



Asiakas- ja potilastietojärjestelmien käyttölokimääritys

Toimittajayhteistyökokous, Kanta-palvelut 7.4.2021

Matti Korhonen

1.4.2021

Terveysten ja hyvinvoinnin laitos

Asiakas- ja potilastietojärjestelmien käyttölokimäärittely

- Sisältö
 - Käyttölokimerkintään liittyvät periaatteet ja käsitteistö
 - Käyttölokimerkinnän tietosisällön vaatimukset
 - Käyttölokimerkinnän tietosisältö
 - Lokitietojen käsittelyn ja säilyttämisen vaatimukset
 - Raportoinnin vaatimukset
 - Lokiraporttien tietosisältö



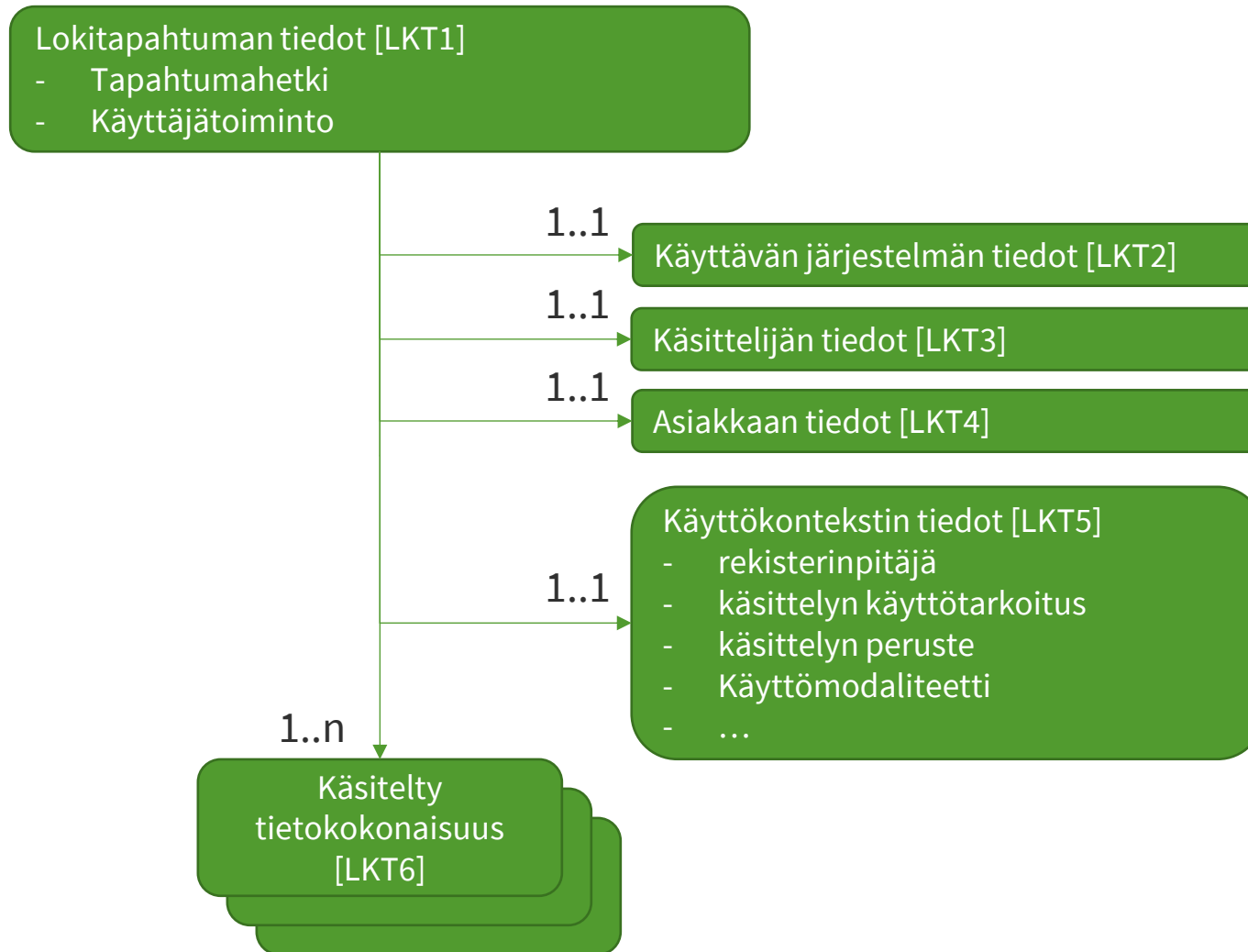
Arkaluonteisten
asiakas- ja
potilastietojen
käytön seurannassa
ja valvonnassa lokit
ovat keskeinen
väline



