

Hyvinvointisovellusten kansalliset hyväksymiskriteerit

HL7 Finland Personal Health SIG

25.10.2016

Juha Mykkänen

THL OPER

juha.mykkanen@thl.fi



TERVEYDEN JA HYVINVOINNIN LAITOS



Tässä esityksessä

- Peruskäsitteet kriteerien näkökulmasta
- Kriteerien lähtökohdat ja perusteet
- Kriteerien osa-alueet
- Kriteerien päälähteet
- Hyväksymismenettelyjen perusteet

- Huom. tässä esityksessä ei määrittely / linjausasioita tai yksityiskohtia muilta osin kuin kriteerien osalta

Hyvinvointi / hoito – jatkumo

TAUSTAA

asiakkaita



kustannuksia / asiakas

- Oman hyvinvoinnin ylläpito
- Itsehoito (hoitosuhteen ulkopuolella, vaiva)
- Ohjattu omahoito (hoito- tai asiakassuhde, asiakkuus)
- Asiointi
- Hoito

Häilyvä raja

Omahoito

Hyvinvointi
Preventio
Itsehoito
Omaseuranta
Neuvonta
Ohjaus
Palveluihin
hakeutuminen
Tuki ja seuranta
Hoitoon
osallistuminen
Potilaan hoito

Omahoito:

Terveyden ylläpitoa ja hoitoa, josta kansalainen itse huolehtii käytettävissään olevan ohjeistuksen ja tukipalvelujen avulla. Omahoitoa voidaan toteuttaa sekä ennen hoitoon hakeutumista että hoitosuhteen aikana

Hyvinvointisovellukset (tässä esityksessä)

- Asiakkaan (tai hänen edustajansa) käyttämiä sovelluksia
 - Voivat liittyä Omakanta Omatietovarantoon
 - Voivat liittyä asiakkaan omiin potilas- ja asiakastietoihin Kanta-palveluissa asiakkaan suostumuksella
- Ei kata ”kaikkia mahdollisia hyvinvointiappseja”
- Eri asia kuin ammattilaisten käyttämät sovellukset
 - Ammattilaisten työvälineitä / järjestelmiä, liittyvät yleensä Kanta potilas- ja asiakastietoihin
 - Myös näiden kautta voidaan jatkossa käyttää asiakkaiden hyvinvointitietoja, kun luvitukset / suostumus kunnossa
- Voivat olla myös lääkinnällisiä laitteita (erillinen kysymys)

Keskeiset tietokäsitteet

- Hyvinvointitiedot
 - kansalaisen terveyttä ja hyvinvointia koskevat tiedot, jotka eivät sisälly asiakastietoihin ja jotka voidaan tallettaa omatietovarantoon
 - ”asiakkaan hallinnassa”: asiakas päättää tallettamisesta, käytöstä, hävittämisestä jne.
- Asiakastiedot
 - potilastiedot, jotka sisältyvät terveydenhuollon potilasasiakirjoihin sekä sosiaalihuollon asiakasta koskevat henkilötiedot, jotka sisältyvät sosiaalihuollon asiakasasiakirjaan (tai mahdollisiin sosiaali- ja terveydenhuollon yhteisiin asiakasasiakirjoihin)

Hyvinvointisovellusten riskit ja niihin varautuminen

- Tietosuojariskit (privacy): asiakkaan tiedot karkaavat sivullisille
- Tietoturvallisuusriskit (security)
- Terveys- ja hyvinvointiriskit (safety): sovellukset ohjaavat vääränlaiseen käyttäytymiseen tai toimivat virheellisesti
- Varautuminen väärinkäyttöksiin
- Varautuminen ohjelmistovirheisiin
- Kuinka vastataan:
 - Ratkaisujen kehittämisessä riskien tunnistaminen ja niihin varautuminen
 - Alustan ja sovellusten pakolliset ominaisuudet
 - Sovellusten hyväksymiskriteerit
 - Hyväksymisprosessi
 - Valvonta

