T:mi Puheterapeutti Kaisa Penttilä

Tietoturvasuunnitelma

Versio 1.0. Päivitetty 7.12.2024

Laatijana Kaisa Penttilä

Yrityksen omistaja, Puheterapeutti, FM, 7.12.2024

Tämä asiakirja on tarkoitettu ylle kirjatun tietoturvasuunnitelman kohteen yksinomaiseen käyttöön. Tätä asiakirjaa ei saa levittää ulkopuolisille, eikä käyttää sellaisenaan hyödyksi yrityksen ulkopuolella. Asiakirja voidaan tarvittaessa luovuttaa valvovien viranomaisten perehdyttäväksi tai muuhun vastaavaan rajattuun käyttöön, kuten esimerkiksi tietosuojan, lupaehtojen tai sopimusehtojen mukaiseen auditointiin.

Tämän tietoturvasuunnitelman pohjana on käytetty Suomen Kuntoutusyrittäjät ry:n ja Nordhealth Oy:n yhdessä laatimaa mallia, jonka perustana on puolestaan THL:n 23.3.2024 julkaistu tietoturvasuunnitelman mallipohja.

Sisällys

1. Tietoturvasuunnitelman käyttötarkoitus

THL:n määräyksen 3/2024 (THL/4/4.05.00/2024) liitteenä on tämä **tietoturvasuunnitelman mallipohja**, joka on tietoturvallisuuden omavalvonnan kohteiden **tietoturvasuunnitelman laatimisen tueksi** tarkoitettu **esimerkinomainen dokumenttipohja**.

Mallipohja ei jokaiselta yksityiskohdaltaan, muun muassa esimerkeiltään ole täysin yksi yhteen THL:n määräyksen 3/2024 kanssa – oleellista on tiedostaa, että **THL:n määräys 3/2024 on velvoittava**; mallipohja ei itsessään voi suoraan tätä ollakaan, koska tietoturvasuunnitelmien laatijoita, tietoturvallisuuden omavalvonnan kohteita on hyvin erikokoisia ja erilaisia – organisaatioita, jotka tekevät monentyyppistä toimintaa sosiaali- ja terveydenhuollossa tai siihen liittyen.

Tietoturvasuunnitelmaa tulee katselmoida ja/tai päivittää säännöllisesti. Tietoturvasuunnitelman laadinnan ja noudattamisen vastuu on sosiaali- ja

Mallipohjasta on THL:n määräyksen 3/2024 liitteeksi laadittu ainoastaan tämä yksi versio. Kooltaan ja toiminnaltaan hyvinkin erilaiset sote-palvelunantajat voivat soveltaa tai täydentää mallipohjaa omaan toimintaansa peilaten. Oleellista on täyttää asiakastietolain 703/2023 77 §:n 1 ja 2 mukaiset velvoitteet.

Tämä dokumentti on T:mi puheterapeutti Kaisa Penttilän tietoturvasuunnitelma. Tämän

tietoturvasuunnitelman käyttötarkoitus on täyttää asiakastietolain 703/2023 77 §:n 1 ja 2 momentin ja THL:n määräyksen 3/2024 mukaiset velvoitteet. Suunnitelma kokoaa yhteen palvelunantajalta, välittäjältä ja Kansaneläkelaitokselta edellytettävät selvitykset ja vaatimukset.

Ennen 1.11.2021 voimaan tulleen asiakastietolain 784/2021 voimaantuloa käytössä ollut vanhan asiakastietolain 159/2007 mukainen omavalvontasuunnitelma vastasi pääosin sisällöltään tietoturvasuunnitelmaa. Tietoturvasuunnitelma korvasi omavalvontasuunnitelman THL:n määräyksen 3/2021 mukaisesti. Nyt kyse on THL:n määräyksen 3/2024 tultua voimaan omavalvonnan kohteen käytössä olevien tietoturvasuunnitelmien päivittäminen määräyksen mukaiseksi.

Tämä tietoturvasuunnitelma päivitetään tarpeen mukaan, tai vähintään vuosittain maaliskuussa. Tarkempi päivittämissuunnitelma löytyy kohdasta 2. [Määritä aikataulu oman tarpeen mukaan, kuitenkin vähintään kerran vuodessa.]