Käyttölokimerkintään liittyvät periaatteet ja käsitteistö

Käyttölokimerkintään liittyvät periaatteet

Yleiskuva käyttötilanteen lokittamisesta



Käyttölokimerkintään liittyvät periaatteet

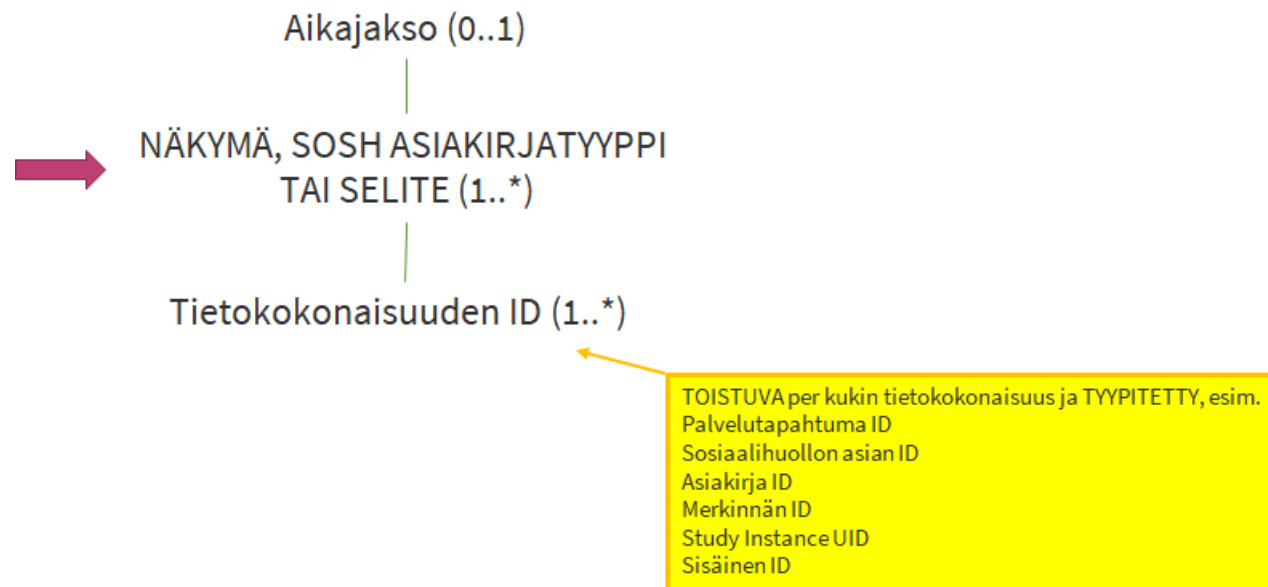
- Käyttäjätoiminto
 - Tietojen käsittelyyn kohdistuvia toimenpiteitä kuvataan tyypillisesti CRUD (Create, Read, Update, Delete) –mallilla
 - ISO 21089 –standardi
- Luokka 1
 - tietojen katselu = access
 - tietojen päivittäminen = amend
 - tietojen allekirjoittaminen tai muu todentaminen = attest
 - tietojen mitätöinti = deprecate
 - tietojen luovuttaminen = disclose
 - tietojen luominen = originate
 - tietojen toimittaminen asianomaiselle tietyssä muodossa = report
- luokka 2
 - tietojen arkistointi = archive
 - tietojen säilytysajan pidentäminen = hold
 - tietojen säilytysajan palauttaminen = unhold
 - tietojen poistaminen säilytysajan päättyessä = destroy
 - tietojen vastaanotto = receive
 - tietojen lähettäminen = transmit

