



Fysio Ohmeroluoma Oy

OMAVALVONTASUUNNITELMA

01.12.2016 versio 1.0

Hannele Ohmeroluoma

Sisällysluettelo

SISÄLLYSLUETTELO	2
1. JOHDANTO	3
2. SUUNNITELMAN KOHDE	4
3. YLEISET TIETOTURVAKÄYTÄNNÖT	6
4. KÄYTTÖYMPÄRISTÖN JA USEIDEN JÄRJESTELMIEN YHTEISET TIETOTURVAKÄYTÄNNÖT	9
5. KÄYTTÖVALTUUKSIEN, PÄÄSYNHALLINNAN JA KÄYTÖN SEURANNAN YLEISET KÄYTÄNNÖT	11
6. KANTA-PALVELUIDEN KÄYTÖN TIETOTURVAKÄYTÄNNÖT	12
7. TIETOJÄRJESTELMÄT	13
8. TIETOJÄRJESTELMÄKOHTAISET OHJEET JA SUUNNITELMAT	14



OMAVALVONTASUUNNITELMA

1. JOHDANTO

Sosiaali- ja terveydenhuollon palvelun antajien, apteekkien ja itsenäisten ammattiharjoittajien, 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.

Omavalvontasuunnitelmalla varmistetaan potilastietojen asianmukainen ja tietoturvallinen käsittely ja säilytys. Omavalvontasuunnitelmaa on päivitettävä jatkuvana prosessina osana yrityksen tietoturvaa ja laadunhallintaa. Kantaan liittymisen yhteydessä tulee omavalvontasuunnitelmaa myös päivittää.

Omavalvontasuunnitelma tulee olla tehtynä voimassa olevan lain mukaan 31.12.2017 mennessä. Suunnitelmaan kirjataan nykyiset käytännöt ja/tai työn alla olevat tulevat käytännöt. Omavalvontasuunnitelma on jatkoa organisaation itseauditoinnille ja tulee sen korvaamaan.

Omavalvontasuunnitelmassa viitataan aina kuin mahdollista olemassa oleviin erikseen ylläpidettäviin ohjeisiin ja dokumentteihin. Olennaista on, että suunnitelman linkkien tai tietojen avulla on selvää, mistä dokumentaatio on löydettävissä tai vaatimuksen täyttyminen on todennettavissa. Mikäli muuta valmista dokumentaatiota ei ole olemassa tai saatavissa, on mahdollista kuvata vaadittavat asiakokonaisuudet ja toimintatavat suoraan omavalvontasuunnitelmaan.

Omavalvontasuunnitelmalla varmistetaan potilastietojen asianmukainen ja tietoturvallinen käsittely ja säilytys. Omavalvontasuunnitelmalla kehitetään yrityksen sisäistä toimintaa. Omavalvontasuunnitelmaa on päivitettävä jatkuvana prosessina osana yrityksen tietoturvaa ja laadunhallintaa.

Omavalvontasuunnitelman tavoite on ylläpitää asiakkaiden ja eri yhteistyökumppaneiden luottamusta yrittäjätarjoaviin palveluihin sekä niiden tietoturvan, tietosuojaan ja yksityisyydensuojan toteutumiseen.



OMAVALVONTASUUNNITELMA

2. SUUNNITELMAN KOHDE

Tämä omavalvontasuunnitelma koskee seuraavaa yritystä.

Yritys	Fysio Ohmeroluoma Oy
Y-tunnus	2770575-6
Päätoimiala	Fysioterapia
Kotipaikka	Vihti
Käyntiosoite	Tuusantie 3, 03100 Nummela
Vastaavana johtajana	Fysioterapeutti Hannele Ohmeroluoma
Oma- valvonnan vastuhenkilö	Hannele Ohmeroluoma
Muut toimitilan käyttäjät	Ammatinharjoittaja fysioterapeutti Jari Kalatie

Aluehallintoviraston lupa myönnetty	8. elokuuta 2016
Tietosuojavastaava	Hannele Ohmeroluoma
Arkistohoitaja	Hannele Ohmeroluoma

Oma-
valvontasuunnitelmaa päivitetään aina tarvittaessa. Päivityksen hoitaa tietosuoja-
vastaava, joka on myös vastuussa tiedon siirtämisestä käytäntöön. Oma-
valvontasuun-
nitelman toteuttamista seurataan jatkuvasti ja epäkohtiin puututaan tarvittaessa.

