Liite 5. Vaatimukset potilastietojärjestelmien käyttölokeille

Arkiston turvallisuus perustuu toisaalta etukäteen tapahtuvaan käytön rajoittamiseen ja toisaalta jälkikäteen tapahtuvaan seurantaan ja valvontaan. Jälkikäteen tapahtuvan valvonnan mahdollistamiseksi järjestelmässä ylläpidetään lokeja, joihin talletetaan kaikista tapahtumista seurannan edellyttämät tiedot.

Lokeja ylläpidetään kahdella eri tasolla, kansallisessa arkistossa ja potilastietojärjestelmissä. Arkistossa ylläpidetään luovutuslokia, jonne kerätään tiedot kaikista sähköisen asiakastietolain mukaisista luovutuksista, eli rekisterinpitäjältä toiselle tapahtuvista siirroista. Paikallisissa järjestelmissä pidetään käyttölokia, jonne kerätään tiedot rekisterinpitäjän sisällä tapahtuvasta potilastietojen käytöstä.

Käytännössä lähes kaikista arkistoon liittyvistä toimenpiteistä tulee merkintä sekä luovutus- että käyttölokiin. Haettaessa toisen rekisterinpitäjän tietoja keskitetystä arkistosta paikalliseen järjestelmään tapahtuu tietojen luovutus, joka kirjataan luovutuslokiin. Terveydenhuollon ammattihenkilön käyttäessä näitä samoja tietoja se kirjataan käyttölokiin. Luovutuslokissa tämä merkitsee yhtä tapahtumaa (tiedot luovutetaan paikalliseen järjestelmään). Käyttölokissa tapahtumia voi olla useita (eri henkilöt käyttävät tietoja tai tietoja käytetään useamman kerran). Luovutusta voi pyytää henkilö, joka ei koskaan itse käytä tietoja.

Luovutuslokeja säilytetään kansallisessa arkistossa. Käyttölokit syntyvät paikallisissa järjestelmissä ja säilytetään siellä. Myös käyttölokit voidaan tulevaisuudessa toimittaa säilytettäväksi kansalliseen arkistoon. Molempiin lokeihin kansalaisilla on Asiakastietojen sähköisen käsittelyn lain 18 §:n mukainen tarkistusoikeus, jota käyttämällä kansalainen näkee kaikki itseään koskevat lokitiedot (pois lukien salassa pidettäväksi määrätyt). Lisäksi kansalaisen katseluyhteyden kautta hän näkee luovutuslokin tiedot omalta osaltaan (pois lukien luovutuksen saajan henkilötiedot). Vaikka käyttölokeja ei tällä hetkellä näytetä katseluyhteyden kautta, on niitä toteutettaessa hyvä varautua myös siihen mahdollisuuteen.

Rekisterinpitäjän potilastietojärjestelmän käyttölokin käsittely ja sisältö

Käyttölokiin talletetaan tiedot niistä tapauksista, joissa potilastietoja tai asiakirjoja käytetään rekisterinpitäjän tietojärjestelmissä. Käyttö voi kohdistua joko rekisterinpitäjän omiin tietoihin tai luovutuksella saatuihin toisen rekisterinpitäjän tietoihin. Lokeja käytetään potilastietojen käytön seurantaan ja valvontaan. Tietosisällön tulee olla sellainen, että tämä seuranta ja valvonta ovat mahdollisia, ja voi olla, että nyt esitetty tietosisältö joudutaan jatkossa vielä hiomaan lokiseurannan kehittämisen tuloksena.

Lokitietoja käytetään vain käytön seurantaan ja valvontaan. Lokitietoja pääsevät käsittelemään vain valvojat ja muut vastaavassa asemassa olevat. Lokitiedoista ilmenee vain valvontaan liittyvää tietoa. Vaikka ne sisältävät tiedon asiakirjasta, valvojat eivät näe asiakirjan sisältöä. Lokitiedot luokitellaan salassa pidettäviksi eikä niitä saa paljastaa sivullisille. Lokitiedoista voidaan haluttaessa tuottaa toimintaa kuvaavia raportteja, jotka eivät sisällä potilaan tietoja (esim. asiakirjapyyntöjä/rekisterinpitäjä/päivä). Lokitiedot on suojattava muuttumiselta ja häviämiseltä teknisen allekirjoituksen ja

varmuuskopioinnin avulla. Lokitietojen saaminen ei ole ajan suhteen kriittinen, eli lokitietoja voidaan tarvittaessa odottaa jonkin aikaa. Käyttölokin säilytysaika määritellään asetuksessa; se voi olla esimerkiksi 10 + 2 vuotta[1].

