Espoon Lähimmäispalveluyhdistys ry

OMAVALVONTASUUNNITELMA TIETOTURVAN JA TIETOSUOJAN TOTEUTUMISESTA

29.4.2015

Kaisa Pekola

Sisältö

1 Johdanto

Espoon Lähimmäispalveluyhdistys on yleishyödyllinen voittoa tavoittelematon kolmannen sektorin sosiaali- ja terveysalan tuottaja jonka tuottamistapa on oma. Toiminta kohdistuu ikääntyvään väestöön ja toimintarajoitteisten hyväksi. Yhdistyksellä on kaksi palvelutaloa, Merikartano ja Puistokartano. Merikartano on valmistunut 1999 ja Puistokartano 2013. Merikartanossa on 117 palvelutaloasuntoa ja Puistokartanossa 107. Palveluasumisen lisäksi Puistokartanossa on myös tehostetun ympärivuorokautisen palveluasumisen yksikkö muistisairaille (Puistohelmi).
Palveluasuminen on ilmoituksenvaraista toimintaa ja tehostettu ympärivuorokautinen palveluasuminen luvanvaraista toimintaa. Espoon kaupunki toimii valvovana viranomaisena ja auditoi tuottamiamme hoivan ja huolenpidon palveluita kerran vuodessa. Seuraava auditointi on 25.4.2017.
Tämä omavalvontasuunnitelma tulee olemaan erillisenä liitteenä, osana voimassa olevia omavalvontasuunnitelmia. Omavalvontasuunnitelmat löytyvät jokaisesta yksiköstä josta ne voi pyytää luettavaksi. Lisäksi ne löytyvät yhdistyksen nettisivuilta, www.elpy.fi.

2. Suunnitelman kohde

Tämä omavalvontasuunnitelma koskee Espoon Lähimmäispalveluyhdistys ry:n tietojärjestelmien, tietoturvan ja tietosuojan käytänteitä. Omavalvontasuunnitelman liitteeksi tulevat erilliset rekisteriselosteet ja muita selvityksiä liittyen eri asiakas rekisterijärjestelmiin joita yhdistyksellä on käytössä.
Tietosuojaan liittyvä omavalvontasuunnitelma on osana yhdistysten eri yksiköiden omavalvontasuunnitelmia. Sen tarkoitus on kuvata yhdistyksen työntekijöille ja muille kuinka meillä käytännössä toimitaan asiakas ja potilasrekisteriin liittyvissä salassa pidettävien tietojen osalta.
Omavalvontasuunnitelma päivitetään vähintään kerran vuodessa tai tarvittaessa useammin. Se on osa perehdytyssuunnitelmaa joten asiat käydään läpi työntekijöiden kanssa.
Käytössämme olevat järjestelmät joissa käsitellään asiakas ja potilastietoja ovat:

- asiakastietojärjestelmä Doma Care
- Rai-soft ohjelmisto joka kuvaa toimintakyvyn ja terveydentilan sekä hoidon laadun ja vaikuttavuuden mittaamista
- Hilmo – hoitoilmoitusjärjestelmä
- rava/ravatar - ikäihmisten toimintakyvyn ja avuntarpeen arviointiin tarkoitettu mittari. (Ohjelman käyttö päättyy 2015)
- Iloq – lukitusjärjestelmä
- citrix joka on Espoon Kaupungin asiakastietojärjestelmän effican ulkoinen järjestelmä jota heidän lääkärinsä käyttävät tullessaan käynnille Puistohelmen yksikköön
- nova/Visma – taloushallinnon järjestelmä joka käsittelee asiakkaiden maksuja
- Vivago - turvapuhelinjärjestelmä

