Toimintaohje Kanta-palveluihin liittyvässä henkilötietojen tietoturvaloukkauksessa ja sen epäilyssä

Apteekit ja sosiaali- ja terveydenhuolto

22.1.2019

Kela
Kanta-palvelut
PL 450, 00056 Kela

FPA
Kanta tjänsterna
PB 450, 00056 FPA

Kanta 280 01.19
www.kanta.fi
kanta@kanta.fi

Sisällysluettelo

1 Johdanto

Tämä ohje on tarkoitettu apteekin ja sosiaali- ja terveydenhuollon palvelujen antajan (jatkossa palvelujen antaja) tueksi tilanteessa, jossa Kanta-palveluihin liittyen on havaittu henkilötietojen tietoturvaloukkaus tai sen epäily. Tätä materiaalia apteekki ja palvelujen antaja voivat hyödyntää, kun laaditaan tietoturvan ja tietosuojan omavalvontasuunnitelmaa sekä erillistä toimintaohjetta.

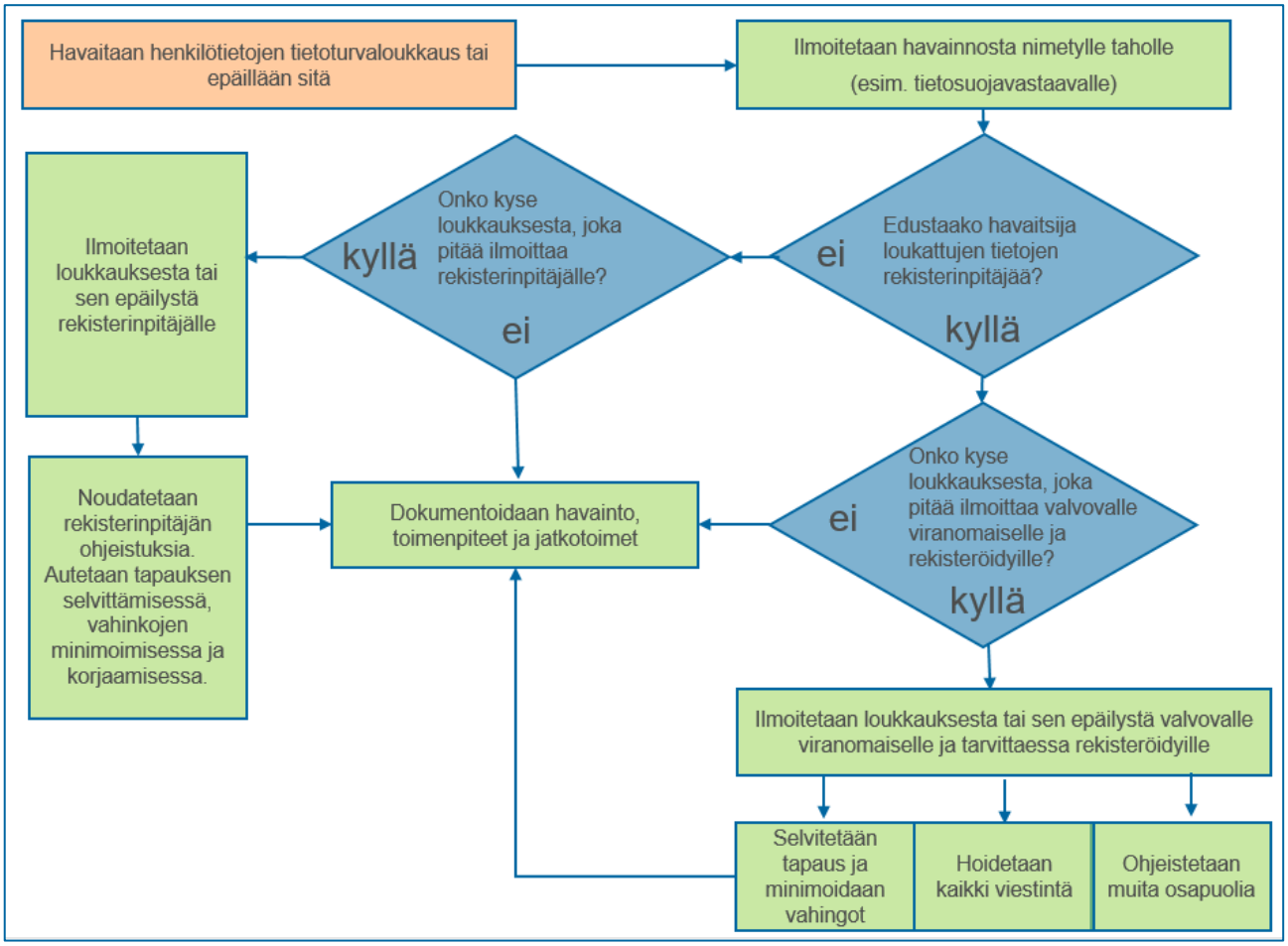
Henkilötietojen tietoturvaloukkaustapauksissa ja niiden epäilyssä noudatetaan EU:n yleistä tietosuoja-asetusta ja muita tietosuojasäännöksiä, kuten erityislainsäädäntöä. Ohjetta päivitetään uuden asiakastietolain ja lain sähköisestä lääkemääräyksetä voimaantulon jälkeen.

Henkilötietojen tietoturvaloukkauksella tarkoitetaan tapahtumaa, jonka seurauksena henkilötietoja tuhoutuu, häviää tai muuttuu, henkilötietoja luovutetaan luvattomasti tai niihin pääsee käsiksi taho, jolla ei ole käsittelyoikeutta.

Apteekin ja palvelujen antajan tulee varautua henkilötietojen tietoturvaloukkaustilanteisiin varmistamalla, että henkilöstö on tietoinen tilanteisiin liittyvästä toiminnasta ja viestinnästä.

