Toimintaohje: Tietosuoja- ja tietoturvakäsikirja

Vastuualue: Hallintopalvelut
Hyväksytty: Pohjois-Karjalan hyvinvointialueen tietosuojatyöryhmä 9.11.2023
Tiedostopankin hyväksyjä: hallintopäällikkö Sini Rantaeskola
Laatijat: tietosuojavastaava Johanna Roivas, tietosuoja-asiantuntija Maarit Keränen

Versiohistoria

Päivämäärä	Tehty muutos	Tekijä
13.12.2023	Julkaistu Siun soten intrassa (Tiedostopankki). Poistettu käsikirjan julkaisun yhteydessä seuraavat asiakirjat ja ohjeet tiedostopankista: -Tietosuoja- ja tietoturvakäsikirja (versio 15.5.2020) -Sosiaalihuollon asiakastietojen käsittely (versio 22.9.2022) -Potilasrekisterin tietosuojaohje (versio 26.2.2020) -Virhekäynti Mediatrin potilastiedoissa ja tietojen korjaaminen (versio 14.12.2021) -Mediatrinumeron käyttö Teamsissa (versio 10.2.2021) -Whatsapp ja Teams-palvelujen käyttö (versio 23.3.2020) -Etätyön tietoturva ja tietosuoja (versio 19.3.2020) -Potilastietojen kopiointi (versio 18.12.2019) -Ohje tietojen luovutuksesta sijaisperheessä oleva lapsi (versio 11.9.2009)	tietosuojavastaava
11.4.2024	Kappale 8.4 Potilastiedon kirjaaminen: lisätty vinkki Mediatrin ajanvarauskirjan tietojen kirjaamisen käytännöstä (s.55).	tietosuoja-asiantuntija
18.9.2024	Kappale 13.3.3 Suojattu sähköposti: lisätty vinkki suojatun sähköpostin TSL-yhteydestä. Päivitetty tiedoston hyväksyjä.	tietosuoja-asiantuntija

Sisällysluettelo

1 Johdanto

EU:n yleisen tietosuoja-asetuksen (679/2016) tarkoituksena on parantaa henkilötietojen suojaa ja antaa ihmisille enemmän keinoja hallita heidän tietojensa käsittelyä. Asetus vastaa uusiin digitalisaatioon ja globalisaatioon liittyviin tietosuojakysymyksiin ja yhtenäistää tietosuojasääntelyä kaikissa EU-maissa. Tietosuoja-asetusta alettiin soveltaa vuonna 2018 kaikessa henkilötietojen käsittelyssä. Vuoden 2019 alusta voimaan tullutta kansallista tietosuojalakia (1050/2018) alettiin soveltaa rinnakkain tietosuoja-asetuksen kanssa ja laissa on täsmennetty EU:n tietosuoja-asetuksen määräyksiä. Näiden lisäksi henkilötietojen käsittelyä ohjaavat monet muut lait, kuten esimerkiksi laki viranomaisten toiminnan julkisuudesta (621/1999) eli nk. julkisuuslaki sekä sosiaali- ja terveydenhuollon ja pelastustoimen erityislainsäädäntö.

Tietosuoja- ja tietoturvakäsikirjan tavoitteena on ohjata Pohjois-Karjalan hyvinvointialueen (jatkossa Siun sote) henkilöstöä toimimaan tietosuojalainsäädännön mukaisesti ja täyttämään tietosuojalainsäädännön velvoitteet toiminnassaan, kunnioittaen ihmisten yksityisyyttä sekä heidän oikeuksiaan henkilötietojen käsittelyssä. Käsikirjan on hyväksynyt Siun soten tietosuojatyöryhmä 9.11.2023. Käsikirjaa ylläpitävät Siun soten tietosuojavastaavat. Käsikirja on jatkuvasti päivittyvä dokumentti, jonka viimeisin versio on saatavilla Siun soten intran Tiedostopankissa.

Tietosuoja rakentuu paloista, jotka on koottava yhteen yksi palanen kerrallaan. Kokonaiseksi tietosuojan palapelin saa vain yhteistyöllä!

2 Keskeisiä käsitteitä

2.1 Tietosuoja

Tietosuojalla tarkoitetaan henkilötietojen suojaa ja henkilötietojen käsittelyä lainmukaisesti yksilön perusoikeuksia kunnioittaen. Henkilötietoja saavat käsitellä vain ne henkilöt ja tahot, joilla on siihen laillinen oikeus. Tietosuojasta huolehtiminen ja sen toteutuminen edellyttää annettujen ohjeiden noudattamista, henkilöstön koulutusta ja osaamisen kehittämistä sekä tietosuojakulttuurin ottamista osaksi arjen toimintaa.

2.2 Tietoturva

Tietoturva on yksi tietosuojan toteuttamisen keino ja siksi se liittyy läheisesti tietosuojaan. Tietoturvalla tarkoitetaan tietojenkäsittelyn turvaamista teknisin ja hallinnollisin ratkaisuin, varmistaen mm. tiedon saatavuus, eheys, käytettävyys sekä tietojen salassapito ja tietojen rajatut käyttöoikeudet.