3. Yleiset tietoturvakäytännöt

Jokainen työntekijä, riippumatta siitä onko hoitotyössä, allekirjoittaa vaitiolosopimuksen aloittaessaan Espoon Lähimmäispalveluyhdistyksen palveluksessa.
Asiakastietojärjestelmän (Doma Care) pääkäyttäjä luo tarvittavan oikeustason mukaiset tunnukset työntekijöille jonka jälkeen työntekijä itse käy vaihtamassa itselle uuden salasanan. Tunnusta luodessa jokaisen työntekijän kohdalle kirjataan koulutuksen mukainen nimike jotta muut työntekijät tietävät mikä ammatillinen oikeus kullakin on. Työsuhteen päätyttyä käyttöoikeudet asiakastietojärjestelmään poistetaan.
Doma caren pääkäyttäjinä toimii vain muutama esimiesasemassa oleva yhdistyksen työntekijä.
Tietokonejärjestelmiin osalla työntekijöistä on omat käyttöjärjestelmätunnukset. Hoitoyksiköillä on omat, yhteisesti käytössä olevat tunnukset. Näillä tunnuksilla pääsee lukemaan esim. sähköpostit. Sähköposteissa emme käytä tunnistettavissa olevia nimiä tai muita tunnisteita mistä voisi paljastua asiakkaan henkilöllisyys. Olemme myös ohjeistaneet omaisia lähettämästä sähköpostia josta henkilöllisyys kävisi ilmi.
Espoon Kaupungin ilmaisvälinehoitajille lähetämme sähköpostia osoitteeseen joka on suojattu Espoon Kaupungin toimesta jotta voimme kohdistaa oikeat tuotteet oikeille henkilöille.
Työterveyshuolto Aavalla on myös käytössä suojattu yhteys jota käytämme tarvittaessa. Tämä yhteys on suojattu Aavan taholta.
Elpy:n tietosuojavastaavana toimii Kaisa Pekola.

Koulutus, ohjeistus ja käyttökokemus ja niiden seuranta

<u>Hoitajien käyttämät ohjelmat</u>
Doma care asiakastietojärjestelmä on ollut yhdistyksen käytössä vuodesta 2009. Esimiehet ovat saaneet opastuksen asiakastietojärjestelmän käytöstä sen suunnittelijalta. Esimiehemme voivat konsultoida suunnittelijaa tarvittaessa mutta käytännössä yhteydenpidon on hoitanut Pia Azengdi, yksi palveluvastaavistamme joka toimii Doma Care järjestelmän vastuuhenkilönä. Esimiehet ja muut työntekijät ovat itse perehdyttäneet uudet työntekijät järjestelmän käyttöön. Tarvittaessa saamme koulutuksen Doma Caren Invian Oystä.
Hoitohenkilökunta käyttää asiakastietojärjestelmää päivittäin, useita kertoja. Järjestelmä on yksinkertainen ja helppo käyttää. Uudet työntekijät perehdytetään omissa yksiköissä henkilökohtaisesti. Tarvittaessa olemme järjestäneet isomman koulutustilaisuuden.

Rai ohjelmaa (ohjelmisto toimintakyvyn ja terveydentilan sekä hoidon laadun ja vaikuttavuuden mittaamiseen) on meillä käytössä kahta eri versiota, kotihoidon ja laitoshoidon Rai. Ohjelmat ovat asennettu koneille ATK tuen ja Rai-softin yhteisvoimin. Ohjelmistokoulutuksesta on vastannut Rai-soft itse. Rai ohjelma on otettu käyttöön Espoon Kaupungin vaatimuksesta ja toiveesta ja Rai raportit lähetetään terveyden- ja hyvinvoinninlaitokselle (thl) kaksi kertaa vuodessa. Lähes koko hoitopuolen henkilökunta on käynyt Rai-softin järjestämän koulutuksen.
Rai raportti lähetetään thl:ään sähköisesti suojatun yhteyden kautta, ns Toimita – järjestelmää

käyttäen.
Toimita-lomakkeiden liikenne on suojattu. Toimitetut aineistot tallennetaan suoraan THL:n palvelinympäristöön. Aineistoihin on rajattu pääsy, joka perustuu THL:n tunnistautumiseen THL:n keskitettyä käyttäjärekisteriä vasten sekä aineistokohtaiseen käyttöoikeuteen. Aineistot säilytetään palvelussa 6 kk toimituksesta salakirjoitetussa muodossa. Salakirjoitukseen käytetään AES-256-algoritmia ja epäsymmetristä salausta.

