Capri hoivapalvelut Oy

Y- 3294208-6

Tietoturvasuunnitelma

8.4.2024

Xhyljeta Dedolli- Kamal Sh,Th amk

vastuuhenkilö ja terveydenhuollosta vastaava johtaja

Sisällys

1. Tietoturvasuunnitelman käyttötarkoitus

Tämä THL:n määräykseen 3/2021 (THL/4309/4.09.00/2021) kuuluva liite.

Tämä dokumentti on *Capri Hoivapalvelut Oy:n tietoturvasuunnitelma*. Tämän tietoturvasuunnitelman käyttötarkoitus on täyttää uuden asiakastietolain[1] 784/2021 27 §:n ja THL:n määräyksen 3/2021 mukaiset velvoitteet. Suunnitelma kokoaa yhteen asiakastietolaissa vaaditut omavalvonnan kohteelta edellytettävät selvitykset ja vaatimukset.

Ennen uuden 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.

Tietoturvasuunnitelman laadinnan ja noudattamisen vastuu on sosiaali- ja terveydenhuollon palvelunantajan vastaavalla johtajalla.

Oleellista on täyttää asiakastietolain 784/2021 27 §:n 1 ja 2 moment

1) henkilöllä, joka käyttää tietojärjestelmiä, on niiden käytön vaatima koulutus
2) tietojärjestelmien yhteydessä on saatavilla niiden asianmukaisen käytön kannalta tarpeelliset käyttöohjeet.

   Capri Hoivapalvelut Oy:n henkilöstöön kuuluu yrittäjät Sh Xhyljeta Dedolli-Kamal ja Lh Zahidullah Kamal sekä terveyden- ja sosiaalialan työntekijöitä.
   Työntekijöillä on asiaan kuuluva koulutus ja työhön perehdytys järjestetty asiakastietojen tietojärjestelmän käyttämiseen.
   Käyttöohjeet tietojärjestelmän avaamiseen ja käyttöön perehdytetään ennen työn aloittamista, mutta työ- ja salassapitosopimuksen allekirjoituksen jälkeen.
   Sisään kirjautumiseen tarvitaan omat käyttäjätunnus ja salasana. Capri Hoivapalvelut Oy tulee vaatimaan käytännön syistä kaikilta mahdollisilta työntekijöiltä terveydenhuollon varmennekortin.

   Ohjelmiston tietoturvallisuudesta vastaa mm lokitiedoston suojaamisen osalta, ohjelmiston tuottaja.

2. Tietoturvasuunnitelman kohde ja päivityskäytännöt

Tämän tietoturvasuunnitelman piiriin kuuluvat:

- Nimi: Capri Hoivapalvelut Oy
- Y-tunnus: 3294208-6
- johtaja Xhyljeta Dedolli-Kamal Sh amk
- Suunnitelman piiriin kuuluvat kaikki yrityksen Työntekijät

Suunnitelman toteuttamisessa ja päivittämisessä noudatetaan seuraavia käytäntöjä:

- Suunnitelman ja sen päivittämisen toteuttamisen vastuuhenkilö on Sh Xhyljeta Dedolli-Kamal

[1] https://www.finlex.fi/fi/laki/alkup/2021/20210784#Pidp447918064

- Tarkistus- ja päivityskäytännöt:
  - Jokainen henkilö, joka saa käyttäjätunnukset toimipisteiden potilastietojärjestelmään allekirjoittaa kirjallisen vaitiolositoumuksen ja saa ohjeet asiakirjojen laatimiseen.
  - Kullakin työntekijällä on erikseen työpuhelin ja henkilökohtainen puhelin

- Suunnitelman seuranta ja seurannan dokumentointi:
  - Yrityksessä työskentelee kaksi yrittäjää ja vaihteleva määrä koulutettuja työntekijöitä
- Suunnitelma tukee päätöksiä hankintoja tehtäessä.
  - Yrityksellä on käytössä DomaCare toiminnanohjausjärjestelmä
  - Järjestelmä on mahdollista liittää yhteyteen THL/RAI ja Kanta potilastiedot
  - Sovelluksessa on mahdollisuus oikeustasojen rajoittamiseen työtehtävien mukaan.
  - Sovelluksen toimittaja vastaa tallennusten tietoturvasta ja esittää siitä *Capri Hoivapalvelut Oy*:lle kirjallisen selvityksen.
- Suunnitelman hyväksyy terveydenhuollon johtaja. Suunnitelmaa tarkastellaan vähintään 3x/vuosi omavalvontasuunnitelman kanssa samaan aikaan ja tarvittavat muutokset tehdään molempiin suunnitelmiin.

