

Toimintaterapia ArkiTaito y: 2764869-1

Tietoturvasuunnitelma

[Päivitetty viimeksi 12.7.2025]

Hanna-Mari Kariaho

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 Kuntoutusyritykset ry:n ja Nordhealth Oy:n yhdessä laatimaa mallia, jonka perustana on puolestaan THL:n 20.12.2021 julkaiseman tietoturvasuunnitelman malli.

Sisälllys

1. Tietoturvasuunnitelman käyttötarkoitus	3
2. Tietoturvasuunnitelman kohde ja päivityskäytännöt	4
3. Yleiset tietoturvakäytännöt	5
4. Menettelyt virhe- ja ongelmatilanteissa sekä jatkuvuudenhallinta	5
5. Henkilöstön koulutus ja osaaminen sekä tietojärjestelmien käyttöohjeet ja tietoturallinen käyttäminen	6
5.1. Henkilöstön koulutus sekä osaamisen ylläpito ja kehittäminen	6
5.2. Tietojärjestelmien käyttöohjeet ja ohjeiden mukainen käyttö	7
6. Tietojärjestelmien tietoturvakäytännöt	7
6.1. Tietojärjestelmien perustiedot, kuvaukset ja olennaisten vaatimusten täyttyminen	7
6.1.1. Kanta-palveluihin liittyvät tietojärjestelmät (luokat A2 tai A3)	8
6.1.2. Muusta syystä tietoturva-auditoidut tietojärjestelmät (luokka A1)	8
6.1.3. Muut asiakastietoja käsittelevät järjestelmät (luokka B)	8
6.1.4. Muut tietojärjestelmät, jotka on otettava huomioon arkaluonteisten asiakastietojen suojaamisen kannalta	8
6.1.5. Tietojärjestelmien olennaisten vaatimusten täyttyminen	8
6.2. Tietojärjestelmien asennus, ylläpito ja päivitys	8
6.3. Käyttövaltuuksien hallinnan ja tunnistautumisen käytännöt	9
6.4. Asiakas- ja potilastietojärjestelmien pääsynhallinnan ja käytön seurannan käytännöt	10
7. Tietojärjestelmien käyttöympäristön tietoturvakäytännöt	11
7.1. Fyysinen turvallisuus osana tietojärjestelmien käyttöympäristön turvallisuutta	11
7.2. Työasemien, mobiililaitteiden ja käyttöympäristön tukipalveluiden hallinta	12
7.3. Alusta- ja verkkopalvelujen tietoturallinen käyttö tietosuojan ja varautumisen kannalta	12
8. Kanta-palvelujen liittymisen ja käytön tietoturvakäytännöt	14

1. Tietoturvasuunnitelman käyttötarkoitus

Tämä dokumentti on Toimintaterapia Arkitaidon tietoturvasuunnitelma. Tämän tietoturvasuunnitelman käyttötarkoitus on täyttää 1.11.2021 voimaan tulleen asiakastietolain¹ 784/2021 27 §:n ja THL:n määräyksen 3/2021 mukaiset velvoitteet. Suunnitelma kokoaa yhteen asiakastietolaissa vaaditut kaikilta sote-palveluntuottajilta edellytettävät tietosuojaan liittyvät 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. Näin ollen kyse on THL:n määräyksen 3/2021 tultua voimaan omavalvonnan kohteen käytössä olevien omavalvontasuunnitelmien päivittämisestä uusiksi tietoturvasuunnitelmiksi.

Tietoturvasuunnitelmaa tulee päivittää säännöllisesti kerran vuodessa. Tietoturvasuunnitelman laadinnan ja noudattamisen vastuu on sosiaali- ja terveydenhuollon palveluntarjoajan vastaavalla johtajalla.

Tämä tietoturvasuunnitelma päivitetään tarpeen mukaan, tai vähintään vuosittain helmikuussa. Tarkempi päivittämissuunnitelma löytyy kohdasta 2.