2. Tietoturvasuunnitelman kohde ja päivityskäytännöt

Tämän tietoturvasuunnitelma koskee yritystä:

Nimi: T:mi puheterapeutti Kaisa Penttilä

Y-tunnus: 1996608-3

Vastuuhenkilö/johtaja: Kaisa Penttilä

Toimipaikat/palveluyksiköt: Vanhantullinkatu 2, 2 krs. 90310 Oulu

Suunnitelman piiriin kuuluvat sopimuskumppanit: Pohde ja Kela

Suunnitelman toteuttamisessa ja päivittämisessä noudatetaan seuraavia käytäntöjä:

Suunnitelman ja sen päivittämisen vastuuhenkilö: Kaisa Penttilä

Suunnitelman toteuttamisen vastuuhenkilöt: Kaisa Penttilä

Katselmointi- ja päivityskäytännöt: Kaisa Penttilä on vastuussa suunnitelman ajantasaisuudesta. Suunnitelma päivitetään vuosittain joulukuun loppuun mennessä. Tämän lisäksi suunnitelmaa tarkastellaan ja päivitetään aina uusia tietojärjestelmiä tai laitteita hankittaessa sekä esimerkiksi muutettaessa toiseen toimipisteeseen.

Suunnitelman seuranta ja seurannan dokumentointi: Tietoturvasuunnitelman ylläpitämisestä vastaa Kaisa Penttilä. Tietoturvasuunnitelman viimeisin päivitys merkitään suunnitelman ensimmäiselle sivulle. Suunnitelmaan tehdyistä muutoksista ei pidetä erillistä muutoslokia, mutta suunnitelman vanhat versiot tallennetaan yrityksen

tietojärjestelmään.

Suunnitelman käyttö tietojärjestelmien hankinnoissa ja päivityksissä: Hankittaessa käyttöön uusia tietosuojaan vaikuttavia järjestelyjä kuten pilvipalveluita, potilastietojärjestelmiä, asiakashallintajärjestelmiä tai asiakirjojen hallintajärjestelmiä, selvitetään tämän suunnitelman käytännön toteuttaminen uusissa tietojärjestelmissä. Tarvittaessa suunnitelmaa täydennetään tai muutetaan yhteensopivaksi uusien tietojärjestelmien kanssa siten,että tietosuoja- ja tietoturvavaatimukset täyttyvät.

Päätös suunnitelman hyväksymisestä ja käyttöönotosta: Kaisa Penttilä hyväksyy suunnitelman ja suunnitelman käyttöönoton, myös päivitysten jälkeen.

3. Yleiset tietoturvakäytännöt

T:mi puheterapeutti Kaisa Penttilä yrityksessä noudatetaan seuraavia yleisiä tietoturvakäytäntöjä ja tehdään tietoturvallisuus-, tietosuoja-, riskienhallinta- ja asiakastietojen käsittelyn omavalvontatyötä seuraavien dokumenttien mukaisesti:

Tietoturvallisuustyötä tehdään seuraavien dokumenttien mukaisesti:

Henkilötietojen käsittelyssä noudatetaan aina salassapitomääräyksiä. Henkilötiedot kirjataan Diarium-potilastietojärjestelmään tai Pohteen ylläpitämään Palse järjestelmään. Potilastietojärjestelmän tietoturvasta vastaa ylläpitäjä Nordhealth, Palsen tietoturvasta Pohde. Yrityksen tietokeneeseen on asennettu F-Secure virustorjuntaohjelma mikä päivitetään säännöllisesti. Muistitkuilla olevat potilastiedot säilytetään yrityksen aina lukittuna olevan toimistotilan lukitun kaapin sisällä olevassa kassakaapissa. Kassakaapin koodi on ainoastaan Kaisa Penttilän tietdossa. Kirjallisessa muodossa olevat henkilötiedot käsitellään asianmukaisesti ja säilytetään lukollisessa arkistokaapissa yrityksen aina lukitussa olevassa toimistohuoneessa. Arkistokaapin ja toimistohuoneen avaimet ovat ainoastaan Kaisa Penttilän käytössä.

Yrityksessä henkilötietoja ei käsitellä muilla digitaalisilla alustoilla kuin ainoastaan Diarium-potilastietojärjestelmällä, Pohteen tarjoaman Palse yhteyden kautta sekä Kelan lähettämien salattujen sähköpostin kautta. Henkilötiedot tallennetaan ainoastaan Diariumiin ja Palseen. Kelan lähettämän salatun sähköpostin kautta tulleet asiakirjat tallennetaan Diariumiin minkä jälkeen sähköpostit tuhotaan.

Yritykselle on laadittu laatukäsikirja.

