

Valtakunnallisten tietojärjestelmäpalvelujen tietoturvallisuus

Asiakas- ja potilastietojen käsittelyn suoja-toimien kokonaisuus

Valtakunnallisiin tietojärjestelmäpalveluihin tallennettujen asiakastietojen käyttöä suojataan monin tavoin. Tietoturvallisuutta varmistavia toimenpiteitä tehdään Kansaneläkelaitoksen toimesta, ja lisäksi valtakunnallisiin liitettäviin asiakas- ja potilastietojärjestelmiin ja sosiaali- ja terveydenhuollon palvelunantajiin kohdistuu tietoturvallisuuteen liittyviä vaatimuksia.

Kanta-palveluiden tietoturvallisuuden varmistaminen¹

Kanta-palvelujen tiedot on suojattu monin eri tavoin, ja tietoturvan on tarkastanut ulkopuolinen tietoturvallisuuden arviointilaitos. Kannan tietoturvaa myös kehitetään jatkuvasti. Tietoturvatestauksissa otetaan huomioon kehittyvät hyökkäys- ja tietomurtomenetelmät. Sekä Kannan tietoverkot, tietokannat että sovellukset on suojattu. Kanta-palvelujen tekniset rajapinnat on suunniteltu niin, että tietosuojan ja tietoturvan vaatimukset täyttyvät tarkasti. Nämä tekniset ratkaisut suojaavat Kanta-palvelujen tietoja myös tietomurroilta.

Tietoja voi hakea vain yhdestä henkilöstä kerrallaan. Kanta-palveluissa tarkistetaan asiakas- tai hoitosuhteen olemassaolo ennen tietojen luovutusta. Terveys-huollon potilastietojen luovutuksia on tehty jo vuosia, ja hoitosuhteen varmistamisen toiminnallisuus on ollut käytössä kaiken aikaa. Hoitosuhteen varmistaminen perustuu potilastiedon arkistoon tallennettuun voimassa olevaan, tietoja hakevan palvelunantajan palvelutapah-tumaan². Omakannasta asiakas voi tarkastaa, mille palvelunantajille asiakas- ja potilastietoja on luovutettu.

Tietoturvallisuus sosiaali- ja terveydenhuollon palvelunantajien toiminnassa

Kanta-palveluihin voi liittyä ainoastaan A-luokkaan kuuluvalla sertifioidulla tietojärjestelmällä. Tietojärjestel-män tietoturvallisuusvaatimusten mukaisuus on siten arvioitu, ja arviointia tulee päivittää sertifioinnin määrä-aikojen ja uusien vaatimusten mukaisesti. Palvelunantajilta edellytetään lisäksi mm. asiakastietolain mukaista omavalvontasuunnitelmaa (lakiehdotuksessa tietoturvasuunnitelma).

Lisäksi asiakastietojen käsittelyä suojataan palvelunantajien toiminnassa eri tavoin asiakastietolain vaatimus-ten mukaisesti.

¹ [https://www.kanta.fi/tiedote/-/asset_publisher/cf6QCnduV1x6/content/kanta-palvelujen-tietoturva-on-
korkealla-tasolla](https://www.kanta.fi/tiedote/-/asset_publisher/cf6QCnduV1x6/content/kanta-palvelujen-tietoturva-on-
korkealla-tasolla)

² [Potilastiedon arkiston toiminnalliset vaatimukset sosiaali- ja terveydenhuollon tietojärjestelmille](#). Terveys-den ja hyvinvoinnin laitos 2018.

Asiakastietojen käsittelyn edellytyksenä on terveydenhuollossa hoitosuhteen tietotekninen varmistus tai muu lakiin perustuva oikeus. Lisäksi ammattihenkilöltä edellytetään vahva tunnistautuminen, kun hän kirjautuu järjestelmään.