2. Tietoturvasuunnitelman kohde ja päivityskäytännöt

Tämän tietoturvasuunnitelman piiriin kuuluvat:

- Nimi: Toimintaterapia ArkiTaito
- Y-tunnus: 2764869-1
- Vastuuhenkilö/johtaja: Hanna-Mari Kariaho
- Toimipaikat: Härkikuja 1a, Hämeenkyrö

Suunnitelman toteuttamisessa ja päivittämisessä noudatetaan seuraavia käytäntöjä:

- Suunnitelman ja sen päivittämisen vastuuhenkilö: Hanna-Mari Kariaho
- Suunnitelman toteuttamisen vastuuhenkilöt: Hanna-Mari Kariaho
- Tarkistus- ja päivityskäytännöt: Suunnitelma päivitetään vuosittain helmikuun loppuun mennessä. Tämän lisäksi suunnitelmaa tarkastellaan ja päivitetään aina uusia tietojärjestelmiä tai laitteita hankittaessa sekä esimerkiksi muutettaessa toiseen toimipisteeseen. Jokainen työntekijä ja yhteistyökumppani veloitetaan perehtymään suunnitelmaan yhteistyön alkaessa ja suunnitelman päivittyessä.
- Suunnitelman seuranta ja seurannan dokumentointi: Tietoturvasuunnitelman ylläpitämisestä vastaa yrityksen tietosuojavastaava. Tietoturvasuunnitelman viimeisin päivitys merkitään suunnitelman ensimmäiselle sivulle. Suunnitelmaan tehdyistä muutoksista ei pidetä erillistä muutoslokiä, mutta suunnitelman vanhat versiot tallennetaan erilliseen kansioon.
- Suunnitelman käyttö tietojärjestelmien hankinnoissa ja päivityksissä: Hankittaessa käyttöön uusia tietosuojan vaikuttavia järjestelmiä (kuten pilvipalveluita, potilastietojärjestelmiä, asiakashallintajärjestelmiä tai asiakirjojen hallintajärjestelmiä) suoritetaan tarpeen mukaisesti tietosuojan vaikutustenarviointi (DPIA, data protection impact assessment) ja selvitetään joka tapauksessa tämän suunnitelman käytännön toteuttaminen uusissa tietojärjestelmissä. Tarvittaessa suunnitelmaa täydennetään tai muutetaan yhteensopivaksi uusien tietojärjestelmien kanssa siten, että tietosuoja- ja tietoturva-vaatimukset täyttyvät.

¹ <https://www.finlex.fi/fi/laki/ajantasa/2021/20210784>

- Uusia laitteita käyttöön otettaessa, niihin asennetaan tietosuojaohjelmisto.

3. Yleiset tietoturvakäytännöt

Toimintaterapia ArkiTaidossa noudatetaan seuraavia yleisiä tietoturvakäytäntöjä ja tehdään tietoturvallisuus-, tietosuoja-, riskienhallinta- ja asiakastietojen käsittelyn omavalvontatyötä seuraavien dokumenttien mukaisesti:

- Vaiheittainen toimintaohje, kun havaitaan tietoturvaloukkaus
- Vaiheittainen toimintaohje, kun yritykselle esitetään tietopyyntö tai pyyntö tehdä korjaus, muutos tai poistaminen henkilötietoihin
- Jos kyse on tietomurrosta, toimintaohje täällä: [TietomurtoToimintaohje.pdf](#) ([kyberturvallisuuskeskus.fi](#))
- laatukäsikirja
- Erilliset toimintaohjeet ja koulutusmateriaali (Diarium)

Tietosuojaavastaavana toimii: Hanna-Mari Kariaho

4. Menettelyt virhe- ja ongelmatilanteissa sekä jatkuvuudenhallinta

[**Määräys 3/2021**: 6.2 Menettelyt virhe- ja ongelmatilanteissa sekä jatkuvuuden hallinta]

[Tietoturvasuunnitelman laatimisessa voi tässä luvussa tarvittaessa hyödyntää eOppivan aineistoja: <https://www.eoppiva.fi/koulutukset/turvaa-digitaalinen-toiminta-hairiotilanteissa>]

Poikkeustilanteisiin varautumisessa ja jatkuvuuden suunnittelussa noudatetaan seuraavia toimintatapoja:

- Varautumis ja jatkuvuussuunnitelma
- Poistumisharjoitukset
- normaalista poikkeavat olosuhteet, lyhyt- ja pitkäkestoiset häiriöt, poikkeusolosuhteet
- varautuminen toimintaan poikkeustilanteissa ilman tietojärjestelmiä ja/tai alusta- ja verkkopalveluita

Virhe- ja ongelmatilanteissa noudatetaan seuraavia toimintatapoja:

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

Nordhealth Connect -asiointipalvelun vikatilanteista vastaa järjestelmän toimittaja Nordhealth Finland Oy. Ongelmatilanteissa tuki palvelee arkipäivisin 8-16 sähköpostiosoitteessa health@navisechealth.fi.