Tietosuojavastaavana toimii: Kaisa Penttilä

4. Menettelyt virhe- ja ongelmatilanteissa sekä jatkuvuudenhallinta

Poikkeustilanteisiin varautumisessa ja jatkuvuuden suunnittelussa noudatetaan seuraavia toimintatapoja

Mikäli potilastietojärjestelmä Diariumissa tai Pohteen Palse järjestelmässä havaitaan ongelmia, otetaan yhteys välittömästi järjestelmän ylläpitäjään.

Mikäli yrityksen omassa tietokoneessa havaitaan tietoturvaa heikentävä toiminto, häiriö tai muu vatstaava tilanne, selvitetään asia alan ammattilaisen kanssa.

Mikäli tietojärjestelmä ei väliaikaisesti toimi, kirjataan asiakastiedot ja puheterapiakuntoutukseen liittyvät tiedot paperille ja paperit säilytetään lukitussa arkistokaapissa sen ajan kun potilastietojärjestelmä saadaan toimimaan. Paperille kirjatut henkilötiedot siirretään potilastietojärjestelmään ja sen jälkeen henkilötietoja sisältävät paperit tuhotaan silppurissa.

Virhe- ja ongelmatilanteissa sekä niistä toipumisessa noudatetaan seuraavia toimintatapoja:

Mikäli potilastietojärjestelmä ei toimi tai siinä havaitaan poikkeamia tai virheitä, otetaan yhteys Diarium:in tukeen tai Pohteen yhteyshenkilöön.

Yrityksen tietokeneen virustorjuntaohjelma (F-Secure) päivitetään säännöllisesti. Tietokeen selaushistoria poistetaan säännöllisesti, vähintään kaksi kertaa viikossa.

Mikäli virus- tai haittaohjelma tai tietojen kalastelua havaitaan yrityksen tietokoneessa, tietokoneen virus- tai haittaohjelma poistamiseen ostetaan palvelu Taitonetti Oy:sta. Tietojen kalastelun havaitsemisen yhteydessä torjutaan yhteydenotot eikä avata mitään linkkejä yms.

Jos asiakkaiden henkilötietoja tai kuntoutukseen liityviä tietoja on vuotanut sivullisille, syy selvitetään ja korjataan välittömästi. Tietojen vuotamisesta tiedotetaan myös asianomaisille välittömästi. Tietojen vuotamisesta ilmoitetaan myös Tietosuojavaltuutetulle ja Valviralle.

Diarium-potilastietojärjestelmä

Diarium-potilastietojärjestelmän vikatilanteista vastaa järjestelmän toimittaja Nordhealth Finland Oy. Ongelmatilanteissa tuki palvelee arkipäivisin 8-16 numerossa 09 4255 0329 ja sähköpostiosoitteessa tuki@diarium.fi.

Diarium-potilastietojärjestelmän valvonnasta, huollosta ja päivityksistä vastaa järjestelmän toimittaja Nordhealth Finland Oy. Päivitykset tapahtuvat noin kuukausittain ja niiden aikataulu ja sisältö ilmoitetaan Diarium-ohjelman sisäisellä tiedotteella ennen päivitystä. Päivitys aiheuttaa lyhyen käyttökatkon. Lisäksi korjauksia tehdään tarpeen mukaan myös muina aikoina. Tällaiset korjaukset eivät aiheuta käyttökatkoa.

Mikäli Diarium-potilastietojärjestelmässä havaitaan tietoturva- tai tietosuojauhka tai ongelma, järjestelmän toimittaja ilmoittaa siitä välittömästi.

Nordhealth Connect -asiointipalvelu

Yrityksellä ei ole käytössä Nordhealth Connect -asiointipalvelua. Mikäli palvelu otetaan käyttöön, palvelua koskevat alla olevat tiedot.

Nordhealth Connect -asiointipalvelun vikatilanteista vastaa järjestelmän toimittaja Nordhealth Finland Oy. Ongelmatilanteissa tuki palvelee arkipäivisin 8-16 sähköpostiosoitteessa connect-support@nordhealth.com.

Asiointipalvelun valvonnasta, huollosta ja päivityksistä vastaa järjestelmän toimittaja Nordhealth

Finland Oy. Päivityksistä ja niiden sisällöstä ilmoitetaan erillisellä tiedotteella ennen päivitystä. Päivitys aiheuttaa lyhyen käyttökatkon. Lisäksi korjauksia tehdään tarpeen mukaan myös muina aikoina. Tällaiset korjaukset eivät aiheuta käyttökatkoa.