Riski

	Vähemmän vakava					Vakava
Toden- näköinen				Ei hyväksyttävissä		
		Kompensoitavissa				
	Hyväksyttävissä					
Epätoden- näköinen						

Kriteerien perusteita ja lähtökohtia

- Omatietovarantoon liittyy kahdenlaisia hyvinvointisovelluksia:
 - vain kansalaisen omaa tietoa käyttäviä hyvinvointisovelluksia
 - myös asiakas- ja potilastietoja käyttäviä sovelluksia
- Kriteerit tiukkemmat niille sovelluksille jotka käyttävät **asiakas- ja potilastietoja** Kanta-palveluista
 - Vastaaventyypisiä kuin muillekin A-luokan järjestelmille
- Omatietovaranto voi olla myös yksi ammattilaissovellusten tietolähde
 - Järjestelmä jossa sekä ammattilais- että asiakasosioita on sekä ATJ/PTJ että hyvinvointisovellus
 - Ammattilaissovelluksilla ammattilaissovellusten ”normaalit kriteerit”
 - Omatietovaranto ei korvaa muita Kanta-palveluita
- Hyvinvointisovellusten kriteerit oltava täytettynä ennen siirtymistä tuotantoympäristöön
 - Lisäksi ”hiekkalaatikko” kehittämiseen, asiakastestiympäristö todentamiseen
- **Tavoitteena riittävä luottamus ratkaisuihin nostamatta liikaa toteuttamis- ja käyttöönottokynnystä**

Kriteerien kehittämisen tavoitteita

- Riittävä luottamus kansallisiin ratkaisuihin (ml. Omatietovaranto)
 - Eriyisen olennaista asiakastietoja käyttävissä sovelluksissa
- Matala kynnys peruskriteerit täyttävälle hyvinvointisovelluksille tulla mukaan ekosysteemiin
- Tiedot ja sovellukset asiakkaan hallinnassa
 - Asiakkaan luvitukset, asiakkaalle näytettävät tiedot, jne.
- Yhteensopivuus kansainvälisten kriteerien kanssa
- Kriteerit täyttävien hyvinvointisovellusten luettelo Omakantan yhteyteen
 - Omatietovarantoon ja Kanta-palveluihin liittyvät hyvinvointisovellukset

Millaisiin järjestelmiin kriteerit kohdistuvat

- Hyvinvointisovelluksiin, yhdistelmiä seuraavista
 - Vain hyvinvointitietoja käyttävät
 - Asiakas- ja potilastietoja käyttävät
 - Huomioitava myös ”natiiviappsit”, jotka nojautuvat suoraan Omatietovarantoon
- Hyvinvointitietojen käytön osalta pohjaa myös ammattilaisjärjestelmien kriteereihin
 - Hyvinvointitietojen ammattilaishyödyntämisen kriteerejä järkevää luoda samalla: linkittyvät tuleviin päivityksiin ammattilaisjärjestelmien olennaisissa vaatimuksissa

Vaatimusten osa-alueita

- **Peruskriteerien tukeminen:** hyvinvoinnin ja terveyden edistäminen, safety (käyttäjäturvallisuus), ”peruspelissäännöt”
- **Selkeät kuvaukset asiakkaalle** (käyttötarkoitus, tietojen käyttö jne.)
- **Tietosisällöt ja (FHIR-)rajapinnat:** yhteiset määrittelyt yhteisesti käytettäville resursseille ja profiileille
- **Luvittamis- ja turvallisuusprotokollat:** avaimet, sovellustunnisteiden säilytys, virallisten asiakas- ja potilastietojen käyttö jne.
- **Sovellusturvallisuus ja tietosuoja:** esim. ei salaamattomia hyvinvointitietoja laitteessa ja verkon yli, laatu prosessi
 - Terveys- ja hyvinvointisovellukset voimakkaan kehityksen kohteena myös kv. ISO-standardeissa
- **Toiminnalliset peruskriteerit / rajaukset**