Käyttölokimerkintään liittyvät periaatteet

- Käyttömodaliteetti
 - Käyttömodaliteetilla tarkoitetaan esimerkiksi tietojärjestelmään toteutettua näyttöä tai muuta vastaavaa tietojen käsittelyn mahdollistavaa käyttöliittymää.
 - henkilötason listaus
 - lista loogisesti yhteen näkymään ja yksittäiseen asiakkaaseen liittyviä tietoja
 - esimerkiksi lista yksittäisen asiakkaan ajanvarauksista
 - usean henkilön listaus
 - lista loogisesti yhteen näkymään ja useisiin asiakkaisiin liittyviä tietoja
 - esimerkiksi lista poliklinikan tulevista ajanvarauksista
 - henkilötason kooste
 - kooste loogisesti useampaan näkymään ja yksittäiseen asiakkaaseen liittyviä tietoja
 - esimerkiksi keskeisten terveystietojen kooste
 - usean henkilön kooste
 - kooste loogisesti useampaan näkymään ja useisiin asiakkaisiin liittyviä tietoja
 - esimerkiksi osaston tuotannonohjauksellinen tilannenäkymä
 - sisältö
 - yksittäisen määritettävissä olevan tietokokonaisuuden käsittely
 - esimerkiksi asiakirjan tai merkinnän lukeminen/tuottaminen
 - jne

Käyttölokimerkintään liittyvät periaatteet

- Käsittelyn kohde
 - Keskeinen osa lokimerkintää asiakas- ja potilastietojen käsittelyn kannalta on käsittelyn kohde eli tietokokonaisuus, johon toimenpide kohdistetaan





Käyttölokimerkinnän tietosisällön ja käsittelyn vaatimukset

Käyttölokin tietosisälto, tietosisällön minimivaatimukset

- Lokitapahtuman tiedot
- Käsittelijän tiedot
- Käyttävän järjestelmän tiedot
- Asiakkaan tiedot
- Käyttökontekstin tiedot
- Käsitelty tietokokonaisuus

Lokitietojen käsittelyn ja säilyttämisen vaatimukset

- Yleiset lokivaatimukset
- Käyttölokia koskevat vaatimukset
- Luovutusilmoitusta koskevat vaatimukset