PERUSTELUT

Asiakastietolain mukaan jokainen sosiaali- ja terveydenhuollon palvelujen antajan on ni-
meltävä seuranta- ja valvontatehtäviä varten tietosuojavastaava. Tietosuojavastaavan
tehtävänä on valmistella tietosuoja koskevia ohjeita ja ylläpitää niitä yhdessä potilasre-
kistereiden vastuu henkilöiden kanssa, toimia erikseen sovitusti asiantuntijana sosiaali-
ja terveydenhuollon asiakastietojen sähköistä käsittelyä koskevan lain mukaisissa tietos-
suojaa ja potilasrekisteriä koskevissa asioissa sekä seurata ja valvoa, että tietosuojaoh-
jeita noudatetaan potilastyössä ja muussa toimintayksikön toiminnassa. Tietosuojavas-
taavalla on oltava myös käytännössä riittävät resurssit sekä toimivalta tehtävässä me-
nestyksellisesti suorittamiseksi.

Itsenäisen ammatinharjoittajan, joka toimii itsenäisesti omissa tiloissa, ei tarvitse nimetä
toiminnalleen tietosuojavastaavaa, mutta tietosuoja koskevat vastuut ja veloitteet
koskevat myös itsenäisiä ammatinharjoittajia.

Tietosuojavastaavan tarkemmat tehtävät on esitetty linkissä:

<http://www.kanta.fi/tietosuojavastaava>

Arkistonhoitaja voi käyttöliittymänsä avulla tehdä arkistohoidollisia toimenpiteitä Poti-
lastiedon arkistoon arkistoiduille asiakirjoille. Arkistonhoitaja voi hakea ja tarkastella ar-
kistoituja asiakirjoja ja niiden kuvailutietoja, muokata tiettyjä asiakirjan kuvailutietoja
sekä tarkastella asiakirjojen hävityslistaa. Arkistonhoitaja ei voi itse poistaa asiakirjoja



OMAVALVONTASUUNNITELMA

vaan asiakirjojen poistaminen Potilastietojen arkistosta tapahtuu automaattisesti, kun asiakirjojen säilytysaika on päättynyt.

Tarkemmat tiedot löytyvät linkistä: <http://www.kanta.fi>

Arkistonhoitaja voi kuitenkin jatkaa potilastietojen säilytystä 1, 3 tai 5 vuotta kerrallaan, mikäli potilastietojen säilyttämiselle on vielä potilaslain tarkoittama tarve.

Arkistohoitajan tehtäviin voidaan sisällyttää myös yrityksen lakisääteinen velvollisuus huolehtia säilytysajan ylittäneiden tietojen poistamisesta myös rekisteripitäjän omista järjestelmistä. Kanta-arkistosta poistettu tieto ei välttämättä poistu yrityksen omasta järjestelmästä, ellei näin ole oman järjestelmätoimittajan kanssa nimenomaisesti sovittu.

Arkistohoitajan tarkemmat tehtävät on esitetty linkissä:

<http://www.kanta.fi/documents/12105/4035331/Arkistohoitajan+toimintamallit+ja+arkistohallinta/2ef5f747-edc8-403c-986f-d5615a97e5af>



OMAVALVONTASUUNNITELMA

3. YLEISET TIETOTURVAKÄYTÄNNÖT

Pääkäyttäjä	Hannele Ohmeroluoma
-------------	---------------------

PERUSTELUT

Jokaiselle tietojärjestelmälle on nimettävä **pääkäyttäjä**, jonka vastuulla on huolehtia järjestelmän käyttöoikeuksista. Pääkäyttäjältä vaaditaan hyvää tietoturva- ja tietosuojaa osaamista. Lisäksi tiedon omistajien ja pääkäyttäjien on huolehdittava tiedon koko elinkaaren hallinnasta ja ICT- varautumissuunnitelmista, missä kuvataan vastuuhenkilöt, roolit ja toimintamallit riskien toteuttamisen varalta.

