IEC 27701: 2019, 7.3.3; ISO/TS 82304-2: 2021, 5.4.1.1.4.1; Yleinen tietosuoja-asetus (EU 679/2016), artikla 12.)	Kaikki

Vaatimus ID	Vaatimus	Rooli
DTS07	Henkilötietojen suojaustason ja yksityisyyden suojaustason säilyminen: Sovelluksen valmistajan on kuvattava, kuinka hyvinvointisovelluksen ja siihen liittyvien palveluiden osalta on varmistettu tietosuojan ja yksityisyyden suojan säilyminen tasolla, joka käyttäjälle ja kansalaiselle informoidaan ja johon tämä on antanut suostumuksen. Jos henkilötietoja käsitteleviä tahoja on muita kuin hyvinvointisovelluksen valmistaja, näiden tahojen kanssa on lähtökohtaisesti tehtävä sopimus tai kuvattava järjestely tietosuojan, tietoturvavallisuuden valvonnan ja yksityisyyden suojan tason varmistamiseksi tasolla, jolla ne on ilmoitettu käyttäjälle. Sopimuksen on oltava kirjallinen ja valmistajan on varmistettava, että sopimus tai sovittu käytäntö sisältää asianmukaisten kontrollien implementoinnin ottaen huomioon tietoturva- ja tietosuojariskien arvioinnin ja henkilötietojen käsittelijän suorittaman henkilötietojen käsittelyn laajuuden, sisältäen esimerkiksi: a) henkilötietojen jakamisen tarkoitus; b) valmistajan ja henkilötietojen muun käsittelijän välisen valvonnan järjestäminen; c) valvonnan piiriin kuuluvien organisaatioiden ja toimijoiden yksilöinti ja yhteystiedot; d) sopimuksen mukaisesti jaettavat ja/tai siirrettävät ja käsiteltävät henkilötiedot, minimointiperiaate huomioiden; e) yleiskatsaus käsittelytoimista (esim. siirto, käyttö); f) kuvaus tehtävien rooleista ja vastuista; g) vastuu teknisten ja organisatoristen turvatoimien toteuttamisesta henkilötietojen suojaamiseksi; h) vastuun määrittely henkilötietojen käyttöön kohdistuvan rikkomuksen sattuessa (esim. ilmoitukset asiakkaille, sopimuksen osapuolille ja viranomaisille); i) henkilötietojen säilyttämisen ja/tai hävittämisen ehdot; j) vastuut sopimuksen noudattamatta jättämisestä; k) seurantakäytäntö; l) asiakkaiden informointi tietojen käsittelystä ja sopimuksesta; m) asiakkaiden tiedonsaanti- ja muiden oikeuksien toteuttaminen; n) asiakkaan luvan pyytäminen ja asiakkaalle ilmoittaminen kaikista henkilötietojen siirroista muille toimijoille, muille osapuolille, muihin maihin tai kansainvälisille organisaatioille. (Mukaillen ISO/IEC 27701: 2019, 7.2.6, 7.2.7, 7.5.1 ja 8.5.1.) Henkilötietojen ja yksityisyyden suojaustason säilymiseen liittyviä vaatimuksen kohtia voi olla sisällytettynä myös rekisterinpitäjänä toimivan palvelunantajan tietoturvasuunnitelmaan.	Potilastietoja käyttävä hyvinvointisovellus
DTS08	Suostumuksen asianmukaisuus: Ominaisuuksissa, joissa nojaudutaan tietosuoja-asetuksen mukaisiin suostumuksiin, on perustuttava selkeään informointiin ja vapaaehtoiseen ja yksilöityyn menettelyyn, jossa kansalainen nimenomaisesti suostuu suostumuksen kohteena olevaan käytäntöön. Suostumuksen tulee olla vapaasti annettu, yksilöity tiedon käsittelyn syyn mukaan sekä yksiselitteinen ja selkeä. Suostumus on pyydettävä ennen kuin suostumuksen kohteena oleva toimenpide toteutetaan. Sekä luvituksiin että suostumuksiin liittyen suostumusta on pyydettävä uudelleen ennen ensimmäistä tiedonsiirtoa, jolla aiemman suostumuksen datasisällön lisäksi halutaan lähettää enemmän dataa, kun suostumusta oli aiemmin pyydetty pienemmälle joukolle tietoja. Suostumusta ei pyydetä jokaisessa lähetyksessä, jos vietyjen tietojen laajuus pysyy muuttumattomana. Suostumuskäytännöt koskevat myös mahdollisia evästeitä ja muita seurantatekniikoita, jos niiden kautta välittyy tietoa kolmansille osapuolille, sekä tietojen jakamista sosiaalisten verkostojen kanssa. (Mukaillen ISO/IEC 27701: 2019, 7.2.4.)	Kaikki
DTS09	Tietosuoja- ja tietoturvapoikkeamien menettelyt: Rekisterinpitäjällä on oltava tietosuoja- ja tietoturvallisuuspoikkeamissa käytettävä menettely, jonka tulee sisältää vähintään a) ilmoitukset henkilötietopoikkeamista tai -rikkomuksista käyttäjille tai asiakkaille; b) ilmoitukset henkilötietopoikkeamista tai -rikkomuksista viranomaisille; c) vastuut ja menettelyt henkilötietoihin liittyvien poikkeamien tunnistamisesta ja kirjaamisesta, ml. kuvaus tapahtumasta, ajanjakso, seuraukset, ilmoittaneen tiedot, ilmoituksen saajan / saajien tiedot, toimenpiteet tapahtuman ratkaisemiseksi, toimenpiteiden vastuuhenkilöt, mahdollinen palautettu data, tapahtumasta johtuneet henkilötietojen häviämiset / paljastumiset / saatavuushäiriöt / muuttumiset tai eheyden vaarantumiset; kuvaus vaarantuneesta tiedosta; c) informointitoimenpiteet; d) muut poikkeamissa sovellettavat toimenpiteet ja vaatimukset. Menettelyt on dokumentoitava. (osin ISO/IEC 27701: 2019, 6.13.1.1 ja 6.13.1.5.) Tietosuoja- ja tietoturvapoikkeamien menettelyihin liittyviä vaatimuksen kohtia voi olla sisällytettynä myös rekisterinpitäjänä toimivan palvelunantajan tietoturvasuunnitelmaan.	Kaikki