3. Yleiset tietoturvakäytännöt

Määräys 3/2021: 6.1 Yleiset tietoturvakäytännöt

Capri Hoivapalvelut Oy:ssä noudatetaan seuraavia yleisiä tietoturvakäytäntöjä ja tehdään tietoturvallisuus-, tietosuoja-, riskienhallinta- ja asiakastietojen käsittelyn omavalvontatyötä seuraavien dokumenttien mukaisesti:

Tietoturvallisuustyötä tehdään seuraavien dokumenttien mukaisesti:

- Capri Hoivapalvelut Oy toimii omassa toimistossa. Varsinainen työ tehdään asiakkaan kotona; kotihoito.
- Yrityksellä on toimisto, jossa dokumentointiin tarkoitetut koneet sijaitsevat.
  Yritys voi tuottaa alihankintaa tai vuokratyönä tehtyä palvelua palvelun ostajan tiloissa tai asiakkaan kotona, ohjelmistoilla ja laitteilla. Henkilöstövuokraus tai alihankintasopimuksessa Capri Hoivapalvelut Oy sitoutuu noudattamaan palvelun ostajan tietoturvallisuus määräyksiä ja vaitiolositoumusta.
  Pääsääntöisesti Capri Hoivapalvelut tekee pääsopijan roolissa työn suoraan hyvinvointialueelle tai yksityiselle asiakkaalle. Kirjaaminen tehdään omassa toimistossa yrityksen laitteilla tai mobiilisti asiakkaan luona.
- Ohjelmistoihin pääsee kirjautumaan käyttäjätunnuksella ja/ tai terveydenhuollon varmennekortilla.
- 20% tietoturvasta on teknistä ja fyysistä turvallisuutta: mm turvallinen tietoverkko, palomuurit, virustorjuntaohjelmat
- 80% hallinnollisia toimenpiteitä: henkilöstön tietotaito ja yrityksen päivittäiset toimintatavat, tietoturvaohjeet ja työn organisointi.

Yrityksen teknisestä tietoturvallisuudesta huolehditaan siten, että kaikki yrityksen laitteet ovat lukitussa huoneessa / tiloissa, johon pääsee vain henkilökohtaisesti kuitatulla avaimella tai sähkölukituksen koodilla / kortilla.

Kaikkiin toimistossa käytössä oleviin laitteisiin pääsee vain henkilökohtaisilla tunnuksilla. Laitteesta kirjaudutaan ulos ja laite sammutetaan. Asiakas- potilastietojärjestelmään ei pääse ilman

tunnuksia. Laitteita ei saa jättää avoimeksi , eikä ohjelmaa auki, jos poistuu huoneesta. Laitteet on sijoitettu siten, että näyttö ei ole ovelle päin.

HENKILÖTIETOJEN KÄSITTELYTOIMIEN KUVAUS
Dokumentin tarkoitus
Lakiin perustuvan velvoitteen täyttäminen.
Capri Hoivapalvelut Oy on rekisterinpitäjä omien asiakkaiden osalta.
Mikäli yritys tuottaa palvelua muulla saman alan toimijalle, kirjaukset tehdään sen yrityksen laitteilla rekisterin käyttäjän ominaisuudessa.

Alihankinta tehtävässä työssä Rekisterinpitäjä on tehnyt Käsittelijän (Capri hoivapalvelut Oy) kanssa sopimuksen, joka koskee sellaista palvelua, jossa käsittelijä toimii Rekisterinpitäjän ylläpitämään henkilötietorekisteriin kuuluvien henkilö- ja potilastietojen käsittelijänä.

Tässä dokumentissa kuvataan käsittelytoimet, joita Käsittelijä ja Rekisterinpitäjä henkilötietojen käsittelijänä tekee, henkilötietojen tyypit sekä käsiteltävät henkilötiedot.

Henkilötietojen käsittelyssä on noudatettava Käsittelijän ja Rekisterinpitäjän välistä sopimusta sekä Rekisterinpitäjän ohjeita.

Henkilötietojen tyypit ja rekisteröityjen ryhmät
Osapuolet sopivat, että Käsittelijä käsittelee Rekisterinpitäjän puolesta Sopimuksessa sovitun palvelun tuottamiseksi seuraavia Rekisterinpitäjän henkilörekisteriin kuuluvia henkilötietoja.
Rekisterinpitäjän asiakkaat / potilaat
Rekisterinpitäjän asiakkaiden henkilötiedot sekä asiakkaiden sosiaali- ja terveystiedot.
Osapuolet sopivat, että Käsittelijä käsittelee kyseisiä henkilötietoja, koska rekisterinpitäjä tilaa käsittelijältä terveydenhuoltolain mukaista palvelua. Tämän vuoksi Käsittelijän on käsiteltävä Rekisterinpitäjän asiakkaiden tietoja potilaiden hyvän ja turvallisen hoidon tuottamiseksi.

Omista asiakkaistaan Capri Hoivapalvelut pitää omaa rekisteriä, ja toimii silloin rekisterinpitäjänä.