Yrityksen tulee laatia toiminnalleen tietoturvapoliittikka, joka koskee kaikkia potilastietoja sekä käsittelyä välineestä riippumatta. Tiedot luovutetaan vain voimassa olevan lainsäädännön puitteissa tai asiakkaan erillisellä kirjallisella luvalla. Tietojen säilyttäminen ja hyödynnettävyys sekä saatavuus turvataan siten, ettei esimerkiksi onnettomuus tai talennusvälineen särkyminen tai välineen teknisen tuen tai luotettavuuden loppuminen vaarana tietojen säilymistä.

Viitaten:

- Malli tietoturvapoliitikaksi (Suomen Fysioterapeuttien ja Fysin oma malli)
- Tietoturvaohjeet henkilöstölle (Suomen Fysioterapeuttien ja Fysin oma malli)
- Johdon tietoturvavelvoitteet fysioterapiayrityksessä (Suomen Fysioterapeuttien ja Fysin oma malli)

PERUSTELUT

Yrittäjän (esimiehen) vastuulla on huolehtia ja noudattaa työnantajaa koskevien lakisääteisten tietoturva- ja tietosuojavelvoitteiden toteutumisesta. Yrittäjät, esimiehet, tietosuojavastaava ja tietojärjestelmien pääkäyttäjät vastaavat työntekijöiden käyttöoikeuksista tietojärjestelmiin ja niiden tietosisältöihin työtehtävien edellyttämässä laajuudessa. He huolehtivat loppukäyttäjien riittävästä perehdytyksestä yrityksen tietoturvakäytäntöihin varmistuen, että jokainen ymmärtää niiden merkityksen työtehtävissään.

Esimieheltä odotetaan esimerkillistä sekä vastuullista tietoturvakäyttäytymistä ja heillä on raportointivelvollisuus tietoturvapoikkeamista tietosuojavastaavalle. Työntekijän vastuulla on myös huolehtia käsittelemänsä tiedon oikeellisuudesta, saatavuudesta ja luokitte- luksesta, sekä huolehtia, että organisaation tiedot ovat asianmukaisesti käytettävissä. Tietojen säilytys- tai arkistointiajan päätyttyä ne on hävitettävä ohjeiden mukaisesti. Työntekijällä on velvollisuus raportoida tietoturvaongelmista oman organisaation tietoturva- vastaavalle.

Tiedot tulee myös suojata tai varmentaa siltä varalta, että onnettomuus tai laitteen tekni- sen käyttöiän päätyminen ei estä arkiston ylläpitoa tai pääsyä tietoihin. Esimerkiksi kovalevy saattaa ajan kuluessa rikkoutua tai vanhentua siten, ettei tiedon lukemiseen teknisesti kykeneviä järjestelmiä ole enää saatavilla.



OMAVALVONTASUUNNITELMA

Koulutus, ohjeistus ja käyttökokemus sekä niiden seuranta

Käytössä on Acute-asiakashallintaohjelma, johon on pääkäyttäjän yhteiskoulutus. Käyttöönottoprojektin aikana käsitellään seuraavat asiat:

- Acute-järjestelmän ohjeet uuden kertomuksen käyttööntamiseksi.
- Koeajoasennus harjoittelukäyttöön, missä harjoitellaan uutta järjestelmää.
- Aiempien kirjausten siirto uuteen kertomukseen.
- Acute-järjestelmän asetuksien määrittely.
- Kortinlukuohjelman asennus.
- Ohjeet eArkistopalvelun käytölle Acute-järjestelmän osalta.
- Acute-järjestelmän kytkeminen eArkiston yhteyteen.