Terveyden ja hyvinvoinnin laitoksen kuvauksessa potilastiedon arkiston toiminnallisista vaatimuksista todetaan seuraavaa:

Hoitosuhde on todennettavissa kahdella tasolla, joista ensimmäisen kohdan on toteuduttava aina, kun asiakas- ja potilastietoja käsitellään:

- 1) Palveluntarjoaja määrittelee ja valvoo, kenellä sen palveluksessa olevista ammattihenkilöistä on asiakkaaseen hoitosuhde tai muu asiallinen yhteys ja näin ollen pääsy asiakas- ja potilastietojärjestelmän tietoihin. Tämä yhteys on dokumentoitava tietojen käytön yhteydessä asiakas- ja potilastietojärjestelmän käyttölokille yhteyden todentavan potilashallinnon tapahtuman muodossa. Mikäli yhteyden perusteena oleva potilashallinnon tapahtuma on asiakas- ja potilastietoja käsittelevän ammattihenkilön itsensä kirjaama, vaaditaan lisäksi kirjaus erityisestä syystä potilastietojen katseluun.*
- 2) Haettaessa asiakas- ja potilastietoja Kanta-palveluista muutoin kuin rekisterinpitäjän omaan käyttöön, todennetaan hoitosuhde tai muu asiallinen yhteys viittaamalla Potilastiedon arkistoon tallennettuun palvelutapahtumaan. Tämä palvelutapahtuma lokitetaan kansalliselle luovutuslokille yhdessä muiden tietojen luovutukseen liittyvien lokitietojen kanssa. Tässäkin tilanteessa viittaus hoitosuhteen tai muun asiallisen yhteyden todentavaan potilashallinnon tapahtumaan on kirjattava asiakas- ja potilastietojärjestelmän käyttölokille*

Potilastietojärjestelmissä hoitosuhde ammattihenkilön ja potilaan välillä varmistetaan tarkistamalla tietojärjestelmässä, että potilaan palvelutapahtumaan liittyy myös toisen henkilön tekemä kirjaus. Lähtökohtaisesti hoitosuhteen tietoteknisen varmistamisen menettelyt perustuvat tietojärjestelmään aiemmin tallennettuihin tietoihin, koska muutoin tietoteknistä päättelyä hoitosuhteen olemassa olosta ei voi tehdä. Lakiehdotuksen perusteluissa on kuvattu malli, jonka mukaisesti hoitosuhde voidaan varmistaa samaan palvelutapahtumaan toisen henkilön tekemällä kirjauksella.

Sosiaali- ja terveystalvetuissa on kuitenkin myös erilaisia tehtäviä, joissa ammattihenkilö hoitaa tehtävää itsenäisesti, ja asiakastietojen käsittelyn tulee olla mahdollista myös näissä tilanteissa. Lakiehdotuksessa ei esitetä täsmällisiä vaatimuksia siihen, millä tavalla hoitosuhteen tietotekninen varmistaminen tulee toteuttaa. Nykyisin käytössä on toimintamalli, jossa ammattihenkilö ilmoittaa asiakastietojen käsittelyn erityisen syyn, jos hoitosuhteen varmistuksessa ei ole käytetty toisen henkilön tekemää kirjausta. Erityisen syyn koodin käyttöä on mahdollista seurata lokeilta erikseen, mikä helpottaa rekisterinpitäjän valvontavastuuta asiakastietojen asianmukaisesta käsittelystä. Myös muita esimerkiksi lakiehdotuksen perusteluissa mainittuja tapoja on mahdollista kehittää ja ottaa käyttöön.

Käyttöoikeuksilla rajataan ammattihenkilöiden pääsy niihin asiakas- ja potilastietoihin, jotka ovat kyseisessä palvelussa ammattihenkilön työtehtävän kannalta välttämättömät. Lisäksi pääsy niin sanottujen erityissuojattavien (psykiatria ja perinnöllisyyslääketiede) potilastietojen katseluun edellyttää erityistä vahvistusta, jolla ammattihenkilö vakuuttaa tietojen olevan välttämättömiä.

Kaikki asiakas- ja potilastietojen käsittely tulee lokittaa käyttölokeille.