Vrt. esim. asiakastietolain vaatimukset:
toiminnallisuus, yhteentoimivuus,
turvallisuus ja tietosuoja, omavalvonta

TERVEYDEN JA HYVINVOINNIN LAITOS

Esimerkki: selkeät kuvaukset asiakkaalle

- Palvelukuvaus: kuvattava selkeästi ja kansantajuisesti
 - Sovelluksen käyttötarkoitus
 - Mitä PHR-tietoja sovellus käyttää, tuottaa, muuttaa
 - Liittyykö sovellus Kanta-palvelujen kautta saataviin asiakastietoihin
 - Mahdollinen maksullisuus ja hinta
 - Millaista tukea käyttäjälle tarjolla (mutta palvelutasosta ei tiukkoja vaatimuksia)
 - Keskeisimmät rekisteri-, tietojen hyödyntämiskäytännöt
 - Tieto siitä, minne tietoja tallennetaan
 - ”Kuinka palvelusta ”pääsee eroon” (myös maksut)”
 - Mitä kieliä sovellus tukee
- Kuvaus näytettävä ja asiakkaan hyväksyttävä ennen käyttöönottoa / sovelluksen luvittamista
- Kuvaus oltava katsottavissa milloin tahansa sovelluksen kautta, kuvaus löydyttävä myös hyväksytyjen sovellusten luettelosta
 - Palvelukuvauksessa linkki Omakanta-käyttöehtoihin

Vaatimusten lähteitä

- Määräys A-luokan tietojärjestelmien olennaisista tietoturva-vaatimuksista (1/2015)
- Draft Code of Conduct on privacy for mobile health applications / EC
 - Edelleen tarkentumassa
- Health and wellness apps – Quality criteria across the life cycle – Code of practice (PAS 277:2015)
 - Pohja myös kv ISO-standardoinnille
- Osin ja tarvittaessa myös:
 - EC Green paper on mobile health (Vihreä kirja terveysalan mobiilisovelluksista)?
 - Määräys sote-tietojärjestelmien olennaisista toiminnallisista vaatimuksista
 - ISO/HL7 PHR-S FM standard
 - Andalucia app certification requirements

Mitä EI vaadita

- 24/7 tukea loppukäyttäjille
- Nojautumista pelkästään omatietovarannon tietoihin / kaikkien tietojen tallentamista omatietovarantoon
- Kaikilta liittyjiltä ”lääkinnällisten laitteiden” statusta – riskitaso huomioitava – jos palvelu on lääkinnällinen laite, vaatii lääkinnällisen laitteen hyväksymismenettelyt
- Kaikilta sovelluksilta kliinistä validointia
- Sovelluksen tuottajalta Y-tunnusta (myös yksityishenkilöt saavat tehdä sovelluksia), mutta pystyttävä nimeämään vastuutaho, joka huolehtii kriteereistä ja hyväksyttämisestä
- Liiketoimintamallin kuvausta (esim. mihin muuttujiin hinnoittelu / kannattavuus perustuu)

Hyväksymismenettelyjen linjaukset

- Omatietovarantoon liittyminen tulisi pitää mahdollisimman kevyenä
 - ”Liittyykö auditointiin/sertifiointiin mitään sisältövaatimuksia?”
- Käyttötarkoitus ja kriteerien täyttäminen kuvattava viimeistään ennen tuotantoympäristöön siirtymistä; todennetaan testausympäristössä
 - Kriteeristö ja ”kysymyspatteristo” täytettävä dokumentoidusti jo ennen testaukseen hakeutumista
 - Suurikin osa tuotannon kriteereistä voidaan tarkistaa jo asiakastestausympäristöön hakeuduttaessa
- Kaikki liittyvät palvelut testataan?
- Täytyykö joidenkin kriteerien täyttäminen varmistaa ulkoisen auditoinnin avulla – aina tai joissain tapauksissa?
- Uudelleentestaus tai –auditointi?
- Asiakastietoihin (palvelutuottajien kautta syntyneet Kanta-tiedot) liittyvät ammattilaissovellukset arvioidaan A-luokan järjestelmien kriteerien mukaisesti
 - Entä ei-laillistettujen ammattilaisten sovellukset tai sellaiset jotka käyttävät vain hyvinvointitietoja mutta joita käyttää ammattilainen?