2.3 Henkilötieto

Henkilötiedolla tarkoitetaan kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyviä tietoja. Tunnistettavana pidetään sellaista henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen (mm. nimi, henkilötunnus) tai yhden tai useamman hänelle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella.

Henkilötietoja ovat henkilön nimen ja henkilötunnuksen lisäksi myös mm. henkilön kotiosoite, puhelinnumero, henkilön kasvot sisältävä kuva, sijaintitieto, auton rekisterinumero, kiinteistötunnus, työaseman IP-osoite tai sormenjälki. Henkilöön liitettäviä tietoja voivat olla myös esimerkiksi terveystiedot tai hänen saamansa tai hänelle myönnetyn palvelun tiedot. Henkilötietoja ovat myös sellaiset tiedot, joista ei suoraan käy ilmi ketä ne koskettavat, mutta jotka ovat yhdistettävissä henkilöön yhdistämällä tiedot muualta saatavaan tietoon.

2.4 Erityisiin henkilötietoryhmiin kuuluva henkilötieto

Erityisiin henkilötietoryhmiin kuuluvien henkilötietojen käsittely on lähtökohtaisesti kiellettyä. Tällaisista henkilötiedoista ilmenee henkilön rotu tai etninen alkuperä, poliittinen mielipide, uskonnollinen tai filosofinen vakaumus, ammattiliiton jäsenyys, geneettinen tai biometrinen tieto henkilön tunnistamista varten, terveyttä koskeva tieto tai henkilön seksuaalista käyttäytymistä tai suuntautumista koskeva tieto. Tietosuoja-asetuksen mukaisesti em. tietoja voi kuitenkin käsitellä, mikäli mm. henkilö on antanut käsittelyyn nimenomaisen suostumuksen, käsittely on tarpeen rekisterinpitäjän tai rekisteröidyn velvoitteiden ja erityisten oikeuksien noudattamiseksi. Tietosuojalain mukaisesti erityisiin henkilötietoryhmiin kuuluvia henkilötietoja voi käsitellä, kun mm. terveydenhuollon palvelun- tai sosiaalihuollon palveluntarjoaja järjestäessään tai tuottaessaan palveluja käsittelee toiminnassa saamiaan tietoja.

2.5 Henkilötietojen käsittely

Henkilötietojen käsittely tarkoittaa henkilötietoihin kohdistettua toimintaa. Käsittely voi olla joko automaattista tietojärjestelmällä tapahtuvaa tai paperisten asiakirjojen manuaalista käsittelyä. Tiedon käsittelyä on tietojen kerääminen, tallentaminen, järjestäminen, jäsentäminen, säilyttäminen, muokkaaminen tai muuttaminen, kysely, käyttö, tietojen luovuttaminen tai asettaminen saataville, tietojen yhteensovittaminen tai yhdistäminen, käytön rajoittaminen, tulostaminen, poisto tai tuhoaminen. Myös tiedon haku tai lataaminen sähköisestä järjestelmästä tai tietokannasta on henkilötietojen käsittelyä. Henkilötiedon käsittelyksi on myös hyvä tunnistaa pelkkä tietojen katselu eli lukeminen tai tietojen selaaminen.

2.6 Henkilötietojen tietoturvaloukkaus

Henkilötietojen tietoturvaloukkauksella tarkoitetaan tapahtumaa, jonka seurauksena henkilötietoja tuhoutuu, häviää, muuttuu tai niitä luovutetaan luvattomasti sivulliselle tai niihin pääsee käsiksi taho, jolla ei ole tietojen käsittelyoikeutta. Tietoturvaloukkaus voi olla tahallinen tai tahaton tapahtuma. Tietoturvaloukkauksesta voi seurata esimerkiksi henkilötietojen valvomiskyvyn menettäminen, identiteettivarkaus tai petos, maineen vahingoittuminen tai pseudonymisoitujen tai salassapitovelvollisuuden alaisten henkilötietojen paljastuminen.

Jokainen työntekijä on velvollinen ilmoittamaan tietoturvaloukkauksesta esihenkilölleen tai Siun soten tietosuojavastaavalle. Siun sotella on rekisterinpitäjänä velvollisuus dokumentoida kaikki tietoturvaloukkaukset sekä niiden vaikutukset ja toteutetut korjaavat toimet riippumatta siitä, mitä toimenpiteitä tietoturvaloukkauksesta lopulta seuraa. Henkilötietojen tietoturvaloukkauksesta täytyy ilmoittaa valvontaviranomaiselle mahdollisuuksien mukaan 72 tunnin kuluessa, jos loukkauksesta voi aiheutua riski luonnollisten henkilöiden oikeuksille ja vapauksille. Henkilötietojen tietoturvaloukkauksesta on ilmoitettava myös loukkauksen kohteena olevalle henkilölle, jos tapahtuma todennäköisesti aiheuttaa korkean riskin tämän oikeuksille ja vapauksille. Valvontaviranomaiselle ilmoituksen tekee tarvittaessa Siun soten tietosuojavastaava, joka auttaa esihenkilöitä tapahtumaan liittyvien riskien arvioimisessa sekä tarvittaessa toimenpiteiden suunnittelussa.