Vaatimus ID	Vaatimus	Rooli
DTS10	Rekisterinpitäjän tietojen saanti- tai siirtopyyntöihin vastaaminen: Rekisteröidyllä on oikeus saada rekisterinpitäjältä tiedot käsitteleekö tämä häntä koskevia henkilötietoja sekä vaatimuksen DTS05 mukaiset tiedot henkilötietojen käsittelystä. Kun käsittely perustuu suostumukseen tai sopimukseen, rekisteröidyllä on myös oikeus saada itseään koskevat tiedot jäsennellyssä, yleisesti käytetyssä ja koneellisesti luettavassa muodossa ja halutessaan siirtää kyseiset tiedot toiselle rekisterinpitäjälle (siirrettävyys / portability), jos tiedot ovat henkilön itsensä toimittamia ja koskevat häntä itseään, kun tiedot ovat automaattisesti käsiteltäviä ja kun tietojen siirto ei vaikuta haitallisesti kolmansien osapuolten oikeuksiin ja vapauksiin. Rekisterinpitäjällä on oltava dokumentoitu käytäntö rekisteröidyn pyyntöihin vastaamiseksi. Tiedot tulee antaa sopivassa tavanomaisessa vaihdettavassa muodossa. Mahdollinen tilanne on esimerkiksi hyvinvointisovelluksen korvautuminen toisella. Pyyntöihin on voitava vastata asianmukaisesti, vaikka hyvinvointisovelluksen valmistaja ei itse toimisi rekisterinpitäjänä. (EU:n tietosuoja-asetuksen 15 artikla, 20 artikla.) Rekisterinpitäjän tietojen saanti- tai siirtopyyntöihin vastaamisen vaatimuksen kohtia voi olla sisällytettynä myös rekisterinpitäjänä toimivan palvelunantajan tietoturvasuunnitelmaan.	Potilastietoja käyttävä hyvinvointisovellus
DTS11	Tietosuojavaikutusten arviointi: Rekisterinpitäjän tulee selvittää, koskeeko vaatimus tehdä EU:n yleisen tietosuoja-asetuksen 35 artiklan mukainen vaikutustenarviointi valmistajan toteuttamasta henkilötietojen käsittelystä. Rekisterinpitäjän tulee tehdä vaikutustenarviointi, mikäli se tietosuoja-asetuksen mukaan koskee sovellusta. (EU:n tietosuoja-asetuksen 35 artikla.)	Kaikki