Terveyden- ja hyvinvointilaitoksen rakenteisen kirjaamisen opiskelu ja kouluttautuminen. Seurataan ohjeistuksia ja noudatetaan niitä Kanta-järjestelmän osalta reaaliajassa.

Kaikkien henkilöiden tulee käydä Potilastiedonarkiston verkkokoulutus ja tietoturvakoulutus.

PERUSTELUT

Tietoturvatointiminta vaatii henkilöstöltä tietoturvakäytänteiden tuntemista ja ohjeiden noudattamista. Tietoturvakoulutukset ja tietoturvatietoisuuden lisääminen ovat osa säännöllistä kehittämis- ja perehdytystoimintaa, jotka työntekijät on velvollinen suorittamaan.

Kanta / Arkistokoulutus: <http://www.kanta.fi/Arkistokoulutus/story.html>

Kanta / Tietoturvakoulutus: <https://verkkokoulut.thl.fi/web/kanta/tietoturva/sisallot>

Toimintamallien koulutus ja perehdytys

Henkilöstön perehdyttämiskäytännöt:

1. Uusi työntekijä
Tällä hetkellä minulla ei ole työntekijöitä.
2. Työsuhteessa oleva henkilö
Tällä hetkellä ei ole työsuhteessa olevia henkilöitä.
3. Henkilöstön kouluttaminen laadunhallintaan ja asiakasturvallisuuteen.
4. Vuokralaisella on perehdytyskansio, josta löytyvät tietoturvallisuuteen, laadunhallintaan ja asiakasturvallisuuteen liittyvät asiat.

Tietojärjestelmien käyttökoulutus

Tietojärjestelmien toimittajat järjestävät koulutuksia tietojärjestelmiin. Henkilökunta veloitetaan osallistumaan näihin tai osoittamaan muutoin osaamisensa tietojärjestelmän käyttöön.

Riittävä kokemus

Mikäli henkilöllä ei ole riittävästä kokemuksesta, käydään hänen kanssaan käytännössä ongelmakohdat läpi ja harjoitellaan ohjelman käyttöä.



OMAVALVONTASUUNNITELMA

Ohjeet ja koulutus potilastietojen käsittelyssä

Potilastietojen käsittelyn ohjeet löytyvät sille varatusta kansioista. Kansio sijaitsee lukitussa kaapissa, mistä löytyvät myös potilastiedot ja -lähetteet. Kaapisto pidetään virkaajan ulkopuolella aina lukittuna ja avataan, kun työskennellään toimitiloissa. Ohjeita päivitetään aina tarvittaessa, esimerkiksi päivitysten yhteydessä.

PERUSTELUT

Potilastiedot ovat lähtökohtaisesti arkaluonteisia henkilötietoja, joita ei saa käsitellä ilman lain tarkoittamaa poikkeusta tai potilaan lupaa.

Käsittelyllä tarkoitetaan henkilötietojen keräämistä, tallentamista, järjestämistä, käyttöä, siirtymistä, luovuttamista, säilyttämistä, muuttamista, yhdistämistä, suojaamista, poistamista, tuhoamista sekä muita henkilötietoihin kohdistuvia toimenpiteitä.

STM: Potilasasiakirjojen laatiminen ja käsittely

Opas terveydenhuollolle:

<https://www.julkari.fi/bitstream/handle/10024/112073/URN%3aNBN%3afe201504225719.pdf?sequence=1>

Henkilötietolaissa säädetään poikkeuksista potilastietojen käsittelykieltoon. Niitä saa käsitellä terveydenhuollossa siltä osin kuin ne ovat välttämättömiä potilaan hoidon tai muun laissa säädetyn tehtävän kannalta.

Henkilörekisterin käyttötarkoitus on aina määriteltävä ennalta:

<http://www.finlex.fi/fi/laki/ajantasa/1999/19990523>

Terveydenhuollon ammattihenkilö, muu terveydenhuollon toimintayksikössä työskentelevä tai sen tehtäviä suorittava ei saa luovuttaa sivullisille potilasasiakirjoihin sisältyviä tietoja, jos siihen ei ole potilaan kirjallista suostumusta taikka luovutukseen oikeuttavaa tai velvoittavaa lain säännöstä.