Muut ohjelmat
Hilmo ohjelmaa käyttävät yksikköjen vastaavat kerran vuodessa. Hilmo on valtakunnallinen sosiaali- ja terveydenhuollon hoitoilmoitusjärjestelmä ja kattaa merkittävän osan sosiaali- ja terveydenhuollon laitos- ja asumispalveluista. Asiakaslaskennan tiedot lähetetään sähköisesti saman suojatun yhteyden kautta thl:ään kun Rai-materiaali.
Hilmo koulutuksesta vastaa thl. Koulutuksista tulee ilmoitukset ja niihin osallistutaan tarpeen mukaan.
Iloq – lukitusjärjestelmää käyttää Vain muutama työntekijä. Koulutus on saatu Turvaykkösiltä joka on myynyt järjestelmän.

Visma/Nova – on taloushallinnon työntekijöiden käytössä johon ovat saaneet koulutuksen. Ohjelmaa käytetään asukkaiden vuokrien ja palveluiden laskutuksessa.

Vivago turvapuhelinjärjestelmä on hoitohenkilökunnan käytössä. He saavat koulutuksen sekä järjestelmän toimittajalta että sisäisessä koulutuksessa.

Toimintamallien koulutus ja perehdytys

Elpylle on laadittu koulutussuunnitelma vuosille 2015-2019. Siihen voidaan tehdä vielä tarkennuksia talousarvioita laadittaessa seuraavalle vuodelle. Siinä on pyritty ottamaan huomioon kaikki säännölliset koulutukset, mm myös eri ohjelmien ja tietojärjestelmien koulutukset.
Osasta koulutuksista henkilökunta saa todistuksen mutta läheskään kaikista ei. Silloin merkintä koulutuksesta tulee esimiehien yläpitämiin taulukoihin.
Tulevaisuuskeskusteluissa joita käydään kerran vuodessa, käydään läpi jokaisen työntekijän kohdalla osaamisalueet ja koulutustarpeet. Tässä on mahdollisuus ottaa puheeksi mahdollinen epävarmuus ja lisäkouluttautumisen tarve. Lisäksi jokainen työntekijä voi jättää kirjallisen koulutushakemuksen koska vaan joka käsitellään käytännössä muutaman päivän sisään.
Kaikkia työntekijöitä koskevat koulutukset, esim tietojärjestelmä, ohjelmisto koulutukset on yleensä kohdistettu koko henkilökunnalle. Kouluttaja tulee silloin taloon jolloin tavoitetaan useita työntekijöitä kerrallaan.

Tietojärjestelmien käyttökoulutus
Viittaa edelliseen kappaleeseen.

Riittävä kokemus
Viittaan kappaleeseen toimintamallien koulutus ja perehdytys.

Ohjeet ja koulutus potilastietojen käsittelystä
Potilas asiamies on ollut kouluttamassa henkilökuntaa potilasasiatietoihin liittyen. Lisäksi häntä voi konsultoida tarvittaessa. Kirjallista materiaalia löytyy myös.

4. Käyttöympäristön ja useiden järjestelmien yhteiset tietoturvakäytännöt

Menettelyt virhe- ja ongelmatilanteissa
Ongelman havaittuamme ilmoitamme asiasta kyseisen järjestelmän tukeen. Sieltä hoidetaan ongelma joko etänä tai tarvittaessa tulevat paikan päälle.
Jokaisella työntekijällä on vastuu ja velvollisuus ilmoittaa välittömästi järjestelmä virheestä mikäli järjestelmä on kriittinen toiminnan kannalta. Hälytysjärjestelmä on esimerkki kriittisestä järjestelmästä. Yleensä näillä kriittisillä järjestelmillä on 24/7 tuki palvelu olemassa. Tukipalveluiden numerot ja sähköpostiosoitteet löytyvät jokaisesta yksiköstä.
Sellaisella järjestelmällä jolla ei ole merkitystä asukkaan terveyden ja hyvinvoinnin kannalta ei ole kiireellinen/kriittinen. Sellaisten järjestelmien virheilmoitukset voi tehdä seuraavana arkena, mikäli virhe huomataan toimisto/virka ajan jälkeen.