Käsittelijä on nimennyt organisaatiossaan tietosuojavastaavan : Vivian Vuolasvirta Sh amk

Käsittelijänä ja rekisterinpitäjänä Capri Hoivapalveluilla on kirjallinen toimintaohje tietosuojaloukkaukseen (sisältyy tähän suunnitelmaan).

Käsittelijänä ja Rekisterinpitäjänä Capri Hoivapalvelut sitoutuu käsittelemään kaikkia potilasasiakirjoja sosiaalihuollon ja terveydenhuollon asiakkaan asiakirjoista laaditun lain mukaan. Käsittelijällä on oma potilasrekisteri, mutta ei yhteisrekisteriä kenenkään kanssa.

Käsittelijän ja rekisterinpitäjän roolissa Capri Hoivapalvelut Oy sitoutuu noudattamaan viranomaisten toiminnan julkisuudesta sekä muusta salassapidosta ja vaitiolovelvollisuudesta annettuja säädöksiä.

Käsittelijän alihankinta- sopimuksen mukaisessa toiminnassa syntyvät asiakkuutta koskevat asiakirjat ovat Rekisterinpitäjän asiakirjoja.

Rekisterinpitäjä varautuu siihen, että tietoja voidaan häiriöttä siirtää toiseen järjestelmään esim. vikatilanteessa tai poikkeusoloissa.

Käsittelijä sitoutuu käsittelemään asiakas- ja potilasasiakirjoja vain tämän sopimuksen mukaiseen potilastyöhön, korjaa havaitut virheet välittömästi, ilmoittaa tietosuojaloukkauksesta rekisterinpitäjälle heti huomattuaan sen ja dokumentoi sovitusti.

Mikäli Capri Hoivapalvelut Oy ostaa alihantana tuotettavaa palvelua muulta saman alan yritykseltä, koskee sopimusta se mitä yllä on kuvattu Capri Hoivapalvlut Oy:n osalta sen ollessa alihankkija.

Henkilötietojen käsittelyn kesto
Käsittelijä käsittelee tässä liitteessä mainittuja potilastietoja vain ollessaan rekisterinpitäjän työnjohdon tai valvonnan alaisessa työssä rekisterinpitäjän toimipisteessä.

Käsittelijä vastaa siitä, että palvelu on koko sopimusajan henkilötietolainsäädännön ja sopimuksen mukainen ja käsittelee potilastietoja sopimuksen mukaisesti.

Rekisteröityjen pyynnöt
Käsittelijä ohjaa viipymättä kaikki kaikkien rekisteröityjen pyynnöistä rekisteriä koskevat pyynnöt Rekisterinpitäjälle, ja avustaa Rekisterinpitäjää täyttämään velvollisuutensa.

TIETOSUOJALOUKKAUS

Tapahtuma, jossa henkilötietoja tuhoutuu, häviää, muuttuu, niitä luovutetaan luvattomasti tai niihin pääsee käsiksi asiaton taho.

esim. - yrityksen tietoja sisältävä tietokone, puhelin tai asiapapereita joutuu vieraan henkilön käsiin

- yrityksen asiakas- tai muun rekisterin tiedostoihin olevia käyttäjätunnuksia ja salasanoja joutuu väärän henkilön käyttöön
- Ongelmia syntyy myös, kun tietokone tai puhelin katoaa tai varastetaan, tietoja hakkeroidaan, järjestelmään lähetetään haittaohjelmia tai se joutuu kyberhyökkäyksen kohteeksi.
- Jos sattuu tulipalo datakeskuksessa, inhimillinen erehdys , terveystietojen postittaminen väärälle henkilölle?

Ilmoitus viranomaiselle ja rekisteröidylle

Siitä hetkestä, kun rekisterinpitäjä havaitsee tietosuojaloukkauksen, hänen on mahdollisuuksien mukaan **ilmoitettava siitä 72 tunnin sisällä valvontaviranomaiselle**. Jokainen organisaatio ja yksittäinen yrittäjä, joka tallentaa henkilötietoja, on rekisterinpitäjä.

Valvontaviranomaisena toimii **Tietosuojavaltuutetun toimisto**, joka sijaitsee Helsingissä. Sen puhelinneuvonta on auki maanantaista torstaihin klo 9-11 ja 13-15 sekä perjantaina klo 9-15. Puhelinnumero on 029 56 16670.

Ilmoituksen tekee **Rekisterinpitäjän** tietosuojavastaava .

Silloin, kun henkilötietojen tietoturvaloukkauksesta voi aiheutua riski henkilön oikeuksille ja vapauksille, ilmoitus on ehdottomasti tehtävä.

