[MÄÄRÄYS 2/2015, LIITE 1, DNRO. THL/1305/4.09.00/2014]

HouseClinic 2312390–0

OMAVALVONTASUUNNITELMA

28.02.2020 Saija Myllykoski

Sisältö

Johdanto

Sosiaali- ja terveydenhuollon palvelun antajien, apteekkien ja itsenäisten ammatinharjoittajien, Kansaneläkelaitoksen sekä Kanta-välityspalveluiden tuottajien tulee tehdä omavalvontasuunnitelma. (Määräys 2/2015, THL/1305/4.09.00/2014). Suunnitelman avulla ylläpidetään ja kehitetään organisaation tietoturvaa ja tietosuojaa.

1 Suunnitelman kohde

Tämän omavalvontasuunnitelman piiriin kuuluvat: Psykoterapiapalvelua tuottava toiminimi HouseClinic 2312390–0/Saija Myllykoski ja tätä suunnitelmaa hyödynnetään sekä omavalvonnassa että tieturvan osalta Diarium tietojärjestelmän käytössä, käytön valvonnassa, hankinnoissa ja kehitystyössä ja tähän mahdollisesti liittyvistä päätöksissä. Toiminimiyrittäjä seuraa omavalvontasuunnitelman toteutumista puolivuosittain (tilikauden päättyessä joulukuun lopussa ja kesäkuun lopussa) ja suorittaa päivittämistä tarpeen mukaan

2 Yleiset tietoturvakäytännöt

Koulutus, ohjeistus ja käyttökokemus ja niiden seuranta

HouseClinic/Saija Myllykoski sitoutuu osallistumaan tietoturvaan liittyviin koulutuksiin tarpeen vaatiessa tai ohjelmistojen muuttuessa tai kehittyessä edelleen. Oma seuranta vuosittain tilikauden päättyessä.

3 Käyttöympäristön ja useiden järjestelmien yhteiset tietoturvakäytännöt

Menettelyt virhe- ja ongelmatilanteissa

Toiminta Diarium-ohjelmaan liittyvissä virhe- ja ongelmatilanteissa

Diarium-ohjelmisto toimii Finnish Net Solutions Oy:n omistamalla palvelinlaitteistolla. Toimittaja seuraa palvelinlaitteiden toimintaa automaattisin seurantavälinen. Ohjelmistossa havaittavista virheistä ilmoitetaan viipymättä ohjelmiston tuottajan tukipalveluun. Ilmoitus voidaan tehdä sähköpostilla osoitteeseen tuki@diarium.fi tai puhelimitse numeroon 09 427 04358.

Internet-yhteyteen liittyvissä virhetilanteissa ongelmasta ilmoitetaan verkkoyhteyden tarjoavalle operaattorille, joka on dna.

Palvelinlaitteiden verkkoyhteydestä vastaa tietojärjestelmän toimittaja. Verkkoyhteys on kahdennettu siten, että toisen yhteyden vikaantuminen ei estä palvelun käyttöä. Mahdollisissa verkkoyhteyteen liittyvissä ongelmatilanteissa otetaan yhteyttä Diarium-ohjelman asiakastukeen.

Kaikista tietojärjestelmän toimintaan liittyvistä poikkeamista ilmoitetaan tietojärjestelmän toimittajalle.

Järjestelmien käyttöohjeiden hallinnointi ja saatavuus

Diarium-ohjelmiston käyttöohjeet on upotettu ohjelmiston sisään. Käyttöohjeet on toteutettu ns. inline-tyylisinä ohjeina ja video-opasteina. Käyttöohjeet ovat kaikkien käyttäjien saatavilla ja tavoitettavissa.

Käyttöohjeita päivitetään ohjelmiston toimittajan toimesta aina, kun ohjelmistoon tehdään muutoksia. Päivitykset jaetaan asiakkaalle automaattisesti.

Pääkäyttäjä vastaa uusien työntekijöiden perehdytyksestä tietojärjestelmän käyttöön. Tietojärjestelmän toimittaja tarjoaa koulutuspalveluita, joita voidaan käyttää hyödyksi henkilökunnan perehdytyksessä.

Järjestelmien asennus ja ylläpito yleisesti

Diarium-ohjelmiston asennuksesta, teknisestä ylläpidosta ja päivityksistä vastaa tietojärjestelmän toimittaja Finnish Net Solutions Oy.