5.9 Lokivaatimukset

Lokivaatimusten osalta noudatetaan THL:n määräyksiä ja olennaisia vaatimuksia siten kuin ne koskevat palvelunantajan digitaalisia asiointipalveluja ja potilastietoa käyttäviä hyvinvointisovelluksia. Lisäksi palvelunantajan digitaalisen asiointipalvelun tulee noudattaa lokitietojen hallinnan kansallisia vaatimusmäärittelyjä. Potilastietoja käyttävän hyvinvointisovelluksen tulee noudattaa Hyvinvointisovellusten rajapintaa potilastietoihin koskevia vaatimuksia ja toiminnallisia määrittelyjä.

5.10 Saavutettavuusvaatimukset

Palvelun tulee täyttää saavutettavuusvaatimukset, mikäli se kuuluu digipalvelulain soveltamisen piiriin. Lain piiriin kuuluvat viranomaiset, julkisoikeudelliset laitokset, osa järjestöistä sekä palvelut, joita käytetään tai kehitetään viranomaisten tuella (saavutettavuusvaatimukset.fi). Palveluntarjoajan tulee arvioida digipalvelulain sekä saavutettavuusvaatimukset.fi-sivuston perusteella kuuluuko sen toteuttaa saavutettavuusvaatimukset palvelussaan. Mikäli palvelu ei kuulu lain soveltamisen piiriin, kannustamme silti sitä täyttämään alla olevat saavutettavuusvaatimukset palvelussaan. Asiakastietolain (703/2023 84§) mukaan hyvinvointisovellusten tulee täyttää saavutettavuusvaatimukset.

Taulukko 5.11 Digipalvelujen saavutettavuusvaatimukset

Vaatimuksen ID	Vaatimus	Rooli
SA01	Saavutettavuusvaatimusten täyttäminen. Palvelun tulee täyttää digipalvelulain §7 esitetyt saavutettavuuskriteerit.	Kaikki, asiointipalvelu vain, jos käyttävä organisaatio digipalvelulain piirissä
SA02	Saavutettavuusselosteen tekeminen. Palvelun tulee tarjota käyttäjille saavutettavuusseloste.	Kaikki, asiointipalvelu vain, jos käyttävä organisaatio digipalvelulain piirissä

Vaatimuksen ID	Vaatimus	Rooli
SA03	Saavutettavuusselosteen tekeminen mobiilisovelluksille. Mobiilisovelluksia koskevan saavutettavuusselosteen on oltava saavutettavassa muodossa ja se on asetettava saataville mobiilisovellusta tarjoavan palveluntarjoajan verkkosivustolle tai muutoin siten, että seloste on saatavilla mobiilisovellusta ladattaessa.	Kaikki, asiointipalvelu vain, jos käyttävä organisaatio digipalvelulain piirissä
SA04	Saavutettavuuspalaute. Palvelulla tulee olla digipalvelulain mukainen yhteystieto tai lomake, johon se ottaa vastaan saavutettavuuspalautetta.	Kaikki, asiointipalvelu vain, jos käyttävä organisaatio digipalvelulain piirissä