Käyttölokiin talletetaan ainakin seuraavat tiedot:
Lokitapahtuman tiedot:

- lokitapahtuman tunniste
- tapahtuman tyyppi (haku, luku, kirjoitus, päivitys, poisto)
- päivämäärä ja kellonaika (alku- ja loppuajat, loppuajankohta ei pakollinen mutta suositeltava)
- käyttävän järjestelmän tunniste (palvelimen ja työaseman tunniste)

Osapuolten tiedot

- rekisterinpitäjä, rekisteri ja tarkenne[2]
- tapahtuman palveluyksikkö
- käyttävä henkilö: nimi, ID, tunnistautumistapa ja käyttäjätunnus sekä palveluyksikkö
- käyttötarkoitus (potilaan hoito, hallinnolliset toimenpiteet)
- palvelutapahtuman tunniste

Käytetyt tiedot

- potilaan henkilötieto
- tapahtumaan liittyvä(t) tiedot(t) ja asiakirja(t)
- tieto siitä, liittyykö tapahtumaan erillisellä vahvistusvaatimuksella seurattavia tietoja

Muuta

- mahdolliset virheilmoitukset (esimerkiksi tapahtuma keskeytynyt tai käyttäjä on keskeyttänyt sen)
- käyttö on tapahtunut poikkeusperusteella ilman potilaan suostumusta (PotL 13§)
- lokitiedon salassapito (salassapidon peruste ja voimassaolo: johonkin asti tai pysyvä)
- potilashallinnon tapahtumalaji (mikäli kyse potilashallinnon tapahtumasta)
- hoitosuhteen olemassaolon todentavan lokitapahtuman tunniste (mikäli kyseessä ei ole itsessään potilashallinnon tapahtuma)
- mahdollinen erityisen syyn käyttö (syykoodi ja sen mahdollinen seliteteksti)

hallinnolliset toimenpiteet + erityinen syy, lokiseurantaa kehitetään jatkossa

Tapahtumaan liittyvät tiedot on yksilöitävä niin, että uskottava valvonta on mahdollista. Kun käyttötapahtumaan liittyy kansallisesta arkistosta luovutettu asiakirjoja, ne on yksilöitävä joko palvelutapahtuman tunnuksen tai asiakirjan tarkkuudella. Myös omassa järjestelmässä olevat asiakirjamuotoiset tiedot yksilöidään asiakirjan tarkkuudella. Mikäli paikallisessa järjestelmässä tiedot on jaettu erikoisalakohtaisesti, näkymittäin tai muulla vastaavalla tavalla, käytetään samaa jaottelua myös lokissa. Myös sellaisesta hausta, jonka tuloksena käyttäjälle ei palaudu tietoja, on jäätävä merkintä lokille. Tällöin tapahtumaan liittyvinä tietoina lokiin tallennetaan haussa käytetyt kyselyparametrit, eli se mitä yritettiin hakea.

[1] Säilytysaika muuten 10 vuotta, mutta lisäksi mahdollisten oikeustapausten käsittelyn vuoksi tähän lisätään 2 vuotta, jotta asiakirja varmasti on tallella sen ajan, jolloin sitä voidaan tarvita oikeustapauksien käsittelyssä.
[2] Esimerkiksi rekisteri=työterveyshuolto ja tarkenne=stm (työnantaja)

Potilastiedon tyypillisin käyttötarkoitus on potilaan hoito. Mikäli ei ole kyse potilaan hoidosta, merkitään käyttötarkoitukseksi hallinnolliset toimenpiteet ja tätä käyttötarkoitusta tarkennetaan erityisen syyn käytöstä annettavalla syykoodilla.

Koska järjestelmän on huolehdittava siitä, että peruste tietojen käsittelylle on olemassa, on lokiin tallennettava joko hoitosuhteen olemassaolon todentavan lokitapahtuman tunniste tai potilashallinnon tapahtumalaji, mikäli tapahtuma itsessään on potilashallinnon tapahtuma (esim. ajanvaraus tai avohoitoon kirjaus). Mikäli hoitosuhteen olemassaoloa ei voida todentaa toisen lokitapahtuman tunnisteella, eikä kyseessä ole potilashallinnon tapahtuma, vaatii tietojen käsittely erityisen syytä, jonka tiedot tallennetaan lokiin.

Lokitiedon salassapito voi perustua ainoastaan asiakastietojen sähköisen käsittelyn lain 18 §:n 2. momentissa olevilla perusteilla, joista käytännössä kyseeseen tulevat viranomaisen rikostutkintaa varten pyytämät tiedot ja tutkimuskäyttöön luovutetut tiedot. Esitutkintaa varten luovutettujen tietojen salassapito poistuu samalla tavalla kuin muissakin rekistereissä esitutkinnan päätyttyä tai määräajan kuluttua. Tutkimuskäyttöön luovutetut tiedot voivat olla pysyvästi salassa pidettäviä. Salassapidon peruste ja määräaika on ilmoitettava luovutuspyyntöasiakirjassa.