Navisec Heath -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.

Yrityksen toimipisteen tietoliikenteeseen liittyvät virhetilanteet

- verkko- tai tietoliikenneongelmat, mobiiliverkko, suojattu salasanalla, Elisa Oy

5. Henkilöstön koulutus ja osaaminen sekä tietojärjestelmien käyttöohjeet ja tietoturvallinen käyttäminen

5.1. Henkilöstön koulutus sekä osaamisen ylläpito ja kehittäminen

Henkilöstön kouluttaminen tietosuoja-asoiden osalta on erittäin tärkeää. Henkilöstön tulee osata hoitaa työtehtäviään tietosuojan periaatteita noudattaen

Asiakastietojen käsittelyn, tietojärjestelmien käytön sekä tietosuojan ja tietoturvan toteuttamisen koulutuksissa, ohjeistuksissa ja seurannassa toimitaan seuraavasti:

Diarium-potilastietojärjestelmä

Diarium-potilastietojärjestelmän alustava koulutus tapahtuu järjestelmän toimittajan toimesta ohjelman käyttöönoton yhteydessä.

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

Nordhealth Connect -asiointipalvelu

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

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

- Terveystietojen asiakastietojen ja potilastietojen käsittelyn toimintamallien/-tapojen koulutuksesta ja perehdytyksestä (esim. asiakkaiden ja potilaiden informointi, tietopyyntöihin vastaaminen jne) on kuvattu työntekijöiden perehdytysohjeessa.
- Tietojärjestelmien ja niiden uusien versioiden käyttökoulutuksesta ja perehdytyksestä sekä osaamisen säännöllisestä ylläpidosta erilaisissa työtehtävissä ja rooleissa suunnitellaan ennen järjestelmän hankintaa järjestelmätuottajan ohjeiden mukaisesti.
- Tietosuoja- ja tietoturva koulutukset tai kouluttautuminen toteutetaan erillisen koulutussuunnitelman mukaisesti (Laatukansiossa)
- Koulutukset arkistoidaan, työntekijöiltä edellytetään todistusta tai koulutuksen jälkeen onnistuneesti suoritettua testiä.
- Pääsääntöisesti työnteon edellytyksinä olevista koulutuksista, joihin työnantaja edellyttää työntekijöidensä osallistuvan, vastaa kaikista kuluista työnantaja.

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.

- Ohjeet ovat saatavilla suoraan käyttöjärjestelmästä, jonka lisäksi ohjeistuksesta kertominen ja siihen perehtyminen kuuluu uuden työntekijän perehdytykseen. Käyttöohjeet ovat käytettävissä suoraan verkon kautta tietojärjestelmän muun käytön yhteydessä. Käyttöohjeet päivittyvät automaattisesti palveluntuottajan toimesta.
- Uusia työntekijöitä perehdytetään nimeämällä tälle määrääjäksi tukihenkilö, joka voi olla joko esimies tai työkaveri.

6. Tietojärjestelmien tietoturvakäytännöt

6.1. Tietojärjestelmien perustiedot, kuvaukset ja olennaisten vaatimusten täyttyminen

Kuvaukset käytössä olevista tietojärjestelmistä ja siitä, millaisia käytäntöjä asiakastietojen käsittelyn, tietosuojan ja tietoturvallisuuden toteuttamisessa ja seurannassa noudatetaan näitä tietojärjestelmiä käytettäessä:

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

Ohjelmisto: Diarium

Toimittaja: Nordhealth Finland Oy

Yhteystiedot: Aleksanterinkatu 30-34, 00100 Helsinki,
tuki@diarium.fi, puh. +358 9 425 50329

Vaatimuksenmukaisuustodistus: FI210617-84

6.1.3. Muut asiakastietoja käsittelevät järjestelmät (luokka B) (Käytössä olevat ei kanta-yhteensopivat tai vanhat potilastietojärjestelmät, päivitetään sitä mukaa kun järjestelmiä luokitellaan uuden asiakastietolain mukaisesti)