Tässä tapauksessa **rekisterinpitäjän on ilmoitettava** tietosuojaloukkauksesta myös **rekisteröidylle**. Tämän on tapahduttava viivyttelemättä. Rekisteröidylle henkilölle tieto tapahtuneesta on annettava niin selkeällä ja yksinkertaisella kielellä, että voidaan varmuudella sanoa hänen ymmärtäneen, mistä on kysymys.
Jos kyseessä on esim. muistisairas henkilö, pitää ilmoitus tehdä hänen etujaan valvovalle taholle (omainen, edunvalvoja).
Samassa yhteydessä **rekisteröidylle on annettava Palvelupisteen tietosuojavastaavan nimi**, yhteystiedot ja yhteyspiste mistä saa lisätietoja
Vastuu tietosuojaloukkauksesta ilmoittamisesta on AINA rekisterinpitäjällä. **Jos henkilötietojen käsittelijä (esim. alihankkija) havaitsee tietosuojaloukkauksen, on siitä ilmoitettava rekisterinpitäjälle välittömästi puhelimella ja kirjallisesti 12 tunnin kuluessa.**

Pelkkä ilmoitus ei riitä
Ei riitä, että rekisterinpitäjä ilmoittaa tietosuojaloukkauksesta valvontaviranomaiselle. Rekisterinpitäjän on myös **dokumentoitava kaikki henkilötietojen tietoturvaloukkaukset** ja pystyttävä osoittamaan niiden **vaikutukset ja korjaavat toimet.**

Dokumentointi on erittäin tarpeen, sillä dokumentaation avulla valvontaviranomainen voi tarkistaa, että tätä artiklaa on noudatettu. Mikäli dokumentteja ei ole tehty, viranomaistoimet ”rankistuvat” ja seuraukset voivat rahallisesti olla merkittävät.
Rekisteröidylle on kerrottava seuraukset
Ilmoitukseen on
1) kuvattava, mitä on tapahtunut
2) millaista ryhmää ihmisiä loukkaus koskee
3) millainen on loukattujen ryhmän profiili
4) kuinka suuresta joukosta ihmisiä on kysymys
5) todennäköiset seuraukset / vaikutukset
6) korjaavat toimenpiteet

Rekisterin **käsittelijän** tulee ilmoittaa tietosuoja-loukkauksesta **kirjallisesti rekisterinpitäjälle 36 tunnin** kuluessa siitä, kun loukkaus on huomattu.

Riskit on arvioitava

Rekisterinpitäjän vastuu henkilötietojen tietoturvaloukkauksen tapahtuessa on suuri. Hänen on kyettävä arvioimaan muun muassa **millainen riski vuodosta aiheutuu rekisteröidylle**. Tämän perusteella määräytyvät tehtävät jatkotoimet. Jos arvion tekeminen tuntuu liian vaikealta, silloin kannattaa ottaa yhteyttä tietosuojavaltuutetun toimistoon.

Mitä arkaluonteisempaan tietoon loukkaus kohdistuu, sitä suurempi riski siitä aiheutuu rekisteröidylle.

Rekisterinpitäjän pitää arvioida loukkauksen kohteeksi joutuneiden henkilötietojen luonne, arkaluonteisuus ja määrä. Hänen on myös pohdittava seurauksia. Ne voivat olla erilaisia riippuen siitä, mihin henkilötietoja on vuotanut. On eri asia, ovatko tiedot joutuneet esimerkiksi internetiin – tai jos niitä ei päästä käsittelemään tietojärjestelmä vian vuoksi.

Vakavia seurauksia

Rekisterinpitäjän on muistettava, että tietosuoja-asetus on nimenomaan säädetty suojaamaan yksityistä ihmistä, myös häntä itseään. Tietosuojaloukkausten seuraukset voivat olla inhimillisesti erittäin vakavia.

Capri Hoivapalvelut Oy:n tietosuojavastaava on Xhyljeta Dedolli-Kamal.

4. Menettelyt virhe- ja ongelmatilanteissa sekä jatkuvuudenhallinta

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

Capri Hoivapalvelut Oy on määritellyt poikkeusoloja varten yrityksen roolin ja tehtävät.

Capri Hoivapalvelut Oy:ssä työskentelee terveydenhuollon koulutettuja hoitajia, jotka osallistuvat poikkeusoloissa jatkuvuuden hallintaan ennalta suunnitellun mukaisesti siinä toimipisteessä, jonka kanssa poikkeusolojen toiminnasta on sovittu.

Palvelupisteet ovat varautuneet toiminnan häiriöttömään jatkumiseen erilaisissa poikkeusoloissa. Automaatio- ja GSM järjestelmissä poikkeus normaaliin on

- työvarausten / potilaslistojen katoaminen
- potilas /asiakastietojen palvelu- ja hoitosuunnitelmien katoaminen
- dokumentaation häiriintyminen
- laskutustietojen katoaminen
- välityspalveluna olevien Kanta-, Kela ja reseptikeskus yhteyksien katoaminen

Toimipisteet ovat tehneet varautumissuunnitelmansa potilasvastaanoton jatkumiseksi.

