

Ajankohtaisia sosiaali- ja terveydenhuollon tietosuojatoteutuksia

Koronavilkku-sovelluksen tietosuoja ja tietoturva, toteutuksen periaatteet ja lähtökohdat

- *Minna Saario, Johtaja, STM, OHO*

Sosiaali- ja terveydenhuollon tietojen yhteiskäyttö edistämään asiakas- ja potilasturvallisuutta ja parempaa hoivaa

- *Heikki Onnela, Tuotekehitysjohtaja, Apotti Oy*

**SOSIAALI- JA TERVEYDENHUOLLON
ATK-PÄIVÄT WEBINAARI
15.10.2020
atkpaivat.fi**

**SOSIAALI- JA TERVEYDENHUOLLON
TIETOSUOJAPÄIVÄT WEBINAARI
24.11.2020
tapahtumat.fcg.fi/sohvitellu**



**Tartuntaketjujen katkaisun tehostamiseen
tarkoitettun tietojärjestelmän
käyttöönottohanke**

**Koronavilkku-sovelluksen
tietosuoja ja tietoturva,
toteutuksen periaatteet ja
lähtökohdat**

Minna Saario
johtaja
Ohjausosasto, Digitalisaation ja
tiedonhallinnan yksikkö

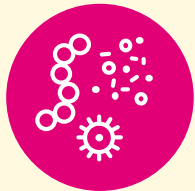