Ohjelmisto: Nordhealth Connect

Toimittaja: Nordhealth Finland Oy

Yhteystiedot: Aleksanterinkatu 30-34, 00100 Helsinki

6.1.5. Tietojärjestelmien olennaisten vaatimusten täyttyminen

- Kaikissa tietojärjestelmäsopimuksissa edellytetään järjestelmiltä jatkuvaa ylläpitoa ja yhteensopivuutta Suomessa ja Euroopan Unionissa voimassa olevan lainsäädännön kanssa. Sopimusehtojen mukaisesti hankittujen asiakastietojärjestelmien on koko sopimuskauden ajan täytettävä lainsäädännön ja Kanta-palveluiden kaupallisille 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. Linkki tietojärjestelmärekisteriin löytyy tältä sivulta. Jos tietojärjestelmää ei löydy luettelosta, otetaan viipymättä yhteys järjestelmätuottajaan.

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. Päivytysilmoituksesta 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 ennakoon 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 ennakoon 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 ennakoon 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.

6.3. Käyttövaltuuksien hallinnan ja tunnistautumisen käytännöt

Tietojärjestelmien ja laitteiden käyttäjiä ja käyttäjäryhmiä hallinnoidaan seuraavasti:

Diarium-potilastietojärjestelmä

Ajantasainen listaus Diarium-potilastietojärjestelmän käyttäjistä ja käyttäjäryhmistä löytyy Diarium-potilastietojärjestelmästä.

Nordhealth Connect -asiointipalvelu

Ajantasainen listaus käyttäjistä löytyy Nordhealth Connect -asiointipalvelusta.

Käyttöoikeuksien ja käyttövaltuuksien osalta noudatetaan seuraavia toimintatapoja:

Diarium-potilastietojärjestelmä

Diarium-potilastietojärjestelmän ylläpitokäyttäjät hallinnoivat käyttäjiä kohdan "Ylläpito" -> "Käyttäjät" toimintojen kautta. Järjestelmän ylläpitokäyttäjät ovat vastuussa uusien käyttäjien luomisesta, käyttäjätunnusten ja salasanojen toimittamisesta käyttäjille sekä poistuvien käyttäjien arkistoisesta.

Tarvittaessa myös Diarium-tuki voi lähettää käyttäjälle uuden, kertakäyttöisen salasanan ennalta määriteltyn, henkilökohtaiseen puhelinnumeroon.

Diarium-potilastietojärjestelmässä käyttäjä liitetään käyttäjäryhmään ja käyttöoikeuden määräytyvät valitun käyttäjäryhmän perusteella. Ajantasainen dokumentaatio käyttäjäryhmistä löytyy Diarium-ohjelman ylläpitotoimintojen kautta. Käyttäjäryhmiä hallitaan "Ylläpito" -> "Käyttäjäryhmät" -toiminnoilla avulla. Käyttäjäryhmiin liitettyt käyttäjät luetaan käyttäjäryhmä-näkymään, jonka saa avattua käyttäjäryhmän nimeä klikkaamalla.

Diarium-ohjelman käyttäjäryhmien ja yksittäisten käyttäjien oikeuksista vastaavat järjestelmän ylläpitokäyttäjät.

Ylläpitokäyttäjät ovat:

Nordhealth Connect -asiointipalvelu

Nordhealth Connect -asiointipalvelun hallinto-, pää- ja ylläpitokäyttäjät hallinnoivat henkilökunta- ja asiakaskäyttäjien käyttäjätunnuksia ja käyttöoikeuksia. Asiointipalvelun peruskäyttäjät hallinnoivat asiakaskäyttäjien käyttäjätunnuksia ja käyttöoikeuksia.

Nordhealth Connect -tuki pystyy tarvittaessa lisäämään palveluun henkilökuntakäyttäjän.

Asiointipalvelun käyttäjäryhmät on valmiiksi määriteltäviä ohjelmaan, eikä niitä voi muokata.

- Yrittäjä vastaa

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 haluamukseen ohjelman salasanan vaihtotoiminnon avulla. Ohjelma varmistaa, että käyttäjä syöttää salasanan 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.

Nordhealth Connect -asiointipalvelu

Nordhealth Connect -asiointipalvelussa käyttäjä tunnistetaan käyttäjätunnuksen ja salasanan avulla. Ylläpitokäyttäjä toimittaa tunnistautumistiedot käyttäjille. Käyttäjä muuttaa itse salasanan haluamukseen ohjelman salasanan vaihtotoiminnon avulla. Ohjelma varmistaa, että käyttäjä syöttää salasanan 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 asiantipalvelun käyttöönottoa.