Hyväksymisprosessin päävaiheet (sovelluksen tuottajan asiakasprosessi)?

1. Kehittäminen, dokumentointi ja oma testaus (hiekkalaatikko)
2. Hakeutuminen asiakastestaukseen (asiakastestausympäristö) ”kihlaus” tuotantoympäristöön
 1. Peruskriteerien / sovelluksen kuvausten, tarkastaminen, yhteystiedot + muut perustiedot
 2. Liittyminen asiakastestausympäristöön, asiakkuudenhallinnan tiedot
 3. Testaus + raportointi
 4. → Kelan testauslausunto
3. Hakeutuminen tietoturva-auditointiin (jos käyttötarkoitus sitä edellyttää)
 - vain A-luokka tai asiakastietoja hyödyntävät → vaatimustenmukaisuustodistus (soveltuvat / sovitetut vaatimukset)
4. Liittyminen tuotantoon
 1. Päivitykset kohdan 2 tietoihin
 2. Rekisteröinti alustaan ja sovellushakemistoon (tuotantoympäristö): riittäisikö valvontaan
 3. Tekninen liittäminen
5. Tuotanto
6. Päivitykset (kohta 1→)

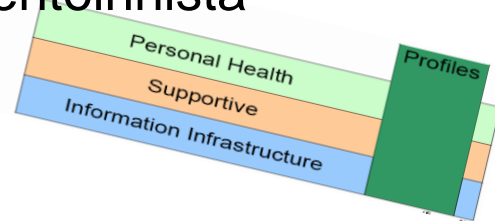
Testaus- ja sertifiointiohjelmia, ryhmiä ja instituutioita

- ORCHA / UK: Organization for the Review of Care & Health Applications
- NHS England Health Apps library
- Happtique Health App Certification Program (HACP) (US): voluntary app certification scheme
- Taltioni –osuuskunnan hyväksymismenettelyt
- HealthVault ”trusted platform”: > 300 apps, > 200 devices, ”families in control”..

- Continua plugfest: yhteentoimivuustestaukset, Continua Test & Certification WG
- IHE Connectathon: yhteentoimivuustestaukset
- HL7 Mobile Health + Conformance & Guidance for Implementation Testing (CGIT) WG
- Kanta-sertifiointi (yhteistestaus ja tietoturvallisuuden auditointi) (FI), CCHIT (USA) ja QREC (EU): pääfokus potilastietojärjestelmissä
- AAL-ohjelmien sertifiointityöpaketit

Mistä kannattaa huolehtia (joka tapauksessa)

- Sovellusten ja ratkaisujen käyttötarkoituksen huolellisesta ja ymmärrettävästä kuvaamisesta
- Selkeydestä: mikä asiakkaan ja mikä sote-palveluntuottajan tietoa
- Riittäväntasoisesta sovellusturvallisuudesta
- Omatietovaranto-tietomallin kehittämiseen osallistumisesta
- Standardien mukaisuudesta
- Ratkaisujen tuottajan laatujärjestelmästä ja dokumentoinnista



Keskusteluun

- Kommentteja, tarkennus-, lisäys- tai poistoehdotuksia?
- Kansainvälisissä malleissa ja suosituksissa selvä siirtymä *riskipohjaiseen* toimintaan, soveltaminen tarkoittaisi:
 - Joukko ”tarkkoja vähimmäisvaatimuksia” eri sovellusluokkiin +
 - Sovelluksen tuottajan velvoite analysoida ja dokumentoida riskit ja niihin varautumisen tavat
 - Vaatimuksissa viittaaminen ulkoisiin, erikseen päivittyviin vaatimuksiin
 - Linjattava mm., missä määrin ”pidettävä riskivaraaminen ajan tasalla”

Jatko / kriteerit ja valvonta

- Lainsäädäntöpohjan tarkennus mm. asiakastietolaki, tietosuoja-asetus, kehittäjien ja valvonnan vastuut
- Omatietovarannon kehittämisen yhteydessä myös kriteerien tarkennukset
- Kriteereissä ja todentamismenettelyissä selvitetty myös pohjoismaisen yhteistyön mahdollisuuksia
- Omatietovarannon tuotanto 2017

Kiitokset!