• **9.9.2020**



Kokonaiskuva



Ei ilmoituksia – sovellus rekisteröi kohtaamisia



Tartunta

Tieto
tartunnasta

Avauskoodi

Sovellus
lukittuu



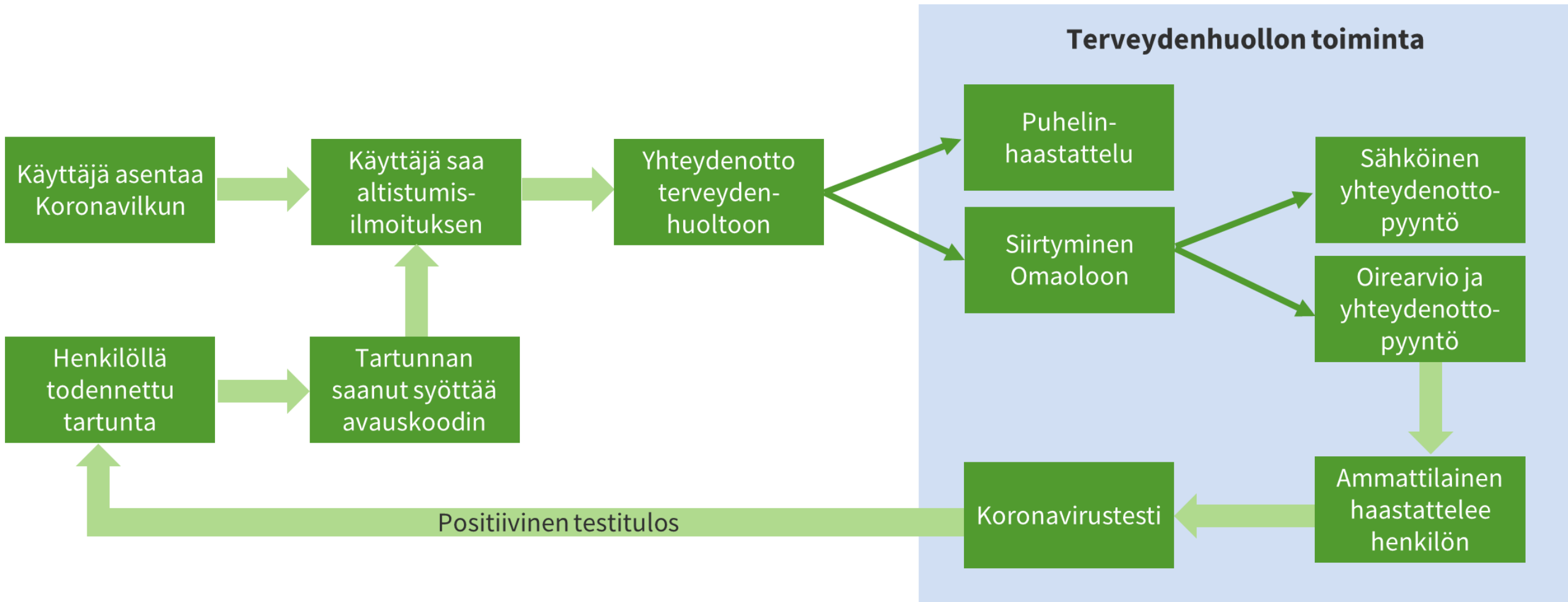
Altistumis-
ilmoitus

Altistumis-
ilmoitus

Toiminta-
ohjeet

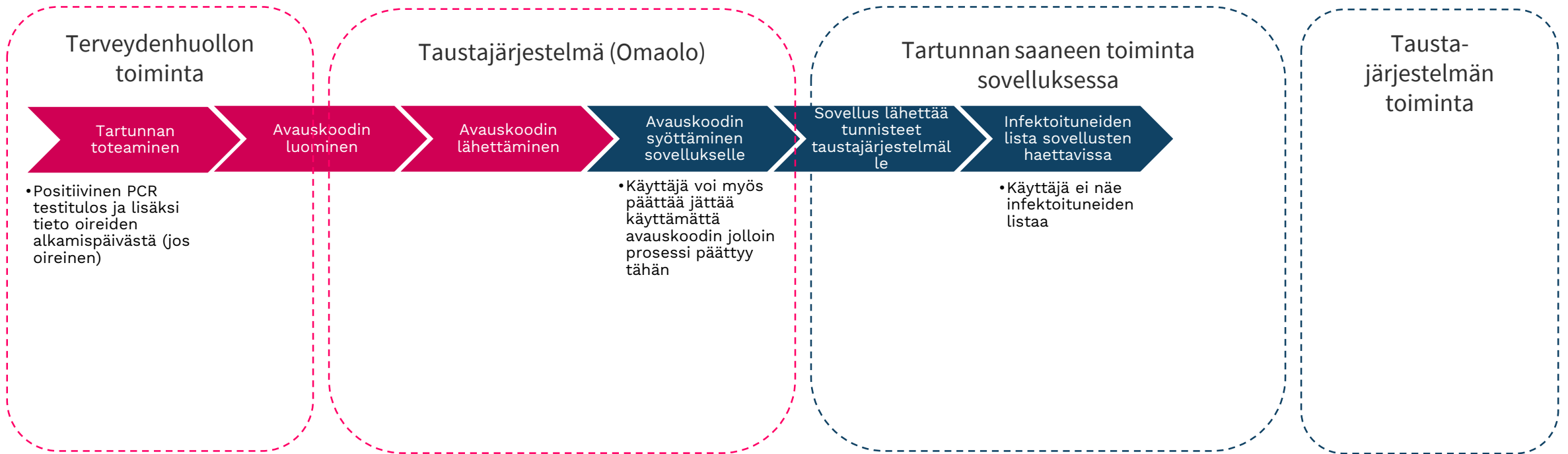
Oirearvio
tai yhteydenotto

Kokonaiskuva



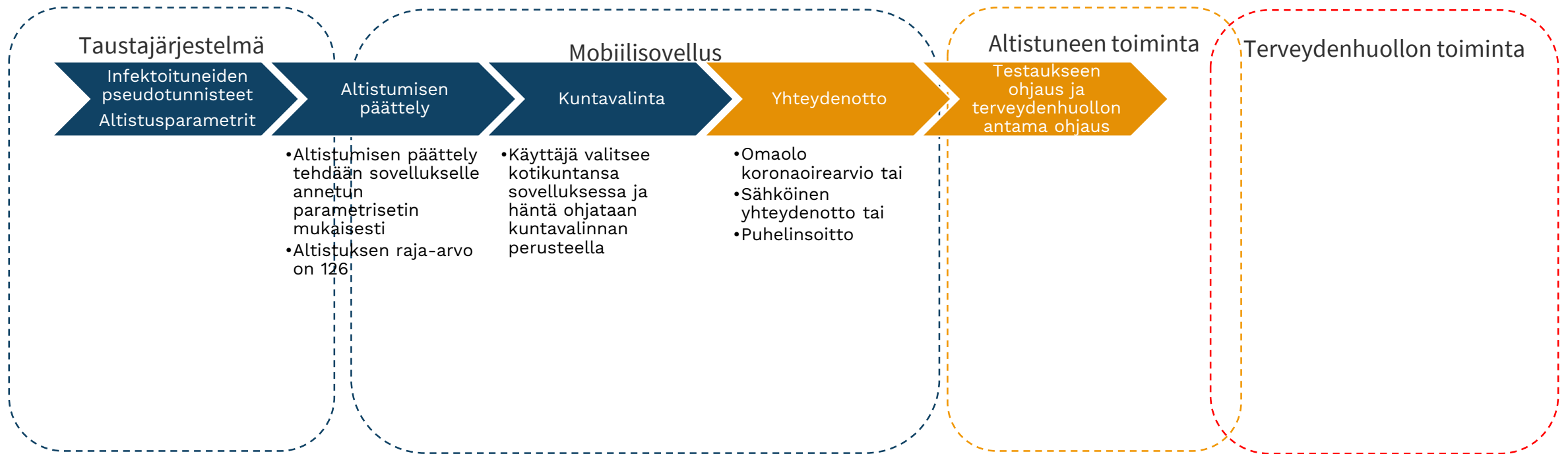
Sovelluskäyttäjän prosessi:

Tartunnan saaneen vuo



Sovelluskäyttäjän prosessi:

Altistuneen vuo



EU-maiden yhteiset tietosuojaperiaatteet

- Sovelluksen käyttö on vapaaehtoista ja maksutonta
- Sovellus ei käsittele sijaintitietoja
- Sovellus ei käsittele tunnistesteellista henkilötietoa
- Koska sovelluksen käyttämät tunnuskoodit/pseudotunnisteet ovat kuitenkin teoriassa yhdistettävissä henkilöön , tietojen käsittely katsotaan henkilötietojen käsittelyksi
 - Tietojen käsittelystä on säädetty lailla, Suomessa tartuntatautilain 4 a luku
 - Laki on määräaikainen ja voimassa 31.3.2021 asti

Mitä Koronavilkku ei tee

- ei tallenna henkilötietoja: nimeä, syntymäaikaa tai yhteystietoja
- ei pysty selvittämään kohtaamisen osapuolten henkilöllisyyttä
- ei kerro, onko joku läsnäolevista saanut tartunnan
- ei kerro, onko jossakin paikassa tartunnan saanut henkilö
- ei kerää sijaintitietoja
- sovelluksen käyttäjiä ei voida suoraan tunnistaa (perustuu säännöllisesti vaihtuviin ja satunnaisiin tunnuskoodeihin)
- ei kerro toisille käyttäjille, ketkä ovat saaneet koronavirustartunnan
- ei kerro toisille käyttäjille, ketkä ovat saaneet altistusilmoituksen

Tartuntatautilaki 4 a luku (HE 101/2020; laki 582/2020)

Covid-19-tartuntaketjujen katkaisua tehostava tietojärjestelmä koronavirukselle mahdollisesti altistuneiden tavoittamiseksi