Toimittaja ilmoittaa tulevasta versiopäivityksestä ennakkoon asiakkaalle. Ilmoituksessa kuvataan päivityksen mukanaan tuomat uudet ominaisuudet ja mahdolliset muutokset vanhoihin toimintoihin. Päivitysilmoituksesta selviää myös päivityksen tarkka asennusajankohta ja tieto siitä, aiheutuuko päivityksen asentamisesta käyttökatkoa. Päivitystiedotteet toimitetaan Diarium-ohjelmiston sisäiselle tiedotepalstalle, jossa ne ovat kaikkien käyttäjien saavutettavissa.

Asiakkaan vastuulle jää uusien ominaisuuksien käyttöönotto. Tietyissä tilanteissa ohjelmistoon tuodaan uusia ominaisuuksia, jotka asiakkaan pääkäyttäjä voi määrittää käyttöön haluamilleen käyttäjäryhmille.

Ylläpitotoimet vaativat teknistä osaamista ja asiantuntemusta. Tietojärjestelmän toimittaja huolehtii oman henkilöstönsä osaamisen ylläpitämisestä ja kouluttamisesta. Kaikki ylläpitotoimia tekevät henkilöt ovat saaneet riittävät koulutuksen ylläpitotoimien suorittamiseen.

Päivitys testataan huolellisesti ennakkoon ohjelmiston toimittajan toimesta. Päivitys asennetaan asiakkaille mahdollisimman rauhalliseen aikaan ja asennuksesta vastaa toimittajan koulutettu asiantuntija. Ohjelmiston päivityksen jälkeen toimittaja varautuu mahdollisiin ongelmatilanteisiin tarvittavin lisäresurssein, jolloin ongelmatilanteisiin voidaan puuttua nopeasti.

Toimittaja käyttää kehitystyössä versionhallintatyökalua, joka pitää kirjaa kaikista järjestelmään tehtävistä muutoksista. Mahdollisiin päivityksen aiheuttamiin häiriötilanteisiin on varauduttu niin, että toimittaja voi palauttaa asiakkaalle käyttöön järjestelmän edellisen toimivan version.

Tilojen, työasemien, tallennusvälineiden ja tulosteiden turvallisuus

Työasemat ja kaikki salassa pidettävä materiaali säilytetään lain edellyttämällä tavalla.

Diarium-ohjelmisto toimii Finnish Net Solutions Oy:n omistamalla palvelinlaitteistolla. Palvelintilat sijaitsevat fyysisesti Espoossa. Asiakas ottaa yhteyttä Diarium-ohjelmaan salatun Internet-yhteyden välityksellä. Palvelintila on lukittu ja kameravalvottu tila ja sinne on pääsy ainoastaan määrätyillä järjestelmän ylläpidosta vastaavilla henkilöillä.

Muut käyttöympäristön käytännöt.

Etäterapiaan käytettävä doxy.me ohjelma on erillinen, mutta tietoturvaltaan vaatimukset täyttävä etäohjelma. Käytössä tulee olemaan 2025 toukokuusta, myös Diarium- ohjelmistoon kuuluva Viivi- etäyhteysohjelma, joka vastaa tietoturvavaatimuksia

4 Käyttövaltuuksien, pääsynhallinnan ja käytön seurannan yleiset käytännöt

Käyttäjäryhmät

Diarium-ohjelman käyttäjä liitetään käyttäjäryhmään ja käyttöoikeuden määräytyvät valitun käyttäjäryhmän perusteella. Ajantasainen dokumentaatio käyttäjäryhmistä löytyy Diarium-ohjelman ylläpitotoimintojen kautta. Käyttäjäryhmiä hallitaan ”Ylläpito” -> ”Käyttäjäryhmät” -toiminnon avulla. Käyttäjäryhmiin liitetyt käyttäjät luetellaan käyttäjäryhmä-näkymään, jonka saa avattua käyttäjäryhmän nimeä klikkaamalla.

Kanta-yhteyden käyttäminen edellyttää Kanta-palvelun aktivointia asiakkaan Diarium-ohjelmaan. Aktivoinnin tekee asiakkaan pyynnöstä järjestelmätoimittaja. Kanta-yhteys aktivoidaan käyttöön asiakkaan haluamille käyttäjille.

Käyttövaltuushallinnan ja käytön seurannan käytännöt

Käyttöoikeuksia hallinnoi pääkäyttäjä. Pääkäyttäjä myöntää käyttöoikeuden järjestelmään, vastaa käyttöoikeuksien määrittämisestä ja käytön seurannasta. Käyttöoikeus myönnetään työsuhteen aloituksen yhteydessä ja käyttöoikeus poistetaan työsuhteen päättyessä. Käyttöoikeuden poisto tehdään Diarium-ohjelman käyttäjähallinnan kautta arkistointitoiminnolla.