OPER



TERVEYDEN JA
HYVINVOINNIN LAITOS

<http://www.kanta.fi/web/ammattilaisille/omakannan-omatietovarannon-maarittelyt>

Lisämateriaalia



TERVEYDEN JA HYVINVOINNIN LAITOS

Ympäristöt

Ympäristö	Säännöt
Hiekkalaatikko	<p>Kehitysympäristö Kaikille avoin, profiileja ja extensioneita voi lisätä vapaasti Toimii ilman rekisteröintiä, voi halutessaan rekisteröityä. Rekisteröityjen käyttäjien resursseja ei voi poistaa + mahdollisesti muut ”edut”.</p> <p>http://fhirsandbox.kanta.fi.</p>
Asiakastestiympäristö	<p>Ympäristö liittymistestejä varten Ympäristöön liittyneet voivat lisätä profiileja ja extensioneita vapaasti Liittymisen ehtona valmis tai melkein valmis sovellus</p>
Tuotanto	<p>Ympäristö todellista käyttöä varten Ylläpitäjä voi lisätä AT-ympäristössä toimiviksi todetut profiilit ja extensionit. Liittymisen ehtona testattu ja sertifioitu sovellus</p>

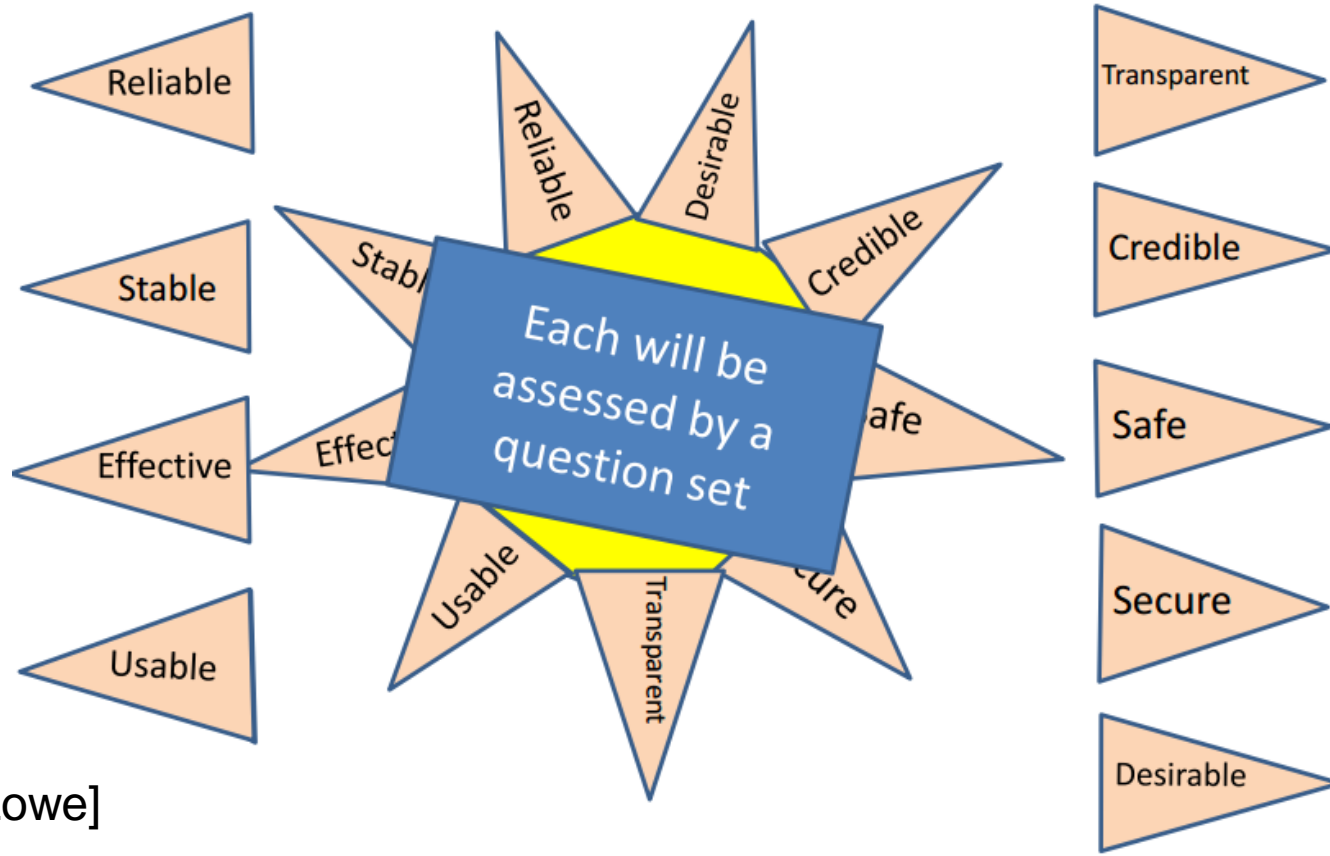
Paremmiin ja huonommin onnistuneita esimerkkejä, suosituksia...