Säännös koskee asemasta, ammatillisesta koulutuksesta tai tehtävästä riippumatta kaikkia niitä, jotka osallistuvat potilaan hoitoon tai siihen liittyviin tehtäviin.

Terveydenhuollon toimintayksikön salassapito- ja käyttäjäsitoutumismalli:

http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetun_toimis-to/opaat/6Jfq4Hak3/Malli_terveydenhuollon_toimintayksikon_salassapito_ja_kayttajasitoutukseksi.pdf



4. KÄYTTÖYMPÄRISTÖN JA USEIDEN JÄRJESTELMIEN YHTEISET TIETOTURVAKÄYTÄNNÖT

Laatukäsikirja löytyy lukitusta kaapista, missä säilytetään myös potilastiedot.

Menettelyt virhe- ja ongelmatilanteissa

Käyttämämme potilastietojärjestelmä (Acute) on A-luokan tietojärjestelmä, joka kytkeytyy kansallisiin palveluihin. Mikäli kyseisessä järjestelmässä havaitaan potilasturvallisuutta, tietosuojaa tai muuta A-luokan tietojärjestelmälle asetetuista olennaisten vaatimusten täyttymisestä havaittu poikkeamaa, menettelemme seuraavasti:

1. Organisaatiossamme pääkäyttäjäroolissa toimiva henkilö selvittää, että kyseessä on tietojärjestelmästä johtuva poikkeama.
2. Mikäli kyseessä on edellä esitetty poikkeama, joka on vakavuudeltaan merkittävä, ilmoittaa pääkäyttäjäroolissa oleva henkilö tästä potilastietojärjestelmän toimittajalle tämän osoittamalla tavalla (tavanomaisimmin puhelimitse tai sähköpostitse).
3. Mikäli poikkeama on merkittävästi potilasturvallisuutta vaarantava, ilmoittaa pääkäyttäjä tästä ensisijaisesti organisaatiomme johdolle, joka tekee poikkeamasta ilmoituksen Valviraan ja ryhtyy tarvittaviin toimiin potilasturvallisuuden palauttamiseksi.

Vastuu potilastietojärjestelmässä havaittujen poikkeamien korjaamiseksi on potilastietojärjestelmän toimittajalla.

Järjestelmien käyttöohjeiden hallinnointi ja saatavuus

Käyttämämme potilastietojärjestelmän ohjeet ovat kaikkien järjestelmäkäyttäjien saatavilla järjestelmän käyttöohjepalvelussa (*Help & Manual*).

Potilastietojärjestelmän toimittaja päivittää ohjeet versiopäivityksen yhteydessä.

Organisaatiomme pitää kirjaa siitä, että kaikki potilastietojärjestelmän käyttäjämme ovat saaneet riittävän koulutuksen potilastietojärjestelmän käyttöön ja tietävät mistä ohjeet löytyvät.

Versiopäivitysten yhteydessä organisaatiomme huolehtii siitä, että kukin potilastietojärjestelmän käyttäjä perehtyy niihin muutoksiin, joita järjestelmään on tullut ja kyseisiin käyttöohjeisiin ja määräyksiin, joita potilastietojärjestelmän toimittaja antaa.

Potilastietojärjestelmän sisäisten ohjeiden lisäksi, versiopäivitysten yhteydessä organisaatiomme tarkistaa sisäiset potilastietojärjestelmään liittyvät käyttötapaohjeistonsa ja varmistaa, että kaikki käyttäjät ovat tietoisia, mikäli näihin tulee muutoksia.

Järjestelmien asennus ja ylläpito yleisesti

Käytämme potilastietojärjestelmää (Acute) sovellusvuokrauksena. Potilastietojärjestelmän asennus-, päivitys- ja ylläpitovastuu on toimittajalla. Potilastietojärjestelmän päivityksen yhteydessä pääkäyttäjäroolissa toimiva henkilömme varmistuu, että potilastietojärjestelmä toimii A-luokan tietojärjestelmän olennaisten vaatimusten mukaisesti. Varmistuminen suoritetaan joko tehostetulla käytön valvonnalla tai testaamalla.