Järjestelmien käyttöohjeiden hallinnointi ja saatavuus
Eri järjestelmien ohjeet on saatavilla järjestelmän tuottajalta. Ohjeet löytyvät tilasta jossa kyseistä järjestelmää käytetään. Lisäksi on mahdollista saada koulutusta järjestelmän tuottajilta jos siirrymme käyttämään uudempaa järjestelmää. Sama koskee, mikäli versiopäivityksen yhteydessä ohjelman käyttö muuttuu oleellisesti. Joihinkin ohjelmiin meillä on tehtynä huoltosopimus joka kattaa mm koulutukset pääkäyttäjille ja muille käyttäjille kerran tai kaksi vuodessa.
Lähes jokaiseen järjestelmään, ohjelmaan löytyy pääkäyttäjä joka on saanut kattavamman, syvemmän koulutuksen ohjelmaan ja joka tarvittaessa opastaa muita käyttäjiä.
Asiakastietojärjestelmä Doma care, jota käytetään eniten kaikista ohjelmista, on käytössä joka päivä, useita kertoja jokaisella laskutukseen ja hoivan ja huolenpitoon osallistuvalla. Opastuksen tähän pystyy jokainen työntekijä antamaan tarvittaessa.
Doma Caren ilmoitus ohjelmapäivityksistä näkyvät jokaisella kun ohjelma avataan omilla tunnuksilla. Jokaisella käyttäjällä on myös mahdollisuus esittää suoria kysymyksiä ohjelmisto tuottajalle suoraan omasta näkymästä kun ohjelman avaa. Vastaukset kysymyksiin näkyy myös suoraan itsellä etusivulla kun ohjelma avataan.
Prog-it tekee säännölliset kuukausi käynnit ja lisäksi on mahdollista saada apua ja tukea etänä. Käyttöjärjestelmien ja ohjelmien päivitykset tapahtuvat heidän toimestaan.

Järjestelmien asennus ja ylläpito yleisesti
ATK tukemme Prog-it huolehtii kaikkien ohjelmien asennuksesta ja päivityksestä yhteistyössä

ohjelmien tekijöiden kanssa. Ohjelmia ei ole mahdollista asentaa ilman admin tunnuksia. Henkilökunnalla ei ole käytössä admin tunnuksia.
Liitteenä lausunto Prog-it Oy:n konesali- ja tietoliikennepalveluiden tietoturvasta ja riskienhallinnasta jota valvoo Silverskin, Information Security.

Tilojen, työasemien, tallennusvälineiden ja tulosteiden turvallisuus
Tietokoneet ovat lukituissa toimistoissa joihin eivät pääse asiakkaat ilman valvontaa. Koneet ovat mahdollisuuksien mukaan sijoitettu niin että näyttö ei ole toimiston ovelle päin tai niin että ulkopuolinen pääsisi vahingossa näkemään. Mikäli tietokoneen sijoittelu ei ole ollut mahdollista toteuttaa niin kuin yllä on mainittu, on meillä käytössä näytön suoja joka estää näkemisen.
Tulostimia on joissakin toimistoissa joihin eivät asiakkaat pääse. Talon yleinen isompi tulostin sijaitsee erillisessä tilassa joka on lukossa. Näitä isompia tulostimia on yksi kummassakin palvelutalossa. Näihin on myös tulossa suojaus/koodisysteemi jolloin jokaisella on oma koodi jonka laittamalla vasta saa tulostimesta omat tulosteet. Tämä varmistaa vielä lisäksi että tulosteita ei pääse sivulliset lukemaan.
Osa tietokoneiden näytöistä lukkiutuu automaattisesti. Tarkoitus on ohjelmoida kaikki koneet tekemään sen. Osalla henkilökuntaa on käytössä oma työpuhelin jossa on pin-koodi ja suojakoodi mikä estää väärinkäytön.
Tableteille jokaiselle on määritelty omat tunnukset joilla kirjaudutaan asiakastietojärjestelmään.
ATK tukemme Prog-it huolehtii meillä kaikkien tietokoneiden suojauksesta, ohjelmien päivityksestä jne. Ohjelmia ei voi ladata itse, siihen tarvitaan admin tunnukset jotka ovat Prog-it:in käytössä.

Muut käyttöympäristön käytännöt.
Espoon lähimmäispalveluyhdistyksen kumppani konesali ja tukipalveluissa on Prog-It Oy.
Prog-It tuottaa tarvittavan konesalikapasiteetin, ylläpitää VPN tunnelit toimipisteiden välillä ja tuottaa lähi ja etätukipalvelut tarpeen mukaan.
Prog-It on vakavarainen ja vuodesta 1994 toiminut ICT:n asiantuntija.