Vahva tunnistautuminen on käytössä

- Toimikortti säilytetään turvallisesti, yrittäjällä ja alihankkijalla on avaimet tilaan. Tietokoneeseen vaaditaan salana, jonka vain yrittäjä tietää. Salasanat vaihdetaan vähintään 90 päivän välein. Mobiililaitteet on myös suojattu salasanoin ja pin-koodein.

Asiakastietoja käsittelevien järjestelmien pääsynhallintaa ja käytön seuranta toteutetaan seuraavasti:

Diarium-potilastietojärjestelmä

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-potilastietojärjestelmässä käyttäjä tunnistetaan käyttäjätunnuksen ja salasanan avulla. Pääkäyttäjä toimittaa tunnistautumistiedot käyttäjille. Käyttäjä muuttaa itse salasanan haluamukseen ohjelman salasanan vaihtotoiminnon avulla. Ohjelma varmistaa, että käyttäjä syöttää salasanan riittävän vahvan salasanan. Ohjelma 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.

- Ainoastaan yrittäjällä on pääsy potilastietojärjestelmään
- Vaikka joku pääsisi tietokoneelle, ei siinä ole suoraa linkkiä potilastietojärjestelmään
- Tietokoneen lokitiedot pyyhitään jokaisen käyttökerran jälkeen
- Tietokoneessa on vahva suojausohjelmisto, jota päivitetään säännöllisesti (F-secure total)

7. Tietojärjestelmien käyttöympäristön tietoturvakäytännöt

7.1. Fyysinen turvallisuus osana tietojärjestelmien käyttöympäristön turvallisuutta

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

Käyttöympäristöstä huolehditaan erillisen henkilöstön tietoturvaohjeen mukaisesti.

- Toimitilat ovat lukossa, aina kun paikalla ei ole henkilökuntaa. Toimistohuone, jossa tietokonetta säilytetään, on aina lukossa.
- Toimitilassa ei säilytetä tietokoneita, vaan kannettava tietokone on yrittäjän mukana
- Istunnon aikakatkaisu on 2 min, jonka jälkeen näyttö lukittuu ja avaamiseen tarvitaan salasana, joka on vain yrittäjän tiedossa.
- Vain yrittäjällä on oikeus asentaa ohjelmistoja ja sovelluksisia laitteille, muut eivät pääse laitteille.
- Yrityksellä on muistitikku, johon varmuuskopioidaan yrityksen yleisiä tietoja, ei asiakastietoja
- tulostin sijaitsee toimitilassa, se ei ole yhteydessä internetiin.
- Arkistoitavia asiakastietoja tai potilastietoja sisältävien paperitulosteiden säilyttäminen tapahtuu toimitilassa paloturvallisesti lukittuna ja suojassa sivullisilta, ne hävittää silppuamalla ja polttamalla siten, etteivät sivulliset pääse tietoihin
-

7.2. Työasemien, mobiililaitteiden ja käyttöympäristön tukipalveluiden hallinta

Työasemien, mobiililaitteiden ja käyttöympäristön tukipalveluiden tietoturvallisuudesta huolehditaan seuraavasti:

- Tietokoneisiin, tabletteihin, matkapuhelimiin ja muihin asiakas- ja potilastietoja käsitteleviin mobiililaitteisiin on hankittu virustorjunnan mahdollistava ohjelmisto. Käytössä on F Secure Oy:ltä hankittu virustorjuntaohjelmisto .

- Asiakastietoja käsittelevät tietokoneet ja mobiililaitteet ovat kaikki etähallittavia ja etätyhjennettäviä yllä kuvatulla tavalla. Sim-korttien PIN-koodit on vaihdettu käyttäjäkohtaisiksi. Laitteiden lukituksen avaaminen edellyttää henkilökorttia, salasanaa, pin-koodia ja/tai sormenjälkitunnistautumista. Tietojärjestelmiin tehtävissä uusissa

sisäänkirjautumisissa hyödynnetään kaksivaiheista (MFA, multi-factor authentication tai monimenetelmäinen todentaminen) tunnistautumista, jolloin salasanan lisäksi käyttäjä varmennetaan esimerkiksi matkapuhelimella. Mobiililaitteet lukittuvat automaattisesti ollessaan minuutin käyttämättä.