OMAVALVONTASUUNNITELMA

Yrittäjän tai tietosuojavastaavan vastuulla on fyysisten salausten (palomuri, virustorjunta) päivitys.

Tilojen, työasemien, tallennusvälineiden ja tulosteiden turvallisuus

Työtiloihin on omat avaimet, joita ei anneta ulkopuolisille. Työtila suljetaan asianomaisesti omalla avaimella. Näyttöpäätteet pyritään suojaamaan siten, ettei sivullisilla ole näköyhteyttä. Näyttö menee lukitustilaan silloin kun sitä ei käytetä 30 min kuluttua ja sisälle pääsee tietyllä salasanalla. Virustorjuntaohjelmaksi käytetään Norton-viruksen torjuntaohjelmaa. Mobiililaitteet, tabletit ja älypuhelimet on suojattu salasanalla. Potilastietojärjestelmään kirjaudutaan käyttäjätunnuksella ja vahvalla salasanalla. SIM-korteissa on PIN -koodit ja laitteissa on viruksen torjuntaohjelma.

Pääkäyttäjällä on oikeus asentaa ohjelmistoja ja sovelluksia yrityksen laitteille. Tulostin on sijoitettu lähelle tietokonetta, jotta tulosteet eivät joudu väärin käsiin. Potilastietoja sisältävät paperitulosteet säilytetään lukittuna. Ulkoiset kovalevyt ja muistitikut on suojattu salasanalla.

Käytämme potilastietojärjestelmää (Acute) sovellusvuokrauksena, jolloin potilastietojärjestelmä ei tallenna mitään työasemalle. Lisäksi käyttäjiä on määrätty olemaan tallentamatta mitään potilastietoa työasemalle. Potilastietojärjestelmän sisältämän tiedon fyysisen tietoturvan ja palvelimen virustorjunnan vastuu on potilastietojärjestelmän toimittajalla. Liikennöinti organisaatiomme työasemien ja potilastietojärjestelmän välillä on salattu.

Muut käyttöympäristön käytännöt

Laitteiston rikkoontuessa hankitaan tukipalvelut alan ammattilaisilta. Verkkoyhteys on hankittu tällä hetkellä (5/2017) Elisan kautta. Sopimusehdot löytyvät työpisteen tiedoista ja laatukansiosta. Tarvittaessa käytetään etäyhteyttä, esimerkiksi Acuten kanssa.

Langaton WiFi-verkko:

- Reititin: TeleWell
- Tyyppi: TW-EAV510 ADSL2+ | VDSL2 WLAN Router
- Suojaus: WPA2/WPA -PSK



5. KÄYTTÖVALTUUKSIEN, PÄÄSYNHALLINNAN JA KÄYTÖN SEURANNAN YLEISET KÄYTÄNNÖT

Käyttäjryhmät

Organisaatiomme käyttämän potilastietojärjestelmän (Acute) käyttöoikeudet toimivat käyttäjäroolien ja -ryhmien mukaisesti. Ajankohtainen tieto käyttäjistä ja heidän käyttäjärooleistaan löytyvät potilastietojärjestelmästä.

Käyttövaltuushallinnan ja käytön seurannan käytännöt

Ylläpitäjällä on oikeudet myöntää käyttöoikeus kunkin ammattiryhmän työn vaatimassa laajuudessa. Tietosuojavastaavalla on oikeus seurata lokitietoa, muuttaa merkintöjä ja poistaa niitä.

Järjestelmään tunnustaudutaan joko henkilökortilla tai käyttäjätunnuksella ja vahvalla salasanalla.