Mikäli Nordhealth Connect -asiointipalvelussa havaitaan tietoturva- tai tietosuojauhka tai ongelma, järjestelmän toimittaja ilmoittaa siitä välittömästi.

nordhealth.fi -portaali

Yrityksellä ei ole käytössä Nordhealth.fi -portaalia. Mikäli palvelu otetaan käyttöön, palvelua koskevat alla olevat tiedot.

Nordhealth.fi -portaalin vikatilanteista vastaa järjestelmän toimittaja Nordhealth Finland Oy. Ongelmatilanteissa tuki palvelee arkipäivisin 8-16 sähköpostiosoitteessa tuki@diarium.fi.

Nordhealth.fi -portaalin valvonnasta, huollosta ja päivityksistä vastaa järjestelmän toimittaja Nordhealth Finland Oy. Päivityksistä ja niiden sisällöstä ilmoitetaan erillisellä tiedotteella ennen päivitystä. Päivitys aiheuttaa lyhyen käyttökatkon. Lisäksi korjauksia tehdään tarpeen mukaan myös muina aikoina. Tällaiset korjaukset eivät aiheuta käyttökatkoa.

Mikäli nordhealth.fi -portaalissa havaitaan tietoturva- tai tietosuojauhka tai ongelma, järjestelmän toimittaja ilmoittaa siitä välittömästi.

Yrityksen toimipisteen tietoliikenteeseen liittyvät virhetilanteet

Mikäli potilastietojärjestelmä ei toimi tai siinä havaitaan poikkeamia tai virheitä, otetaan yhteys Diarium:in tukeen tai Pohteen yhteyshenkilöön.
Yrityksen tietokeneen virustorjuntaohjelma (F-Secure) päivitetään säännöllisesti. Tietokeen selaushistoria poistetaan säännöllisesti, vähintään kaksi kertaa viikossa.

Mikäli virus- tai haittaohjelma tai tietojen kalastelua havaitaan yrityksen tietokoneessa, tietokoneen virus- tai haittaohjelma poistamiseen ostetaan palvelu Taitonetti Oy:sta. Tietojen kalastelun havaitsemisen yhteydessä torjutaan yhteydenotot eikä avata mitään linkkejä yms.

Jos asiakkaiden henkilötietoja tai kuntoutukseen liityviä tietoja on vuotanut sivullisille, syy selvitetään ja korjataan välittömästi. Tietojen vuotamisesta tiedotetaan myös asianomaisille välittömästi. Tietojen vuotamisesta ilmoitetaan myös asianmukaisesti tilanteen vaativalla tavalla joko tietosuojavaltuutetulle ja Valviralle.

Kaikki yrityksessä henkilötietoja käsittelevien järjestelmien tunnukset ovat Kaisa Penttilän hallussa eikä niitä luovuteta eteenpäin.

Luokan A tai luokan B järjestelmien merkittävistä poikkeamista ilmoitetaan Valviralle ja tietosuojavaltuutetun toimistolle, jos poikkeama aiheuttaa merkittävän riskin potilasturvallisuudelle tai tietoturvalle.

5. Yrityksen ostajan koulutus ja osaaminen sekä tietojärjestelmien käyttöohjeet ja tietoturvallinen käyttäminen

5.1. Henkilökunnan koulutus sekä osaamisen ylläpito ja kehittäminen

Yrityksen omistaja ja ainut työntekijä ostaa tietojärjestelmien käyttöön ja tietoturvaan liittyviä koulutuksia aina tarpeen mukaan.

Tähän mennessä käydyt koulutukset:

Diarium potilasteitojärjestelmän käyttöönottokoulutus

Ohjeita tietoturvaan koulutus, Diarium 10.12.2024

Kantaan liittyminen-koulutus, Diarium 19.12.2024

Asiakas- ja potilastietojen käsittelyn, tietojärjestelmien käytön sekä tietosuojan ja tietoturvan toteuttamisen koulutuksissa, ohjeistuksissa ja seurannassa toimitaan seuraavasti:

Diarium-potilastietojärjestelmä

Diarium-potilastietojärjestelmän koulutus on toteutunut järjestelmän toimittajan toimesta ohjelman käyttöönoton yhteydessä.

Nordhealth Connect -asiointipalvelu

Nordhealth Connect -asiointipalvelun alustava koulutus tapahtuu järjestelmän toimittajan toimesta ohjelman käyttöönoton yhteydessä.