Apteekin ja palvelujen antajan tulee lisäksi tutustua häiriötilanneohjeisiin, jotka löytyvät sekä kanta.fi- että kela.fi-verkkosivuilta.

Henkilötietojen tietoturvaloukkaustapauksessa tai sen epäilyssä toimitaan tässä ohjeistuksessa alempana olevan henkilötietojen tietoturvaloukkausprosessi -kaavion esittämän mallin mukaisesti (Kuva 1). Kaaviossa esitetyistä eri vaiheista on kirjoitettu lyhyet kuvaukset seuraavissa kappaleissa.



Kuva 1. Toimintaohje, kun havaitaan henkilötietojen tietoturvaloukkaus tai epäillään sitä

2 Henkilötietojen tietoturvaloukkauksen havaitseminen ja siitä ilmoittaminen

Henkilötietojen tietoturvaloukkaus voi tapahtua ilman teknistä häiriötä (esim. henkilötietojen urkinta) tai se voi liittyä myös järjestelmähäiriöön (esim. järjestelmä tallentaa henkilötiedon virheellisesti). Jos tietoturvaloukkaukseen liittyy järjestelmähäiriö, toimitaan sen osalta häiriötilanneohjeiden mukaisesti. Tietoturvaloukkausen osalta toimitaan tietoturvaloukkausprosessin mukaisesti.

Kun havaitaan henkilötietojen tietoturvaloukkaus tai epäillään sitä, apteekki tai palvelun antaja arvioi riskin vakavuuttaa ja sitä, pitääkö siitä ilmoittaa rekisterinpitäjälle, valvovalle viranomaiselle ja rekisteröidylle.

Apteekin ja palvelujen antajan toimintaohje henkilötietojen tietoturvaloukkauksissa tai sen epäilyssä on erilainen riippuen siitä, onko tapahtuman havaitsija henkilötietojen käsittelijä vai edustaako hän rekisterinpitäjää.

2.1 Havaitsija edustaa loukattujen henkilötietojen rekisterinpitäjää

Rekisterinpitäjä vastaa EU:n yleisen tietosuoja-asetuksen mukaisesti tapauksen selvittelystä ja viestinnästä.

Jos henkilötietojen tietoturvaloukkaus tai sen epäily vaarantaa todennäköisesti potilaan tai asiakkaan tietosuoja-asetuksessa mainittuja oikeuksia, on rekisterinpitäjän ilmoitettava asiasta tietosuojavaltuutetulle (lomakkeella) 72 tunnin kuluessa. Rekisteröidylle ilmoitus on tehtävä tarvittaessa ilman aiheetonta viivytystä.

Jos ilmoittamiskynnys ei ylity, tapaus tulee dokumentoida organisaation sisäisten ohjeiden mukaisesti.

Silloin kun Kela ei ole loukattujen henkilötietojen rekisterinpitäjä, mutta Kelan apua tarvitaan vakavan henkilötietojen tietoturvaloukkaustapauksen selvittämisessä, ollaan yhteydessä Kelan tekniseen tukeen, ks. kohta 2.3.

2.2 Havaitsija edustaa loukattujen henkilötietojen käsittelijää

Henkilötietojen käsittelijä ilmoittaa havaitsemastaan henkilötietojen tietoturvaloukkauksesta tai sen epäilystä tietojen rekisterinpitäjälle.

Reseptikeskuksen ja Tiedonhallintapalvelun (informoinnit, suostumukset, kiellot) osalta tehdään ilmoitus Kelaan. Kela vastaa rekisterinpitäjänä tapauksen selvittelystä ja viestinnästä EU:n yleisen tietosuoja-asetuksen mukaisesti. Kela tekee näiden tietojen rekisterinpitäjänä tarvittavat ilmoitukset viranomaisille ja rekisteröidylle.

2.3 Ilmoitus Kelan tekniseen tukeen

Henkilötietojen tietoturvaloukkauksesta tai sen epäilystä ilmoitetaan Kelan tekniseen tukeen puhelimitse ja/tai suojatulla sähköpostilla. Vakavasta henkilötietojen tietoturvaloukkauksesta tai sen epäilystä tulee aina ilmoittaa myös puhelimitse Kelan tekniseen tukeen.

Kelan tekninen tuki
- puhelin: 020 634 7787

Suojattu sähköposti lähetetään osoitteen https://securemail.kela.fi/posti kautta osoitteeseen tekninentuki@kela.fi. Suojatun sähköpostin lähettämisen ohje.

Kelan tekniseen tukeen ilmoitetaan
- mitä tietoja on loukattu
- miten tietoja on loukattu (esim. arkaluonteisia tietoja on joutunut asiattomien käsittelyyn)
- havainnon päivämäärä ja kellonaika
- tapahtumapaikka
- tarkka kuvaus toiminnasta tilanteessa

3 Dokumentoidaan havainto, toimenpiteet ja jatkotoimet

Henkilötietojen tietoturvaloukkaustapaus tai sen epäily dokumentoidaan. Apteekki tai palvelujen antajan tulee kirjata ylös tapahtuma, sen vaikutukset sekä tehdyt toimenpiteet riippumatta siitä, mitä jatkotoimia tietoturvaloukkauksesta lopulta seuraa.

Rekisterinpitäjälle tehdyn ilmoituksen jälkeen noudatetaan rekisterinpitäjältä saatuja toimintaohjeita sekä apteekin tai palvelujen antajan omaa ohjeistusta.

Henkilötietojen tietoturvaloukkaustapauksissa tulee kaikkien osapuolien auttaa rekisterinpitäjää tilanteen selvittämisessä, viestinnässä, vahinkojen minimoinnissa ja korjaamisessa.