Useimmissa paikoissa on varavoimaa käytettävissä.

Hyvä perehdytys tilanteisiin.

Virhe- ja ongelmatilanteissa noudatetaan seuraavia toimintatapoja:

Mikäli tietojärjestelmät eivät toimi toteutetaan poikkeusolojen toimintatapaa potilaiden hoidon turvaamiseksi. Se voi tarkoittaa käsin kirjaamista ja edelleen tilanteen korjaannuttua tiedot viedään potilastietojärjestelmään. Tarvittaessa manuaalinen materiaali säilytetään kahden lukituksen takana palvelupisteen suunnitelmien mukaisesti.

Ongelman ollessa ulkopuolisessa palveluiden ja ohjelmistojen tuottajissa, potilastietojärjestelmän palveluntuottaja vastaa omista haittatilanteista. Mikäli kyseessä on rajattu tilanne, yhteys yleensä saadaan palveluntuottajaan.

Mikäli terveydenhuollon asiakkaan tietoja vuotaa sivullisille, siitä ilmoitetaan asiakkaalle itselleen, palvelun ostajalle , tehdään tietosuojaloukkausilmoitus (menettely kuvattu aiemmin).

Virus tai haittaohjelma koneessa. Konetta ei käytetä , se tarkistetaan ja selvitetään onko haittaohjelma tosiasiallisesti mahdollista poistaa siitä. Yleensä ei, joten tilalle hankitaan uusi kone. Viruksen saanut laite tuhotaan asianmukaisesti. Yhteistyöstä on sovittu atk laitteita tuhoavan yrityksen kanssa. Tuhoaminen tarkoittaa, että laitteesta poistetaan kaikki tieto purkamalla se osiin ja sen jälkeen osien lajittelu edelleen tuhottavaksi.

Capri Hoivapalvelut Oy:n laitteissa on yhteys vain omaan toiminnanohjausjärjestelmään.

Samaan aikaan tulee selvittää onko kyseessä hyökkäys kaikkiin toimipisteen koneisiin ja niiden käyttöä tulee välttää kunnes asia selviää. Jos kyseessä on tietty ohjelma, jossa haitta / virus esiintyy, sitä ohjelmaa ei avata ennen asian selvittämistä.

Tietojen kalastelua tapahtuu ajoittain, ja siihen on varauduttu. On etukäteen selvillä mistä voi tulla kysymyksiä tai tiedonhankintaa. Asiasta tehdään aina ilmoitus ja varoitetaan muita.

Mikäli tietojärjestelmissä on havaittavissa poikkeamia tai ne toimivat selvästi väärin, asiasta ilmoitetaan valvontaviranomaiselle ja ohjelman toimittajalle korjauksia varten. Ohjelman käyttöä vältetään, kunnes vika tai haitta on korjattu. Toimitaan, kuten poikkeusoloissa.

Merkittävästä riskistä ilmoitetaan Valviraan, ja jos kyseessä on esim. lääkkeisiin liittyvä tilanne, on lääkärille ilmoitettava asiasta ja apteekkiin . Asiakas asetetaan erityiseen tarkkailuun ,voinnin seurantaan ja kriittisimmät tapaukset päivystykseen monitoroitavaksi. Myös omaiselle ilmoitetaan välittömästi asiasta.

Tietosuojapoikkeamasta ohjeet tietosuojavaltuutetulle ilmoittamisesta.

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

5.1. Henkilöstön koulutus sekä osaamisen ylläpito ja kehittäminen

Määräys 3/2021: 6.3 Henkilöstön koulutus sekä osaamisen ylläpito ja kehittämine

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

Jokainen toimipiste antaa perehdytyksen tietojärjestelmiä koskevaan toimintaan. Capri Hoivapalvelut Oy:n henkilöstö varmistaa, että on tietoinen potilastietojärjestelmien toiminnoista.

5.2. Tietojärjestelmien käyttöohjeet ja ohjeiden mukainen käyttö

[**Määräys 3/2021**: 6.4 Tietojärjestelmien käyttöohjeet ja ohjeiden mukainen käyttö]

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

Yritys joutuu käyttämään eri toimipisteissä eri potilastiedon järjestelmiä.

Perehdytys ohjelmistojen käyttöön suoritetaan kaikissa toimipisteissä.

6. Tietojärjestelmien tietoturvakäytännöt

6.1. Tietojärjestelmien perustiedot, kuvaukset ja olennaisten vaatimusten täyttyminen

[**Määräys /2021**: 6.5 Tietojärjestelmien perustiedot, kuvaukset ja olennaisten vaatimusten täyttyminen]

Tietoturvakäytännöt ohjelmistoittain on esitelty sopimusta tehtäessä, silloin kun CApri Hoivapalvelut Oy toimii rekisterin (rekisterien) käsittelijänä.