T:mi puheterapeutti Kaisa Penttilä ei käytä tällä hetkellä Nordhealth Connect-asiointipalvelua. Mikäli kyseinen palvelu otetaan käyttöön, yrityksen omistaja ja ainut työntekijä käy koulutukset joissa perehdytään suraaviin asiohin:

-Asiakas- ja potilastietojen käsittelyn toimintamallit/-tavat (mm. asiakkaiden ja potilaiden informointi, tietopyyntöihin vastaaminen, tietojen luovuttaminen jne.

-Lisäksi Tietojärjestelmien ja niiden uusien versioiden käyttökoulutus ja perehdytys sekä osaamisen säännöllinen ylläpito.

5.2. Tietojärjestelmien käyttöohjeet ja ohjeiden mukainen käyttö

Tietojärjestelmien käyttöohjeiden hallinnassa, saatavuudessa ja ohjeiden mukaisessa käytössä toimitaan seuraavasti:

Diarium-potilastietojärjestelmä

Diarium-ohjelmiston käyttöohjeet on upotettu ohjelmiston sisään. Käyttöohjeet on toteutettu ns.

inline-tyylisinä ohjeina, verkkokoulutuksena ja video-opasteina. Käyttöohjeet ovat kaikkien käyttäjien saatavilla ja tavoitettavissa.

Diarium-ohjelmiston käyttöohjeita päivitetään ohjelmiston toimittajan toimesta aina, kun ohjelmistoon tehdään muutoksia. Päivitykset jaetaan asiakkaalle automaattisesti.

Nordhealth Connect -asiointipalvelu

Nordhealth Connect -asiointipalvelun käyttöohjeet toimitetaan tilauksen yhteydessä. Tarvittaessa ne voi pyytää uudelleen tuesta. Käyttöohjeet on toteutettu ns. inline-tyylisinä ohjeina ja verkkokoulutuksena.

Nordhealth Connect - asiointipalvelun käyttöohjeita päivitetään ohjelmiston toimittajan toimesta aina, kun ohjelmistoon tehdään muutoksia. Päivitykset jaetaan asiakkaalle automaattisesti.

nordhealth.fi **-portaali**

nordhealth.fi -portaalin käyttöohjeet toimitetaan tilauksen yhteydessä. Tarvittaessa ne voi pyytää uudelleen tuesta. Käyttöohjeet on toteutettu ns. inline-tyylisinä ohjeina ja verkkokoulutuksena.

nordhealth.fi -portaalin käyttöohjeita päivitetään ohjelmiston toimittajan toimesta aina, kun ohjelmistoon tehdään muutoksia. Päivitykset jaetaan asiakkaalle automaattisesti.

Kaisa Penttilä noudattaa Diariumin, Pohteen ja Kelan kaikkia tietoturvaa koskevia ohjeistuksia ja toimii niiden mukaisesti.

6. Tietojärjestelmien tietoturvakäytännöt

6.1. Tietojärjestelmien perustiedot, kuvaukset ja olennaisten vaatimusten täyttyminen

T:mi puheterapeutti Kaisa Penttilä käyttää seuraavaia henkilötietoja käsitteleviä tietojärjestelmiä:

-Nordhealth Finland Oy:n Diarium-potilastietojärjestelmää, joka vastaa kyseisen järjestelmän valvonnasta, huollosta ja päivityksistä.

-Pohteen ylläpitämää Palse-portaalia minkä ylläpidosta kokonaisuudessaan vastaa Pohde.

Sekä Diariumin ja Palsen kautta tapahtuvaa Kanta-yhteyttä.

6.1.1. Kanta-palveluihin liittyvät tietojärjestelmät (luokat A2 ja A3)

Ohjelmisto: Diarium
Toimittaja: Nordhealth Finland Oy
Yhteystiedot: Albertinkatu 25, 00180 Helsinki,
tuki@diarium.fi, puh. +358 9 425 50329
Vaatimuksenmukaisuustodistus: FI210617-84

Ohjelmisto: Palse-portaali, versio 3.0.158C

Toimittaja: Pohde/ Polycon Oy
Yhteystiedot: Pohde, Kajaanintie 50, 90220 Oulu
Puhelinnro/ Vaihde: 083152011