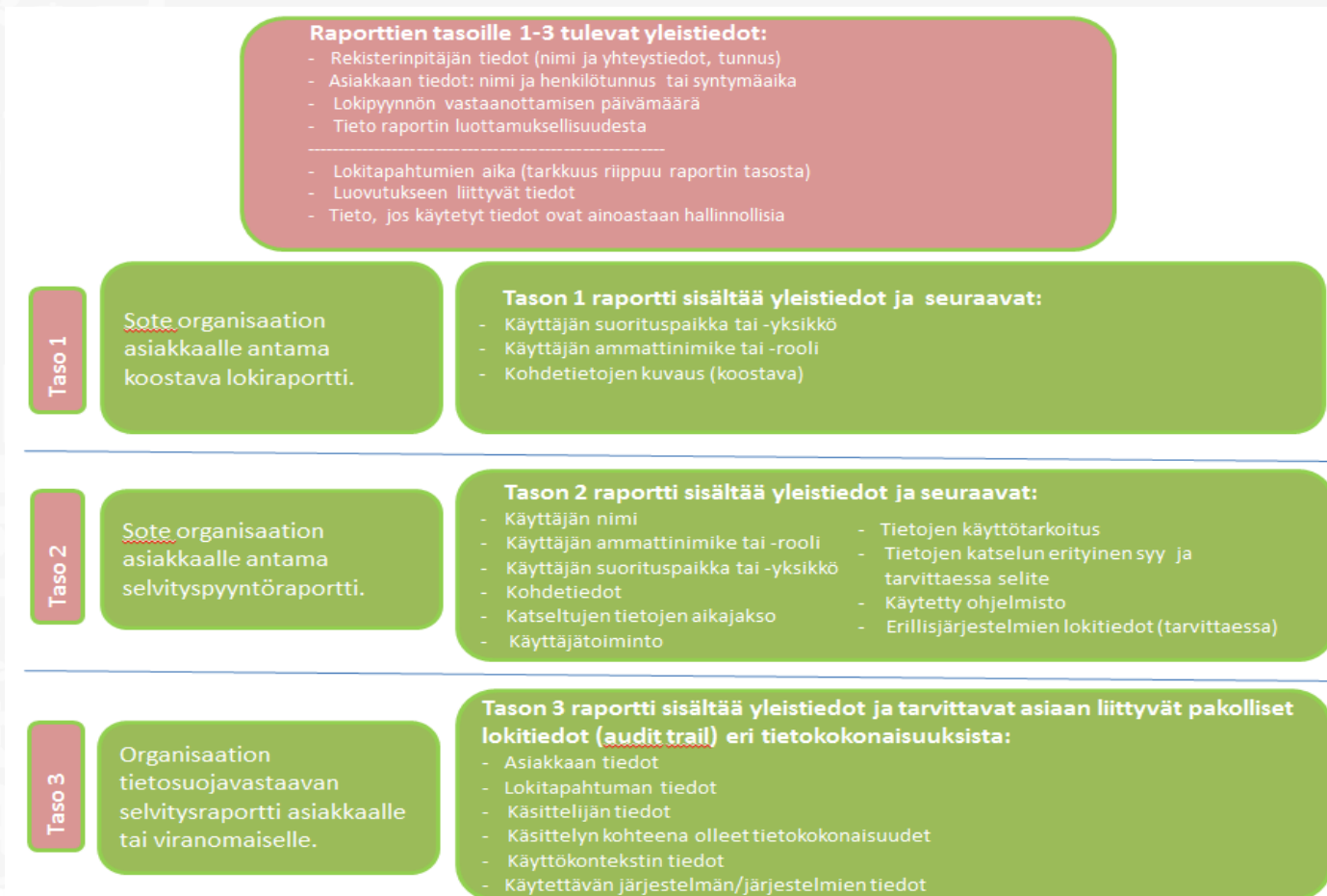
Raportoinnin vaatimukset

Raportoinnin vaatimukset

- Raportoinnin vaatimukset
 - Lokiraporttien minimitietosisältö
 - Asiakasaloitteista käytönseuranta toteutetaan vastaamalla asiakkaiden tekemiin pyyntöihin tietojen käytöstä ja näihin vastataan yleensä käyttölokiraporttien avulla (3 eri tarkkuustasoa)
 - Organisaation sisäiseen käyttöön tarkoitetut raportit tietojen käytön seurannaksi
 - Väärinkäytösten selvittämiset
 - Lokien seuranta automaattisen analysoinnin avulla
 - SIEM, Security information and event management

Raportoinnin vaatimukset

- Lokiraporttien minimietosisältö



Raportoinnin vaatimukset

Raporttien tasoille 1-3 tulevat yleistiedot:

- Rekisterinpitäjän tiedot (nimi ja yhteystiedot, tunnus)
 - Asiakkaan tiedot: nimi ja henkilötunnus tai syntymäaika
 - Lokipyynnön vastaanottamisen päivämäärä
 - Tieto raportin luottamuksellisuudesta
-
- Lokitapahtumien aika (tarkkuus riippuu raportin tasosta)
 - Luovutukseen liittyvät tiedot
 - Tieto, jos käytetyt tiedot ovat ainoastaan hallinnollisia

Taso 1

Sote organisaation
asiakkaalle antama
koostava lokiraportti.

Tason 1 raportti sisältää yleistiedot ja seuraavat:

- Käyttäjän suorituspaikka tai -yksikkö
- Käyttäjän ammattinimike tai -rooli
- Kohdetietojen kuvaus (koostava)

Raportoinnin vaatimukset

Taso 2

Sote organisaation asiakkaalle antama selvityspyyntöraportti.

Tason 2 raportti sisältää yleistiedot ja seuraavat:

- Käyttäjän nimi
- Käyttäjän ammattinimike tai -rooli
- Käyttäjän suorituspaikka tai -yksikkö
- Kohdetiedot
- Katseltujen tietojen aikajakso
- Käyttäjätoiminto
- Tietojen käyttötarkoitus
- Tietojen katselun erityinen syy ja tarvittaessa selite
- Käytetty ohjelmisto
- Erillisjärjestelmien lokitiedot (tarvittaessa)

Taso 3

Organisaation tietosuojavastaavan selvitysraportti asiakkaalle tai viranomaiselle.

Tason 3 raportti sisältää yleistiedot ja tarvittavat asiaan liittyvät pakolliset lokitiedot (audit trail) eri tietokokonaisuuksista:

- Asiakkaan tiedot
- Lokitapahtuman tiedot
- Käsittelijän tiedot
- Käsittelyn kohteena olleet tietokokonaisuudet
- Käyttökontekstin tiedot
- Käytettävän järjestelmän/järjestelmien tiedot



Kiitos!