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

Kaikki käytettävät ohjelmistot ovat yhteydessä Kanta-Palveluihin.

6.1.2. Muusta syystä tietoturva-auditoidut tietojärjestelmät (luokka A1)

ei muita järjestelmiä

Kaikki potilastietojärjestelmät, joita Capri Hoivapalvelut Oy toimipisteissä käyttää ovat A luokiteltuja.

6.1.3. Muut asiakastietoja käsittelevät järjestelmät (luokka B)

Luokkaa B kuuluviin (järjestelmät, jotka eivät ole yhteydessä Kanta-palveluihin) järjestelmiin, jos siihen on tarvetta.

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

ei muita asiakastietoja käsitteleviä järjestelmiä

6.1.5. Tietojärjestelmien olennaisten vaatimusten täyttyminen

Tietoja ylläpidetään ja päivitetään aina niiden muuttuessa.

6.2. Tietojärjestelmien asennus, ylläpito ja päivitys

[**Määräys 3/2021**: 6.6 Tietojärjestelmien asennus, ylläpito ja päivitys]

Ei asennuksia yrityksen laitteisiin.

6.3. Käyttövaltuuksien hallinnan ja tunnistautumisen käytännöt

[**Määräys 3/2021**: 6.7 Käyttövaltuuksien hallinnan ja tunnistautumisen käytännöt]

Ohjelmiston lataaminen henkilökohtaiseen laitteeseen ei ole sallittu.

Käyttöoikeuksien ja käyttövaltuuksien osalta noudatetaan seuraavia toimintatapoja:

Sopimussuhteen päättyessä käyttöoikeudet poistetaan 30 min viimeisen työvuoron päätyttyä. Koska kaikki kirjaaminen tulee tapahtua reaaliajassa ei tunnuksia tarvita enää työvuoron päätyttyä ja laite jää vastaanoton tiloihin suljettuna.

Käyttäjien tunnistamisessa ja todentamisessa noudatetaan seuraavia käytäntöjä:

Kaikkiin yrityksen laitteisiin on salasana, jolla pääsee laitteen käyttöön. Laitteen kadotessa ulkopuolinen henkilö ei saa laitetta aktivoitua.

Asiakaskirjauksiin ja työjärjestelyihin pääsee omilla tunnuksilla: käyttäjätunnus ja salasana, käyttöoikeustason mukaan. Vaaditaan terveydenhuollon ammatti/ varmennekortti.

6.4. Asiakas- ja potilastietojärjestelmien pääsynhallinnan ja käytön seurannan käytännöt

[**Määräys 3/2021**: 6.8 Asiakas- ja potilastietojärjestelmien pääsynhallinnan ja käytön seurannan käytännöt]

Asiakastietoja käsittelevien järjestelmien pääsynhallintaa ja käytön seurantaa toteutetaan seuraavasti:

Järjestelmät kirjaavat lokitietoihin kaikki ohjelmistoon kirjautumiset. Lokitiedoista voidaan selvittää kuka ja milloin on ollut kirjautuneena ohjelmistoon.

Tietosuojaloukkaus selitetään kaikille perehdytyksessä.

Mikäli Kela luovuttaa rekisterin pitäjälle tietoja kuten reseptikeskuksen lääkitykseen liittyviä tietoja, siitä kerrotaan asiakkaalle itselleen ja kerrotaan: hänen oikeuksistaan, minne tietoja luovutetaan, millä ehdoilla luovutetaan, hänen oikeutensa vaikuttaa tietojen liikkumiseen, toimintajärjestelmien periaatteista ja hallinnoijasta, miten hänen tietonsa on suojattu ja omakannasta ja miten sinne voi kirjautua.

7. Tietojärjestelmien käyttöympäristön tietoturvakäytännöt

7.1. Fyysinen turvallisuus osana tietojärjestelmien käyttöympäristön turvallisuutta

[**Määräys 3/2021**: 6.9 Fyysinen turvallisuus osana tietojärjestelmien käyttöympäristön turvallisuutta]

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

Näyttöpäätteet on sijoitettu siten, että käytävältä katsoen ei näe näyttöä. Käyttämätön pääte lukittuu 5 min kuluessa viimeistä kosketuksesta. Jokaisella työntekijällä on omat tunnukset joilla voi edetä ohjelmistoon, kun on saanut koneen auki.

Ulkoisten kovalevyjen tai muistitikkujen käyttö ei ole sallittu. Omien laitteiden kuten kannettavat tietokoneet tuominen ei ole sallittu työpaikalle.