- THL:n tehtävät tietojärjestelmän toteuttamisessa (rekisterinpitäjä)
- Kansaneläkelaitoksen tehtävät taustajärjestelmän ylläpidossa
- Tietojärjestelmän käytön yhteydessä tapahtuva henkilötietojen käsittely (dia 9)
- Poikkeus 22 §:ssä säädetystä ilmoitusvelvollisuudesta (lääkärille)
- Tietojärjestelmästä saatujen mahdollista altistumista koskevien tietojen käsitteleminen (THL voi luovuttaa tietoja)
- Taustajärjestelmän ylläpidon ohjaus (STM –Kela)
- Tietojärjestelmän tietoturvallisuuden arvioiminen (LVV, KTK)
- Valvonta (Valvira)

Tartuntatautilaki 43 c §

Tietojärjestelmän käytön yhteydessä tapahtuva henkilötietojen käsittely

Tietojärjestelmän käytön yhteydessä saadaan käsitellä seuraavia henkilötietoja:

- 1) käyttäjän pseudonyymiset tunnisteet;
- 2) käyttäjän kohtaamien toisten käyttäjien pseudonyymiset tunnisteet ja näihin kohtaamisiin liittyvät tarpeelliset tiedot niiden kestosta ja ajankohdasta sekä mobiililaitteen bluetooth-signaalin voimakkuudesta;
- 3) tartunnastaan ilmoittaneen käyttäjän pseudonyymiset tunnisteet;
- 4) käyttäjän saama tieto mahdollisesta altistumisestaan;
- 5) käyttäjän 43 e §:n 1 momentissa tarkoitetun yhteydenottopyynnön yhteydessä ilmoittamat nimi, puhelinnumero, kotikunta ja tarvittaessa tilapäinen asuinpaikka ja oiretiedot.
- Edellä **2 momentin 1, 2 ja 4 kohdassa tarkoitetut tiedot saadaan tallentaa käyttäjän mobiililaitteeseen.** Taustajärjestelmään saadaan tallentaa 2 momentin 3 kohdassa tarkoitetut tiedot mahdollisesti tartunnalle altistuneiden mobiilisovelluksen käyttäjien tavoittamiseksi ja 5 kohdassa mainitut tiedot luovutettaviksi kunnan tai sairaanhoitopiirin kuntayhtymän terveydenhuollon toimintayksikölle sekä Ålands hälso- och sjukvård -nimiselle viranomaiselle siten kuin 43 e §:ssä säädetään.
- Edellä 2 momentin 1-5 kohdassa tarkoitetut tiedot on poistettava ja tuhottava 21 vuorokauden kuluessa niiden tallentumisesta. Tiedot on kuitenkin poistettava ja tuhottava viimeistään, kun tietojärjestelmä poistetaan 43 a §:n 4 momentin mukaisesti käytöstä.

Tietoturvan lähtökohdat

- Käyttötarkoituksen rajaaminen laissa
- Käyttö muuhun tarkoitukseen kielletty
- Tiedot poistetaan 21 vrk jälkeen
- Tiedot talletetaan Kelan palvelimelle ja pidetään Suomessa
- Tietojen käsittelyn minimointi
- Järjestelmään talletetaan ja siinä välitetään vain pseudotunnisteita, jotka on vaikea yhdistää henkilöön
- Paikkatietoja ei talleteta lainkaan
- Henkilöille ei paljasteta kohtaamisten aikaa
- Järjestelmän luotettavuus
- Tartunnat varmistetaan terveystieteiden toimesta eikä henkilö voi itse päättää lähettää varoituksia
- Tekninen tietoturva
- Kontaktitiedot talletetaan salattuna puhelimeen
- Tartunnan saaneiden tiedot talletetaan salattuna Kelan palvelimelle
- Tietoliikenneyhteydet on salattu
- Järjestelmän turvallisuus on varmistettu
- Kyberturvallisuuskeskus on arvioinut sovelluksen ja sen taustajärjestelmän tietoturvan.
- Sovelluksen lähdekoodi on julkaistu avoimena.