5.11 Muut yleiset vaatimukset

Taulukko 5.12 Digipalvelujen yleiset vaatimukset

Vaatimukset ID	Vaatimus	Rooli
YL01	Käyttäjälle tekstiviestitse tai muun viestikanavan käyttöä varten, käyttäjältä tulee pyytää suostumus tai lupa.	Kaikki
YL02	Käyttäjälle tai puolesta asioijalle lähetetyt tekstiviestit eivät saa sisältää yksilöivää/suojattua/salassa pidettävää tietoa, vaan niiden on oltava yleisluontoisia. Rekisterinpitäjä vastaa, että yleisen tietosuoja-asetuksen 32 artiklan 1 ja 2 kohdan vaatimukset, kuten henkilötietoihin pääsyyn liittyvien riskien asianmukainen hallinta, täyttyvät lähetettäessä tekstiviestejä asiakkaalle (Henkilötunnuksen sisältävien automatisoitujen tekstiviestien lähetys terveydenhuollossa).	Kaikki
YL03	Mobiilisovelluksen näyttävissä ilmoituksissa tai herätteissä ei saa näkyä käyttäjän asiakas- tai potilastietoja. Näitä tietoja voidaan näyttää käyttäjälle vasta kun hänellä on sovellus auki tai aktiivissa käytössä. Asiakas- tai potilastietojen näyttäminen edellyttää aina käyttäjän vahvaa tunnistautumista. Ilmoituksessa voidaan kertoa esimerkiksi, että käyttäjälle on tullut uusi kirjaus tai resepti, mutta ei kertoa tarkempaa sisältöä.	Kaikki

Lähteet

Covid-19-epidemian vaikutukset hyvinvointiin, palvelujärjestelmään ja kansantalouteen Asiantuntia-arvio, syksy 2020

Suomen Kestävän kasvun ohjelma

Digitaalisuus sosiaali- ja terveydenhuollon kivijalaksi: Sosiaali- ja terveydenhuollon digitalisaation ja tiedonhallinnan strategia 2023–2035

Sote-ajanvaraus - yleiskuvaus ja terveydenhuollon ajanvarausratkaisujen kansalliset vaatimukset : versio 2.1

Sosiaali- ja terveydenhuollon digitaalisten palvelujen sanasto

Tiima-foorumi sosiaali- ja terveydenhuollon ajankohtaisista kehittämisnäkymistä

Puolesta asioinnin yleiskuvaus sosiaali- ja terveydenhuollossa

Yleisopas digitaalisten sote-palvelujen kehittämiseen 1.1

Hyvinvointisovellusten rajapintaa potilastietoihin koskevat vaatimukset ja toiminnalliset määrittelyt

Sote-sanastot

Sähköinen tunnistaminen

Laki sosiaali- ja terveydenhuollon asiakastietojen käsittelystä 703/2023

Määräys 4/2024: Määräys sosiaali- ja terveydenhuollon tietojärjestelmien ja hyvinvointisovellusten luokittelusta ja sertifioinnista

Valtuuksien sanasto

GDPR

Tieto hyvinvoinnin ja uudistuvien palvelujen tukena - Sote-tieto hyötykäyttöön -strategia 2020

Sosiaali- ja terveydenhuollon tietojärjestelmäpalveluiden seuranta ja arviointi

Sosiaali- ja terveydenhuollon tiedonhallinnan viitearkkitehtuuri

Euroopan parlamentin ja neuvoston direktiivi (EU) 2019/882, annettu 17 päivänä huhtikuuta 2019, tuotteiden ja palvelujen esteettömyysvaatimuksista (ETA:n kannalta merkityksellinen teksti)

Ehdotus EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUS eurooppalaisesta terveysdata-avaruudesta

Apulaistietosuojavaltuutetun päätös TSV/29/2020

Kanta-palvelujen käsikirja sosiaalihuollon toimijoille

Suomi.fi -valtuudet

Potilastietovarannon toimintamallit

Sähköisen lääkemääräyksen toimintamalli

Tietosuojavaltuutetun toimisto / säilytyksen rajoittaminen

Kansallinen koodistopalvelin

THL määräykset

Asiakas- ja potilastietojen käsittelyssä syntyvien lokitietojen hallinnan kansalliset vaatimusmäärittelyt

Saavutettavuusvaatimukset -sivusto

Henkilötunnuksen sisältävien automatisoitujen tekstiviestien lähetys terveydenhuollossa

Sote-luokitusstrategia 2025–2030