Tulostimet sijaitsevat pääteiden välittömässä läheisyydessä. Joka päivä tarkistetaan että tulostimeen ei ole jäänyt tulostumattomia papereita.

Kaikki sosiaali- tai terveydenhuollon paperitulosteet säilytetään paloturvallisessa kaapissa toimistossa. Kaappi on lukittu ja siihen on kahdet avaimet. tarpeettomat asiakirjat tuhotaan tietoturvallisesti tietoturvajätteenä. Ennen lopullista tuhoamista ne säilytetään silputtuna lukitussa jätesäiliössä, joka tyhjennetään tietoturvallisia tapoja noudattaen.

7.2. Työasemien, mobiililaitteiden ja käyttöympäristön tukipalveluiden hallinta

[**Määräys 3/2021**: 6.10 Työasemien, mobiililaitteiden ja käyttöympäristön tukipalveluiden hallinta]

Työasemien, mobiililaitteiden ja käyttöympäristön tukipalveluiden tietoturvallisuudesta huolehditaan seuraavasti:

Vastuu- ja työnjako kysymyksiin oman ja ulkoistetun toiminnan välillä, on tehty sopimus. Mikäli alihankkija tuottaa osan palvelua, alihankkijan työntekijä noudattaa samoja sääntöjä laitteiden käytössä kuin yrityksen oma henkilöstö. Ja sama koskee vuokratyönä tehtävää palvelua. Vuokratyöntekijä tai alihankkija ei saa ladata ohjelmistoa omalle laitteelle, vaan käyttää vastaanoton laitetta ja allekirjoittaa samat tietosuojaa ja salassapitoa koskevat sopimukset. Samoin perehdytys tietosuojasta on sama kuin omalle henkilöstölle. Lähtökohtana on silti, että alihankkijana toimivan yrityksen vastuuhenkilö vastaa kuitenkin oman henkilöstönsä perehdytyksestä ja ohjeistuksesta.

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

[**Määräys 3/2021**: 6.11 Alusta- ja verkkopalvelujen tietoturvallinen käyttö tietosuojan ja varautumisen kannalta]

Alusta- ja verkkopalveluiden tietoturvallisuudesta huolehditaan seuraavasti:

Yleistä

Tietoverkkojen hallinta, verkkolaitteet, langattomat verkot ja reitittimet,

Sopimuksissa on kuvattu miten paljon tietoa ohjelmalta saadaan offline tilassa , jos verkkoon ei saada yhteyttä.
Toiminnassa pyritään varmistettujen verkkojen käyttöön, ei langattomiin.
Reitit ykset ovat vain yrityksen käytössä, ja ne on suojattu kaikin tarjolla olevin keinoin.
Langaton verkko tulee suojata vähintään WPA2-AES- salauksella.
Lisäksi virustorjunnat ja hyökkäysyritysten ilmoitus.

Salasana vaaditaan aina langatonta verkkoa käytettäessä ja se vaihdetaan riittävän usein, vähintään kerran kuukaudessa.
Toimipisteen sisäistä verkkoa ei anneta vierailijoiden käyttöön, vierailijat saavat eri verkon tai käyttävät omia verkkoja (jakavat omasta puhelimesta)

Palomuuri valitaan siten, että se suojaa etätyönä tehtävää työtä ja laitteita. Etätyönä käytettävät laitteet suojataan esim. päätoimipisteen palomuurin kanssa yhteensopivan VPN- ohjelmiston kanssa.
Käytämme asiantuntijoita näiden verkkojen ja palomuurien rakentamisessa ja huollossa.

Capri Hoivapalvelut Oy ei tee etävastaanottoja.

Henkilötietoja ei käsitellä Suomen rajojen ulkopuolella.

8. Kanta-palvelujen liittymisen ja käytön tietoturvakäytännöt

[**Määräys 3/2021**: 6.12 Kanta-palvelujen liittymisen ja käytön tietoturvakäytännöt]

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

Kanta-Palvelujen osalta käyttäjät ovat terveydenhuollon ammattihenkilöitä, joilla on voimassaoleva sosiaali- ja terveydenhuollon sote- varmennekortti.

Sote-organisaatiorekisteri tietojen tai IAH-koodiston tietojen tarkastaminen:
1.1.2024 soteri- rekisteri

- Yritys tarkastaa tiedot kansallisen koodistopalvelun Sote-organisaatio rekisteristä / Soteri- rekisterissä
- virheellisten tietojen korjaukset ja lisäykset tehdään yrityksen omasta aloitteesta suoraan soteri- rekisteriin.
- Otetaan huomioon eri aikaan tapahtuvat rekisterien muutokset
- otettava huomioon myös muutostilanteissa tehtävät päivitykset

Kanta-palveluihin (tietojärjestelmä taso A1) ovat yhteydessä Toimipisteen lääkärit ja sairaanhoitajat .