- Unaddressed privacy and security risks in accredited health and wellness apps: lessons from a cross-sectional systematic assessment:
<http://bmcmmedicine.biomedcentral.com/articles/10.1186/s12916-015-0444-y>
- Happtique suspends mobile health app certification program:
<http://mobihealthnews.com/28165/happtique-suspends-mobile-health-app-certification-program> , <http://whats.harold.in/2013/12/certification-for-lack-of-certification.html>
- ‘Trust but verify’ – five approaches to ensure safe medical apps:
<http://bmcmmedicine.biomedcentral.com/articles/10.1186/s12916-015-0451-z>

EU guidelines

- EU draft mHealth app assessment guidelines: Open Stakeholder Meeting 9th June Andrew Ruck & Charles Lowe
 - Vapaaehtoiset ohjeistukset, jotka kuitenkin tarkoitettu sitovien säädösten soveltamishajaksi
 - https://www.eiseverywhere.com/file_uploads/a564484398e8342b6a384dd296a2af12_Andrew-Ruck_Charles-Lowe-EU-draft-mHealth-app-assessment-guidelines.pdf
- mHealth assessment guidelines – Introduction, Carmen Laplaza Santos
 - Yleiskuva EU aktiviteeteista mHealth green paperin pohjalta:
 - Guidelines for the assessment of the validity and reliability of mHealth apps
 - Medical device legislation + kysely “safety of apps and other non-embedded software”
 - Code of Conduct on privacy for mobile health
 - European standard on quality criteria for the development of health and wellness apps
 - https://www.eiseverywhere.com/file_uploads/c1b39ec5ced9612a1065208f3f4c8362_Carmen-Laplaza-Santos_mHealth-assessment-guidelines-Introduction.pdf
- Teemupekan esitys:
https://www.eiseverywhere.com/file_uploads/bc59d67605e0298087fcd773ff46ec74_TeemupekkaVirtanen-13.30_14.30.pdf

Kriteerien luokkia / EU-valmistelut



[Ruck & Lowe]

2020

[Ruck & Lowe]

High medical risk

Low medical risk

GDPR

App Code of Conduct on privacy (voluntary)

MDR/IVDR/IDDR

Guidelines on app assessment (voluntary)

Guidance for app developers

Possible legislation/Code of Conduct on safety following current consultation

Possible legislation/Code of Conduct on usability following consultation shortly