Lisätieto

- [Tartuntatautilaki 4 a luku](#)
- <https://www.finlex.fi/fi/laki/ajantasa/2016/20161227#L4a>
- <https://finlex.fi/fi/esitykset/he/2020/20200101?search%5Btype%5D=pika&search%5Bpika%5D=tartuntatautilaki#idp446090416>

- <https://www.slideshare.net/THLfi/koronavilkkusovellus-ja-yksityisyyden-suoja-webinaari>

- <https://koronavilkku.fi/ukk/>

Kiitos

- Ohjausosasto
- Digitalisaation ja tiedonhallinnan yksikkö



Sosiaali- ja terveydenhuollon tietojen yhteiskäyttö edistämään asiakas- ja potilasturvallisuutta ja parempaa hoivaa

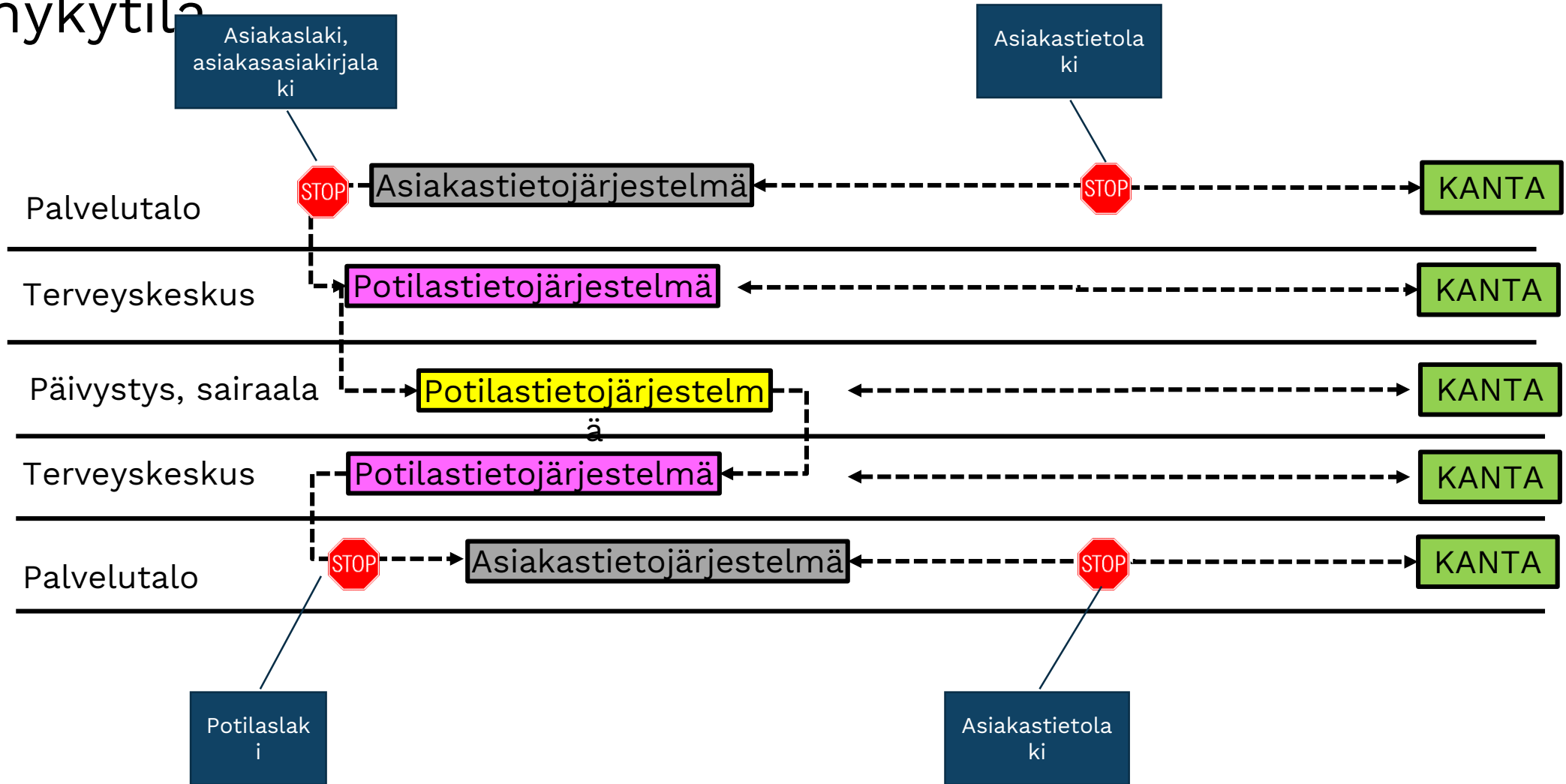
Heikki Onnela, LL

Tuotekehitysjohtaja, Apotti Oy

Nykytilan keskeisiä ongelmia

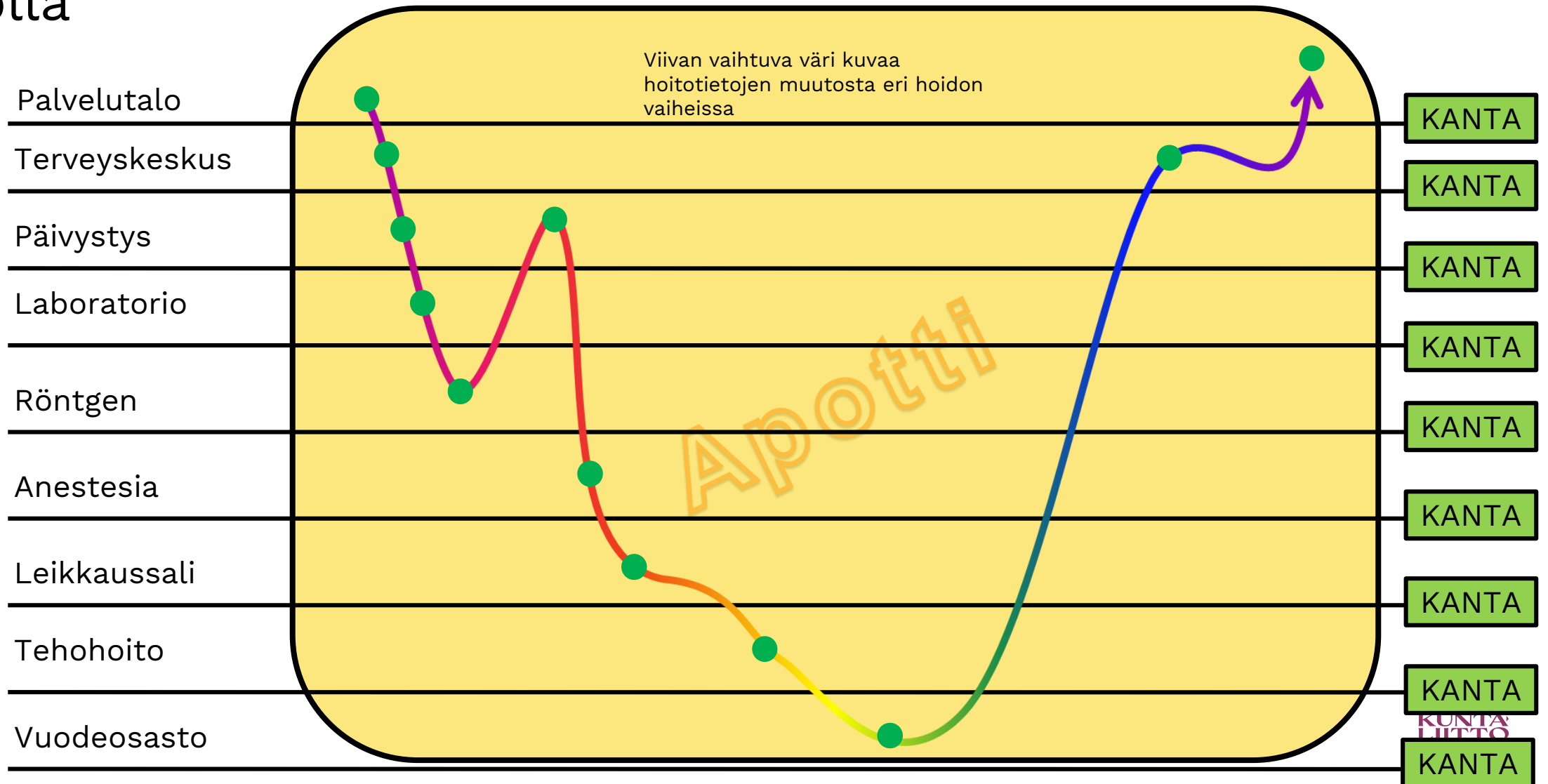
- Sosiaali- ja terveydenhuollon palveluissa toimitaan laajasti integroidusti ja palveluiden tuottamistapa on muuttunut. Säädökset elävät kuitenkin vanhaa erillistä maailmaa