9.1. Järjestelmät X (luokkiin A2 ja A3 kuuluvat)

A2 ja A3 ovat Kelan kanssa yhteyteen vaaditut luokitukset.

muissa luvuissa kuvatut käytännöt

- käyttöohjeet:
- ohjeiden päivittäminen ja jakelu:
- menettelyt virhe- ja ongelmatilanteissa:
- järjestelmäkohtaiset tukipalvelut:
- asennus- ja ylläpitovastuut ja -vaatimukset:
- menettelytavat ja vastuut virhe- ja poikkeustilanteissa:
- käyttövaltuushallinta järjestelmässä:
- kirjautuminen järjestelmässä:
- lokit:
- järjestelmän lukittuminen:
- Kantaan liittyvän järjestelmän tietoturvallisuuden arviointia koskevan todistuksen tietojen varmistaminen (luokka A):
- järjestelmän tiedot Kelan testaustulokset sivulla (luokka A):
- järjestelmän tiedot Valviran tietojärjestelmä rekisterissä:
    - tietojärjestelmän tietojen tarkastusajankohta Valviran tietojärjestelmä rekisteristä
    - tietojärjestelmän tietoturvallisuus todistuksen voimassaolon päättymispäivä
    - tietojärjestelmään toteutetut olennaisten vaatimusten profiilit
    - tietojärjestelmälle hyväksytysti suoritetut Kelan Kanta-palvelujen yhteistestaukset (Valviran tietojärjestelmä rekisteristä ja/tai Kelan testaustulokset sivulta)
    - Valviran tietojärjestelmä rekisteristä mahdollisesti löytyvät tietojärjestelmien käytössä tai käyttöönotossa huomioitavat asiat

9.2. Järjestelmät X (luokkaan A1 kuuluvat)

Kanta-palveluihin yhteydessä

- järjestelmäversio, toimittaja, yhteystiedot:
- käyttötarkoitus
- käyttäjäryhmät:

luvuissa 3-5 kuvatut käytännöt

- käyttöohjeet:
- ohjeiden päivittäminen ja jakelu:
- menettelyt virhe- ja ongelmatilanteissa:
- järjestelmäkohtaiset tukipalvelut:
- asennus- ja ylläpitovastuut ja -vaatimukset:
- menettelytavat ja vastuut virhe- ja poikkeustilanteissa:
- käyttövaltuushallinta järjestelmässä:
- kirjautuminen järjestelmässä:
- lokit:
- järjestelmän lukittuminen:
- Luokkaan A1 kuuluvan järjestelmän tietoturvallisuuden arviointia koskevan todistuksen tietojen varmistaminen:
- järjestelmän tiedot Kelan testaustulokset sivulla (luokka A):
- järjestelmän tiedot Valviran tietojärjestelmärekisterissä:
    - tietojärjestelmän tietojen tarkastusajankohta Valviran tietojärjestelmä rekisteristä
    - tietojärjestelmän tietoturvallisuus- todistuksen voimassaolon päättymispäivä
    - tietojärjestelmään toteutetut olennaisten vaatimusten profiilit

- mahdolliset maininnat järjestelmän osallistumisesta yhteistestaukseen osana laajempaa tietojärjestelmäkokonaisuutta (Valviran tietojärjestelmärekisteristä ja/tai Kelan testaustulokset sivulta)
- Valviran tietojärjestelmärekisteristä mahdollisesti löytyvät tietojärjestelmien käytössä tai käyttöönotossa huomioitavat asiat

9.3. Järjestelmät Y (luokkaan B kuuluvat)

- järjestelmä, versio, toimittaja, yhteystiedot
- Käyttötarkoitus: sosiaalihuollon toiminnan ohjaus
- käyttäjäryhmät: ei käyttäjiä

tietoturvasuunnitelman luvuissa 3-5 kuvatut käytännöt

- käyttöohjeet:
- ohjeiden päivittäminen ja jakelu:
- menettelyt virhe- ja ongelmatilanteissa:
- järjestelmäkohtaiset tukipalvelut:
- asennus- ja ylläpitovastuut ja -vaatimukset:
- menettelytavat ja vastuut virhe- ja poikkeustilanteissa:
- käyttövaltuushallinta järjestelmässä:
- tunnistautuminen järjestelmässä:
- lokit:
- järjestelmän lukittuminen:
- järjestelmän tiedot Valviran tietojärjestelmärekisterissä:
  - tietojärjestelmän tietojen tarkastusajankohta Valviran tietojärjestelmärekisteristä
  - tietojärjestelmään toteutetut olennaisten vaatimusten profiilit
  - Valviran tietojärjestelmärekisteristä mahdollisesti löytyvät tietojärjestelmien käytössä tai käyttöönotossa huomioitavat asiat

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

Ei muita järjestelmiä.