Käyttämäämme potilastietojärjestelmään (Acute) käyttövaltuuksia antaa vain järjestelmän pääkäyttäjä. Käyttöoikeuden toteaminen tehdään joko pääkäyttäjän tai organisaatiomme johdon toimesta. Käyttövaltuuksien muuttaminen tai poisto tapahtuu pääkäyttäjän toimesta, johdon aloitteesta tai erikseen sovitun käytännön mukaisesti. Potilastietojärjestelmään kirjaudutaan joko

1. Käyttäjätunnus ja salasana- yhdistelmällä tai
2. Toimikortilla

PERUSTELU

Sähköisten potilasasiakirjojen käyttöä seurataan ja valvotaan lokitietojen avulla ennalta määritellyn suunnitelman mukaisesti. Sähköisten potilastietojen käyttöön ja luovutukseen liittyvät lokitiedot tulee säilyttää eheinä ja muuttumattomina **12 vuotta** niiden syntymisestä.

Katso lisätiedot osoitteista:

Tietovaltuutettujen toimisto: <http://www.tietosuoja.fi/fi>

Viestintävirasto: <https://www.viestintavirasto.fi>

Potilastietojärjestelmäämme tietosuojaan liittyviä käyttölokeja valvotaan pistokokein tietovastaavan toimesta. Mikäli väärinkäytösepäilyjä esiintyy, tietosuojavastaava selvittää asiaa. Mikäli väärinkäytösepäilyjä havaitaan, eskaloi tietosuojavastaava asian organisaation johdolle, joka asioi viranomaisten kanssa asiaan liittyen.



6. KANTA-PALVELUIDEN KÄYTÖN TIETOTURVAKÄYTÄNNÖT

Käytämme potilastietojärjestelmäämme (Acute) sovellusvuokrauksella toimittajapalveluksena. Potilastietojärjestelmän tietoturva on toimittajan vastuulla. Tämä potilastietojärjestelmä tarjoaa Kanta-palveluiden edellyttämät tunnistamis- ja todentamisratkaisut sekä tarjoaa riittävät varmenneratkaisut.

Luvussa 5 on kerrottu tarkemmin potilastietojärjestelmämme käyttövaltuuksien hallintaa.

Toimenpiteet poikkeustilanteessa

Potilasarkiston kirjauksissa siirrytään poikkeustilanteessa paperikirjaukseen siihen asti, kunnes tilalle saadaan uusi järjestelmän toimittaja tai ongelma ratkeaa.

Kelan häiriöviestinnänohje:

http://www.kanta.fi/documents/12105/3447366/Toiminta+häiriötilanteissa_31072015/d12408b1-aaa5-4ba3-a7e3-45eced40a2ef



7. TIETOJÄRJESTELMÄT

Kanta-palveluihin liittyvät tietojärjestelmät (luokka A)

Acute

- Versio: 5.2 tai sitä uudempi
- Toimittaja: Acuvitec Oy
- Osoite: Aleksanterinkatu 32, 33100 Tampere

Muut asiakas- tai potilastietoja käsittelevät järjestelmät (luokka B)

Acute

- Versio : 4.2
- Toimittaja : Acuvitec Oy
- Osoite: Aleksanterinkatu 32, 33100 Tampere

Muut tietojärjestelmät, jotka on otettava huomioon arkaluonteisten asiakas- ja potilastietojen suojaamisen kannalta

- Operaattori: Elisa
- Osoite: PL 1, 00061 Elisa
- Internet: ADSL
- OS-järjestelmä: Windows 7

8. TIETOJÄRJESTELMÄKOHTAISET OHJEET JA SUUNNITELMAT

Acute (luokkaan A kuuluva)

Acute (tarkemmat tiedot ks. luku 7)