Käyttöympäristön tukipalvelut,

- Yrittäjä huolehtii yleisistä käyttöympäristön tukipalveluista: esimerkiksi käyttöjärjestelmän päivitykset ja varusohjelmistojen, kuten esim. MS Office-päivitykset

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

Alusta- ja verkkopalveluiden tietoturallisuudesta huolehditaan seuraavasti:

Käytössä ei ole alusta- tai verkkopalveluita

Tietoverkkojen hallinta, verkkolaitteet, langattomat verkot ja reitittimet,

- Käytetään yrittäjän oman mobiililaitteen verkkoa, joka on suojattu salasanalla. Salasana vaihdetaan vähintään 90 päivän välein.
- Mobiililaitte päivitetään laite- ja laiteohjelmistojen päivityksillä säännöllisesti ja aina tarvittaessa

8. Kanta-palvelujen liittymisen ja käytön tietoturvakäytännöt

Yrityksellä on liittynyt Kanta-palveluun. 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. Kanta-toimintojen koulutus tapahtuu joko yrityksen toimesta, Diariumilta tilatussa koulutuksessa tai käyttäen Diarium-potilastietojärjestelmän sisäisesti jaettu verkkokoulutusta.

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

- Kaikilta työntekijöiltä ja alihankkijoilta edellytetään perehtyneisyyttä Kanta.fi -palvelun ohjeisiin tietojen luovuttamisen (sisältäen Kanta-palveluista informoimisen) ja omakannan käytön ohjaamiseen liittyen. Asiakkaita kannustetaan seuraamaan omien tietojensa käyttöä, jonka lisäksi yrityksessä valvotaan potilastietojen lukemisesta kertyvää lokia pistokokeilla ja asiakkaiden ilmoitusten perusteella. Potilasasiakirjojen väärinkäytöstä ja sen rangaistavuudesta on opastettu henkilökuntaa.
- Kanta-palveluun kirjaudutaan toimikortilla ja salasanalla, mahdollisuus lisäksi authenticator todentamiseen. Yrittäjä huolehtii, että toimikortti on voimassa. Yrittäjä seuraa omaa

käyttöään.

- Sote-organisaatiorekisteritietojen tai IAH-koodiston tietojen tarkastaminen:
 - [IAH-koodistosta](#)
 - Tiedot haetaan syöttämällä haetun yrityksen Y-tunnus Tarkennettu haku -ominaisuuden avaamaan Y-tunnuskenttään. Y-tunnus kirjoitetaan kokonaan ja täysin oikein. Hakuja ei tehdä yrityksen nimellä, sillä se on Y-tunnushakua huomattavasti epävarmempi tapa.
 - virheellisten tietojen korjaukset ja lisäykset tehdään aina oman alueen AVI:in tai Valviraan otettava huomioon myös muutostilanteissa tehtävät päivitykset
- Yrittäjä varmistaa vuosittain, että Kanta-palveluihin liittyvillä tietojärjestelmillä (erityisesti A2 tai A3-luokan järjestelmät) ja muilla sertifiointia edellyttävillä tietojärjestelmillä ja välityspalveluilla (luokan A1 järjestelmät) on voimassa oleva todistus tietoturvallisuuden arvioinnista, ja tiedot Valviran tietojärjestelmärekisterissä (A1, A2 tai A3-luokan järjestelmä)
- Yrittäjä varmistaa, että hankittava tai päivitettävä järjestelmä täyttää sitä koskevat olennaiset vaatimukset (kuinka asia kuvataan sopimuksissa, mitä tarkistuksia tehdään esim. THL:n määräyksistä, järjestelmäprofileista ja järjestelmältä vaadittavasta todistuksesta tietoturvallisuuden arvioinnista, Valviran tietojärjestelmärekisteristä ja Kelan yhteistestauksen tuloksista)
- Järjestelmän käyttö lopetetaan, yrittäjä ottaa vastuun tilanteessa, jossa käytössä olevalta järjestelmältä peruutetaan todistus tietoturvallisuuden arvioinnista määräajaksi tai kokonaan, jossa todistusta tietoturvallisuuden arvioinnista rajoitetaan tai tilanteessa, jossa tietojärjestelmän käyttö kielletään, tällöin tiedot siirretään hyväksytyyn järjestelmään tai tulostetaan manuaaliseen arkistoon.