6.1.2. Muut järjestelmät, joille on tehty tietoturvallisuuden ulkoinen arviointi (luokka A1)

Yrityksellä ei ole käytössä muita järjestelmiä

6.1.3. Muut asiakastietoja käsittelevät järjestelmät (luokka B)

Ohjelmisto: Nordhealth Connect
Toimittaja: Nordhealth Finland Oy
Yhteystiedot: Albertinkatu 25, 00180 Helsinki
connect-support@nordhealth.com, +358 75 325 7594

Ohjelmisto: Nordhealth.fi
Toimittaja: Nordhealth Finland Oy
Yhteystiedot: Albertinkatu 25, 00180 Helsinki
tuki@diarium.com, +358 9 425 50329

6.1.4. Muut tietojärjestelmät, jotka on otettava huomioon arkaluonteisten asiakastietojen suojaamisen kannalta

Yrityksellä ei ole käytössä muita asiakastietoja käisttteleviä järjestelmiä.

6.1.5. Tietojärjestelmien olennaisten vaatimusten täyttyminen

Kaikissa tietojärjestelmäsopimuksissa edellytetään järjesttelmiltä jatkuvaa ylläpitoa ja yhteensopivuutta Suomessa ja Euroopan Unionissa voimassa olevan lainsäädännön kanssa. Sopimusehtojen mukaisesti hankittujen asiakastietojärjestelmien on koko sopimuskauden ajan täytettävä lainsäädännön ja Kanta-palveluidenkaupallisille potilas- ja asiakashallintaohjelmille esittämät vaatimukset.

Tietojärjestelmien vaatimustenmukaisuuden voimassaolo tarkistetaan yrityksissä vuosittain tammikuun loppuun mennessä avaamalla Valviran hyväksymien tietojärjestelmien rekisterilinkki ja etsimällä käytetyt potilas- ja asiakastietojärjestelmät luettelosta. Jos tietojärjestelmää ei löydy luettelosta, otetaan viipymättä yhteys järjestelmätuottajaan

Linkki tietojärjestelmärekisteriin.

6.2. Tietojärjestelmien asennus, ylläpito ja päivitys

Tietojärjestelmien asennuksissa, ylläpidossa ja päivityksissä noudatetaan seuraavia toimintatapoja:

Diarium-potilastietojärjestelmä

Diarium-ohjelmiston asennuksesta, teknisestä ylläpidosta ja päivityksistä vastaa tietojärjestelmän toimittaja Nordhealth Finland 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 tai jotka tulee erikseen tilata järjestelmän toimittajalta.

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.

Nordhealth Connect -asiointipalvelu

Nordhealth Connect -asiointipalvelun asennuksesta, teknisestä ylläpidosta ja päivityksistä vastaa tietojärjestelmän toimittaja Nordhealth Finland 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.

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

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.

Nordhealth,fi -portaali

nordhealth.fi -portaalin asennuksesta, teknisestä ylläpidosta ja päivityksistä vastaa tietojärjestelmän toimittaja Nordhealth Finland 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.

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

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.

Palse-portaalin ylläpidosta ja päivityksestä vastaa Pohde.

6.3. Käyttövaltuuksien hallinnan ja tunnistautumisen käytännöt

Yrityksen T:mi puheterapeutti Kaisa Penttilä tietojärjestelmiä ja tietokonetta käyttää vain Kaisa Penttilä.

Diarium-potilastietojärjestelmä ja Palse-portaali
Käyttäjä Kaisa Penttilä

Nordhealth Connect -asiointipalvelu

Ei ole yrityksen käytössä. Mikäli otetaan käyttöön, käyttäjä Kaisa Penttilä.

nordhealth.fi -portaali

Ajantasainen listaus käyttäjistä löytyy nordhealth.fi -portaalista.

Käyttäjä Kaisa Penttilä, portaalia käytetään yrityksen tietokoneen kautta.

Diarium-potilastietojärjestelmä

Diarium-potilastietojärjestelmää käyttää ja hallinnoi Kaisa Penttilä “Ylläpito” -> “Käyttäjät” toimintojen kautta. Järjestelmän ylläpitokäyttäjä on vastuussa järjestelmän käytöstä ja käyttäjätunnusten salassapitämisestä. Tarvittaessa Diarium-tuki voi lähettää käyttäjälle uuden, kertakäyttöisen salasanan ennalta määriteltyyn, henkilökohtaiseen puhelinnumeroon.

Nordhealth Connect -asiointipalvelu

Mikäli yritys ottaa käyttöön Nordhealth Connect -asiointipalvelun, hallinto-, pää- ja ylläpitokäyttäjänä toimii Kaisa Penttilä.

nordhealth.fi **-portaali**

nordhealth.fi -portaalin yritysprofiilin pääkäyttäjä Kaisa Penttilä hallinnoi yritysprofiilin tietoja ja käyttöoikeuksia.