- Käyttötarkoitus:
 - Potilastietojärjestelmä.
- Käyttäjryhmät:
 - Ajankohtainen lista käyttäjryhmistä löytyy potilastietojärjestelmästä.
 - Ks. luku 5.
- Käyttöohjeet:
 - Järjestelmän sisäiset ohjeet.
 - Organisaation sisäiset toimintaohjeet.
- Ohjeiden päivittäminen ja jakelu:
 - Ks. luku 4.
- Menettely virhe- ja ongelmatilanteessa:
 - Ks. luku 4.
- Käyttövaltuushallinta järjestelmässä:
 - Ks. luku 4.
- Tunnistautuminen järjestelmässä:
 - Ks. luku 5.
- Lokit:
 - Potilastietojärjestelmässä on käyttöloki, jonka avulla pystytään seuraamaan järjestelmän käyttöä ja havaitsemaan mahdolliset väärinkäytökset.
- Järjestelmän lukkiutuminen:
 - Järjestelmä lukkiutuu, kun järjestelmä on käyttämättä 30 min tai kun toimikortti otetaan pois kortinlukijasta.
 - Järjestelmän käyttäjätunnus lukkiutuu viidestä väärästä salasanasta tai asetetun päivämäärän umpeuduttua.
- Järjestelmä on Kelan auditoima.

Acute (luokkaan B kuuluva)

Acute (tarkemmat tiedot ks. luku 7)

- Käyttötarkoitus:
 - Potilastietojärjestelmä.
- Käyttäjryhmät:
 - Ajantasainen lista käyttäjryhmistä löytyy potilastietojärjestelmästä.
 - Ks. luku 5.
- Käyttöohjeet
 - Järjestelmän sisäiset ohjeet.
 - Organisaation sisäiset toimintaohjeet.
- Ohjeiden päivittäminen ja jakelu:
 - Ks. luku 4.
- Menettelyt virhe- ja ongelmatilanteissa:
 - Ks. luku 4.
- Käyttövaltuushallinta järjestelmässä:
 - Ks. luku 4.
- Tunnistautuminen järjestelmässä:
 - Ks. luku 5.
- Lokit:
 - Potilastietojärjestelmässä on käyttöloki, jonka avulla pystytään seuraamaan järjestelmän käyttöä ja havaitsemaan mahdolliset väärinkäytökset.
- Järjestelmän lukkiutuminen:
 - Järjestelmä lukkiutuu, kun järjestelmä on käyttämättä 30 min tai kun toimikortti otetaan pois kortinlukijasta.
 - Järjestelmän käyttäjätunnus lukkiutuu viidestä väärästä salasanasta tai asetetun päivämäärän umpeuduttua.

Järjestelmä Y (muut järjestelmät)

- Järjestelmät, versiot, toimittajat ja toimittajien osoitteet:
 - Ks. luku 7.
- Käyttötarkoitus:
 - Potilastietojärjestelmän toimintavalmius.
- Käyttäjryhmät:
 - Pääkäyttäjä ja vuokralainen.
- Käyttöohjeet:
 - Arkistokaapissa.
- Ohjeiden päivittäminen ja jakelu:
 - Tarvittaessa.
 - Päivitykset tulevat toimittajan kautta säännöllisesti.
- Menettely virhe- ja ongelmatilanteessa:
 - Yhteys alan ammattilaiseen tai Elisan asiakaspalveluun.
- Järjestelmäkohtaiset tukipalvelut:
 - Yhteys alan ammattilaiseen.
- Asennus- ja ylläpitovastuut sekä vaatimukset:
 - Vastuu pääkäyttäjällä, joka huolehtii, että käyttöjärjestelmä toimii asianmukaisesti ja huolehtii tarvittavista huoltotoimenpiteistä.
- Menettelytavat ja vastuut virhe- ja poikkeustilanteissa:
 - Pääkäyttäjä vastaa siitä, että virhe- ja poikkeustilanteessa potilastietoa ei saa nähdä ulkopuoliset ja tarvittaessa potilastieto dokumentoidaan paperisena siihen saakka kun tilanne on saatu hallintaan.
- Käyttövaltuushallinta:
 - Pääkäyttäjällä ja vuokralaisella.
- Tunnistautuminen järjestelmässä:
 - Salasanalla.
- Lokit:
 - Windowsin oma suojausjärjestelmä palomuurilla ja Norton- virustorjuntaohjelma.
- Järjestelmän lukkiutuminen:
 - Järjestelmä lukkiutuu järjestelmän ollessa käyttämättömänä 30 min.
 - Järjestelmän saa avattua uudelleen antamalla salasanan.