Domacare asiakastietojärjestelmän toimittamisesta ja tukipalveluista vastaa Invian Oy

Espoon lähimmäispalveluyhdistyksen toimipisteissä käytetään Elisan ja Suomicomin tietoliikenneyhteyksiä.
Operaattori vastaa internetkapasiteetin tuottamisesta, tietoturvalaitteet ja VPN yhteydet hallinnoidaan Espoon lähimmäispalveluyhdistyksen omilla
Watchguard UTM laitteilla. Varayhteytenä toimipisteissä voidaan käyttää 3G/4G tekniikkaa.

Espoon lähimmäispalveluyhdistyksen etäyhteydet ovat hyvin rajoitetut.
Hallinnollisilla työntekijöillä on henkilökohtaiset VPN tunnukset, jotka on sidottu AD autentikointiin.
Salasanat vaihtuvat AD politiikan mukaisesti. Etäyhteydet on sallittu vain yhdistyksen omilta työasemilta.

Toimipisteiden välillä liikenne on salattu IPSec VPN tunnelein. Hallintohenkilökunnan käytössä on SSL VPN tyyppinen yhteys.

Langattomat verkot perustuvat keskitetysti hallittuun Watchguard AP tekniikkaan. Vierasverkon ja tuotantoverkon liikenne on eriytetty toisistaan omiin virtuaaliverkkoihinsa. Kaikki liikenne suodatetaan palomuurilaitteen läpi, verkkoliikenteestä voidaan tuottaa tarkka logi.
Käytetty tunnistautumistekniikka on WPA2 AES.

5. Käyttövaltuuksien, pääsynhallinnan ja käytön seurannan yleiset käytännöt

Käyttäjäryhmät
Yhdistyksen työntekijät joilla on tunnukset asiakastietojärjestelmä Doma caren, näkyy itse ohjelman käyttäjä rekisterissä johon vain pääkäyttäjällä on oikeus.
[Mistä on saatavissa dokumentaatio niistä käyttäjäryhmistä, jotka käyttävät asiakas- ja/tai potilastietojärjestelmiä. Kanta-palveluihin liittyvien tahojen osalta tulee myös olla dokumentoituna käyttäjäryhmien Kanta-palveluiden käyttöoikeudet.]

Käyttövaltuushallinnan ja käytön seurannan käytännöt
Yksikön esimiehet, vastuuhenkilöt jotka myös toimivat pääkäyttäjinä luovat käyttäjätunnukset työntekijöille asiakastietojärjestelmä Domacaren. Vastuuhenkilöt myös poistavat rekisteristä henkilöt joilla ei enää ole oikeuksia päästä asiakastietojärjestelmään. Tunnusten luominen tapahtuu itse Doma care järjestelmän kautta.
Rai asiakasrekisteriin pääsevät myös vain ne joilla on käyttöoikeus Domacare järjestelmään.
Hilmo rekisteriä käyttää vain yksikköjen esimiehet jotka ovat saaneet tunnukset suoraan Thl:ältä.
Visma/Nova taloushallinnon järjestelmää käytetään ainoastaan taloushallinnossa. Muilla ei ole oikeuksia sinne.

6. Kanta-palvelujen käytön tietoturvakäytännöt

Elpyn henkilökunta ei kuulu palveluntuottajina Kanta-palvelujen käyttäjiin.

7. Tietojärjestelmät

Kanta-palveluihin liittyvät tietojärjestelmät (luokka A)
Elpyllä ei ole käytössä Luokka A tietojärjestelmää

Muut asiakas- tai potilastietoja käsittelevät järjestelmät (luokka B)
Liitteenä Doma Care rekisteriseloste järjestelmästä ja sen käytöstä.

Muut tietojärjestelmät, jotka on otettava huomioon arkaluonteisten asiakas- ja potilastietojen suojaamisen kannalta
Liitteenä rekisteriselosteet eri järjestelmistä liittyen asiakas- ja potilasrekisteröintiin jotka ovat käytössä Elpyssä

8. Tietojärjestelmäkohtaiset ohjeet ja suunnitelmat

Viittaan tässä rekisteri selosteisiin ja muihin lausuntoihin jotka ovat liitteenä omavalvontasuunnitelmassa.

Päivitetty: 24.3.2017