Käyttäjien tunnistautumisessa ja todentamisessa noudatetaan seuraavia käytäntöjä:

Diarium-potilastietojärjestelmä

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

Diarium-potilastietojärjestelmässä on myös mahdollista ottaa käyttöön kaksivaiheinen tunnistautuminen. Tällöin käyttäjätunnuksen ja salasanan lisäksi käyttäjää pyydetään 7-10 päivänä välein tai aina uudelta laitteelta kirjauduttaessa antamaan kertakäyttöinen, tekstiviestitse toimitettu vahvistuskoodi.

Kaksivaiheinen tunnistautuminen ei ole T:mi puheterapeutti Kaisa Penttilä käytössä.

Nordhealth Connect -asiointipalvelu

Nordhealth Connect -asiointipalvelussa käyttäjä tunnistetaan käyttäjätunnuksen ja salasanan avulla. Ylläpitokäyttäjä toimittaa tunnistautumistiedot käyttäjille. Käyttäjä muuttaa itse salasanan haluamakseen ohjelman salasanan vaihtotoiminnon avulla. Ohjelma varmistaa, että käyttäjä syöttää salasanaksi riittävän vahvan salasanan. Ohjelma pakottaa käyttäjän vaihtamaan

salasanan uudeksi 90 vuorokauden välein.

Nordhealth Connect -asiointipalvelussa on lisäksi mahdollista ottaa käyttöön vahva tunnistautuminen, jolloin uuden käyttäjän tulee tunnistautua käyttäen vahvaa tunnistautumista, esim. pankkitunnuksia, ennen asiointipalvelun käyttöönottoa.

Yrityksellä ei ole käytössä Nordhealth Connect-asiointipalvelua.

nordhealth.fi **portaali**

nordhealth.fi -portaalissa käyttäjä tunnistetaan käyttäjätunnuksen ja salasanan avulla. Profiilin luoja luo salasanan profiilin luonnin yhteydessä. Ohjelma varmistaa, että käyttäjä syöttää salasanaksi riittävän vahvan salasanan. Ohjelma pakottaa käyttäjän vaihtamaan salasanan uudeksi 90 vuorokauden välein.

Yrityksellä T:mi puheterapeutti Kaisa Penttilä ei ole käytössä nordhealth.fi portaalia.

6.4. Asiakas- ja potilastietojärjestelmien pääsynhallinnan ja käytön seurannan käytännöt

Asiakastietoja käsitteleviä järjestelmiä käyttää ainoastaan Kaisa Penttilä joten pääsynhallintaa ja käytön seurantaa ei toteuteta.

7. Tietojärjestelmien käyttöympäristön tietoturvakäytännöt

7.1. Fyysinen turvallisuus osana tietojärjestelmien käyttöympäristön turvallisuutta

Fyysisestä turvallisuudesta osana tietoturvallisuuden varmistamista huolehditaan asiakastietojen ja tietojärjestelmien käyttöympäristössä seuraavasti:

Yrityksen toimisto sijaitsee osoitteessa Vanhantullinkatu 2, 90100 Oulu. Toimistotila on lukittu, avaimet ovat Kaisa Penttilän hallussa. Kaikki henkilötietojen käsittely tapahtuu lukitussa toimistotilassa, ikkunat on peitetty lamelliverhoilla joita pidetään kiinni. Toimistotilaan ei ole näköyhteyttä eikä kulkulupaa ulkopuolisille. Yrityksen tietokonetta käyttää ainoastaan Kaisa Penttilä. Kaikki yrityksen toimintaa vaativat salasanat ovat Kaisa Penttilän tiedossa. Salasanat on kirjattu muistiin erilliselle paperille suljettuun kirjekuoreen, kirjekuori on yrityksen kassakaapissa. Kassakaapin avauskoodi on Kaisa Penttilän puolison tiedossa. Poikkeustilanteen vaatiessa Kaisa Penttilän puolisolla on oikeus avata kassakaappi ja luovuttaa salasanat tarvittaessa viranomaiselle, jolla on oikeus avata asiakastiedot.