Käyttäjätunnuksen arkistoinnin jälkeen käyttäjä ei voi käyttää ohjelmaa.

Diarium-ohjelmassa käyttäjä tunnistetaan käyttäjätunnuksen ja salasanan avulla. Pääkäyttäjä toimittaa tunnistautumistiedot käyttäjille. Käyttäjä muuttaa itse salasanan haluamakseen ohjelman salasanan vaihtotoiminnon avulla. Ohjelma varmistaa, että käyttäjä syöttää salasanaksi riittävän vahvan salasanan. Ohjema pakottaa käyttäjän vaihtamaan salasanan uudeksi 90 vuorokauden välein.

Lokitapahtumia seurataan Diarium-ohjelman lokitoiminnon avulla. Toiminto löytyy kohdasta ”Raportit” -> ”Lokitapahtumat”.

Lainvastaisesta asiakas- ja potilastietojen käsittelystä ilmoitetaan viipymättä viranomaisille ja tietojärjestelmän toimittajalle.

Kanta-yhteyteen liittyvät tapahtumat kirjataan erilliseen lokiin. Lokitapahtumia seurataan ”Raportit” -> ”Kanta-loki”. Lokiin kirjataan kaikki Kanta-arkistoon tehtävät lähetykset, haut ja virhetilanteet.

5 Kanta-palvelujen käytön tietoturvakäytännöt

Pääkäyttäjä vastaa siitä, että Kanta-palveluita käyttävä henkilö (Saija Myllykoski) on perehdytetty ja koulutettu palvelujen käyttämiseen.

Kanta-palveluiden käyttäjä tunnistetaan aina ennen palveluiden käyttöä terveydenhuollon varmenteella käyttäjän omalta toimikortilta. Palveluiden käyttö estetään, jos varmenne ei ole voimassa tai henkilöllä ei ole ammattioikeutta.

Kanta-palveluita käyttävällä henkilöllä tulee olla Väestörekisterikeskuksen myöntämä terveydenhuollon käyttöön tarkoitettu toimikortti.

Kanta-yhteyteen liittyvät tapahtumat kirjataan erilliseen lokiin. Lokitapahtumia seurataan ”Raportit” -> ”Kanta-loki”. Lokiin kirjataan kaikki Kanta-arkistoon tehtävät lähetykset, haut ja virhetilanteet.

Kanta-palveluiden käyttäjä tunnistetaan aina ennen palveluiden käyttöä terveydenhuollon varmenteella käyttäjän omalta toimikortilta. Palveluiden käyttö estetään, jos varmenne ei ole voimassa tai henkilöllä ei ole ammattioikeutta.

Sosiaalihuollon ja terveydenhuollon dokumentit eritellään palvelutapahtumakohtaisesti. Diariumissa hoitojakson perustiedoissa valitaan rekisteri, johon dokumentti tallennetaan. Vain terveydenhuollon dokumentteja voi lähettää Kanta-arkistoon.

Diarium-järjestelmän toimittaja Finnish Net Solutions Oy on toimittanut vaatimuksenmukaisuustodistuksen.

Poikkeustilanteessa järjestelmätoimittaja sulkee liityntäpisteen, jonka jälkeen liikenne Diarium-järjestelmän ja Kanta-palveluiden välillä keskeytyy. Liityntäpisteen sulkemisen jälkeen Diarium-ohjelma toimii normaalisti, mutta kommunikointi Kanta-palveluiden kanssa on estetty. Järjestelmätoimitta pyrkii omilla toimillaan ratkaisemaan ongelmatilanteen mahdollisimman nopeasti, jonka jälkeen liityntäpiste voidaan ottaa jälleen käyttöön.

6 Tietojärjestelmät

Ohjelmisto: Diarium
Toimittaja: Finnish Net Solutions Oy
Yhteystiedot: Tekniikantie 12, 02150 Espoo, tuki@diarium.fi, puh. 09 427 04358
Vaatimuksenmukaisuustodistus: FI160613-21

7 Tietojärjestelmäkohtaiset ohjeet ja suunnitelmat

8.1 Järjestelmä X (luokkaan A kuuluva)

Ohjelmisto: Diarium 1.1.21
Toimittaja: Finnish Net Solutions Oy
Yhteystiedot: Tekniikantie 12, 02150 Espoo, tuki@diarium.fi, puh. 09 427 04358
Vaatimuksenmukaisuustodistus: FI160613-21
Käyttötarkoitus: Potilasrekisteri, ajanvaraus ja laskutustoiminnot.
Käyttäjäryhmät: Kaikki yrityksen työntekijät