- Esimerkiksi Ikäihmiset hoidetaan pääsääntöisesti sosiaalihuollon palveluissa – jossa tarjotaan sekä sosiaalihuoltoa, että terveydenhuoltoa.
- Samoin Ikäihmiset siirtyvät toistuvasti sosiaali- ja terveydenhuollon palveluiden välillä
- Vastaavia palveluja ovat mm. päihdehuolto, vammaispalvelut, lastensuojelulaitokset
- Eri säädösten salassapitosäännöt estävät ja jopa voivat potentiaalisesti vaarantaa potilaan saumattoman hoidon
- Sosiaalihuollossa syntyvät potilastiedot eivät siirry KANTA järjestelmään
 - Tiedot eivät siten ole Omakanassakaan (esim. puolesta-asiointi)
- Tällä hetkellä sosiaalihuollon terveydenhuollon henkilöstöllä ei ole pääsyä KANTA järjestelmään.
 - Oikeus on vain terveydenhuollon palvelun antajilla
- Potilaslaki 13§: tietojen luovutus terveydenhuollon toimintayksikön ulkopuolelle mahdollista käytännössä vain suostumuksella terveydenhuollon toimesta
 - HUOM! Luovutus edes suostumuksella ei ole mahdollinen sosiaalihuollon palveluun, jos ko palvelussa ei ole terveydenhuollon henkilöstöä terveydenhuollon tehtävässä.
 - ⇔ GDPR: Suostumus voi olla ongelmallinen peruste henkilötietojen käsittelylle julkisessa sosiaali- ja terveydenhuollossa. (Guidelines 05/2020 on consent under Regulation 2016/679)
- Vain sosiaalitoimella on tietyn edellytyksin oikeus sekä pyytää, että antaa potilaan hoidon turvaamiseksi välttämättömät tiedot. Terveydenhuollolla ei vastaavaa oikeutta ole, vaikka esimerkiksi potilaan saumaton lääkehoitoketju katkeaa tämän vuoksi.

Case: Ikäihminen kaatuu suihkussa palvelutalossa, nykytila



CASE Ikäihminen kaatuu palvelutalossa, miten asia pitäisi olla

● Hoitotietojen tarkistuspiste





**SOSIAALI- JA TERVEYDENHUOLLON
ATK-PÄIVÄT WEBINAARI
15.10.2020
atkpaivat.fi**

**SOSIAALI- JA TERVEYDENHUOLLON
TIETOSUOJAPÄIVÄT WEBINAARI
24.11.2020
tapahtumat.fcg.fi/sohvitellu**