Kaisa Penttilä on rekisterinpitäjänä vastuussa kaikista henkilötietojen lainmukaisesta säilyttämisestä. Ennen Diarium-potilastietojärjestelmän käyttöönottoa laaditut kirjalliset aisiakastiedot on arkistitoitu yrityksen lukitun toimiston arkistokaappiin,minkä avaimet ovat Kaisa Penttilän hallussa. Henkilötietoja sisältävät muistitikut säilytetään toimiston lukitun kaapin sisällä olevassa kassakaapissa. Kassakaapin avauskoodi on ainoastaan Kaisa Penttilän tiedossa ja poikkeustilanteita varten puolison Jaakko Penttilän tiedossa.

7.2. Työasemien, mobiililaitteiden ja käyttöympäristön tukipalveluiden hallinta

Työasemien, mobiililaitteiden ja käyttöympäristön tukipalveluiden tietoturvallisuudesta

huolehditaan seuraavasti:

Henkilötietoja käsitellään ainoastaan yrityksen tietokoneella missä on F-securen virustorjuntaohjelma. Virustorjuntaohjelma päivitetään uuteen välittömästi vanhan version käyttöajan loputtua.

7.3. Alusta- ja verkkopalvelujen tietoturvallinen käyttö tietosuojan ja varautumisen kannalta

Yrityksellä T:mi puheterapeutti Kaisa Penttilä ei ole käytössä Alusta- ja verkkopalveluita. Ainoastaan nettiyhteyden jakaminen iPhonen kautta mikä on suojattu salasanalla.

8. Kanta-palvelujen liittymisen ja käytön tietoturvakäytännöt

Kanta-palvelujen osalta noudatetaan seuraavia tietoturvakäytäntöjä ja asiakastietojen käsittelyn käytäntöjä:

Diarium-potilastietojärjestelmä

Diarium-potilastietojärjestelmässä Kanta-yhteyttä käytetään kirjautumalla ensin järjestelmään ja tunnistautumalla sitten henkilökohtaisella ammatti- tai toimijakortilla. Kaisa Penttilä on käynyt Diariumin tarjoaman Kanta-toimintojen koulutuksen 5.12. ja 19.12.2024.

Tarkemmin Kanta-palveluiden liittymisen ja käytön tietoturvakäytännöt on kuvattu kohdassa: 6. Tietojärjestelmien tietoturvakäytännöt

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

9. Tietojärjestelmäkohtaiset tarkemmat kuvakset, ohjeet ja suunnitelmat

T:mi puheterapeutti Kaisa Penttilän käytössä on vain yksi tietojärjestelmä. Tarkemmat kuvaukset tietojärjestelmistä käyttötarkoituksista on tehty kohdassa 6.1.

9.1. Järjestelmät, luokkiin A2 ja A3 kuuluvat

Tarkemmat kuvaukset tietojärjestelmistä käyttötarkoituksista on tehty kohdassa 6.1.

9.2. Järjestelmät, luokkaan A1 kuuluvat

Tarkemmat kuvaukset tietojärjestelmistä käyttötarkoituksista on tehty kohdassa 6.1.

9.3. Järjestelmät, luokkaan B kuuluvat

Yrityksellä T:mi puheterapeutti Kaisa Penttilällä ei ole käytössä luokkaan B kuuluvia tietojärjestelmiä

9.4. Järjestelmät, muut järjestelmät, jotka eivät kuulu luokkiin A tai B

Yrityksellä T:mi puheterapeutti Kaisa Penttilällä ei ole käytössä muita tietojärjestelmiä jotka eivät kuulu luokkiin A tai B luokkaan B kuuluvia tietojärjestelmiä

lähteitä:

Traficomin Kyberturvallisuuskeskuksen kybermittari – Työkalu organisaatioiden kyberturvallisuuden arviointiin ja kehittämiseen: https://www.kybermittari.fi/

Julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri), Suositus ja kriteeristö (6/2023): https://julkaisut.valtioneuvosto.fi/handle/10024/165015

Tietosuojavaltuutetun toimisto – Henkilötietojen siirrot Euroopan talousalueen ulkopuolelle: https://tietosuoja.fi/henkilotietojen-siirrot-etan-ulkopuolelle

Kyberturvallisuuskeskus – Sosiaali- ja terveydenhuollon hankintojen tietoturva- ja tietosuojavaatimukset: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/sosiaali-ja-terveydenhuollon-hankintojen-tietoturva-ja]

- Digi- ja väestötietovirasto 12/2022 – Digitaalisen turvallisuuden arkkitehtuuri -viitekehys: https://wiki.dvv.fi/display/DTARK/]