2.7 Tietoturvapoikkeama

Tietoturvapoikkeamalla tarkoitetaan esimerkiksi tietojen kalastelua, tietomurtoa, haittaohjelmahyökkäystä tai palvelunestohyökkäystä tai niiden yritystä. Tietoturvapoikkeama voi olla tahallinen tai tahaton tapahtuma, jonka seurauksena tietojen tai palvelujen eheys, luottamuksellisuus ja saavutettavuus voi heiketä. Kaikki tietoturvapoikkeamat ja niiden epäilyt on otettava vakavasti.

Jokainen työntekijä on velvollinen ilmoittamaan tietoturvapoikkeamasta tai sen epäilystä esihenkilölleen tai Siun soten turvallisuuspäällikölle, digijohtajalle tai Meidän IT ja talous Oy:lle. Huomioitavaa on, että tietoturvapoikkeaman vuoksi myös henkilötiedot saattavat olla uhattuina. Tietoturvapoikkeaman arvioinnissa on aina siis otettava huomioon, kuinka se vaikuttaa mahdollisesti henkilötietoihin, millaisia seurauksia poikkeamasta on henkilötiedoille sekä kohteena oleville henkilöille. Tarvittaessa tapahtuma on käsiteltävä myös henkilötietojen tietoturvaloukkauksena.

2.8 Rekisteröity

Rekisteröity tarkoittaa henkilöä, jonka tietoja on tallennettu johonkin rekisteriin ja jonka tietoja käsitellään ennalta määriteltyä käyttötarkoitusta varten. Siun sotessa rekisteröityjä ovat esimerkiksi asiakkaat ja potilaat sekä Siun soten työntekijät.

Rekisteröidyllä on myös erilaisia oikeuksia, joita hän voi käyttää sen perusteella, mikä on ollut henkilötietojen käsittelyn oikeusperuste. Rekisteröidyllä voi olla esimerkiksi oikeus saada tietoa henkilötietojensa käsittelystä, oikeus tutustua tietoihin ja oikaista niitä tai rajoittaa niiden käsittelyä.

2.9 Rekisteri

Rekisteri tarkoittaa henkilötiedoista koostuvaa tietojoukkoa, josta tiedot ovat saatavilla tietyin perustein. Rekisterissä olevat tiedot on kerätty samaa käyttötarkoitusta varten. Rekisterin sisältämät tiedot voivat olla sähköisessä järjestelmässä ja/tai paperilla. Siun sotessa tällaisia rekistereitä ovat esimerkiksi potilaiden terveystiedoista koostuva terveydenhuollon potilasrekisteri, asiakkaiden sosiaalihuollon asiakastietoista koostuva asiakasrekisteri sekä Siun soten työntekijöiden tiedoista koostuva henkilöstön rekisteri.

Huomioitavaa on, että yhden rekisterin tietoja voi olla useammassa tietojärjestelmässä tai vastaavasti samalla tietojärjestelmällä voi käsitellä eri rekisterin tietoja käyttöoikeuksin rajattuna.

2.10 Rekisterinpitäjä

Rekisterinpitäjällä tarkoitetaan tahoa, joka määrittelee, mihin tarkoitukseen ja millä tavalla henkilötietoja käsitellään. Rekisterinpitäjällä on velvollisuus ja vastuu toimia tietosuojaperiaatteiden mukaisesti sekä osoittaa noudattavansa toiminnassaan tietosuojalainsäädäntöä.

Siun sote toimii rekisterinpitäjänä sen toiminnassa syntyville tai toimintaa varten kerätyille ja tallennetuille tiedoille. Rekisterinpitäjänä toimii Siun soten aluehallitus. Siun soten eri henkilötietoja sisältäville rekistereille on nimetty rekisterinpitäjän edustajat, jotka edustavat rekisterinpitäjää, kun on kyse tietosuoja-asetukseen perustuvista rekisterinpitäjän velvollisuuksista. Rekisterinpitäjyys ja rekisterinpitäjän edustajuus pohjautuvat Siun soten hallintosääntöön.

2.11 Tietosuojavastaava

Siun soten tietosuojavastaavat ovat hyvinvointialuejohtajan nimeämiä tietosuoja-asiantuntijoita, joiden tehtävät ja asema on määritelty EU:n yleisessä tietosuoja-asetuksessa. Tietosuojavastaavat seuraavat ja valvovat henkilötietojen käsittelyä sekä tietosuojasäännösten ja -ohjeiden noudattamista Siun sotessa. He neuvovat ja ohjaavat työntekijöitä, esihenkilöitä ja johtoa sekä asiakkaita tietosuojakysymyksissä sekä toimivat asiantuntijoina vaikutustenarvioinnin prosessissa (DPIA). He seuraavat tietoturvaloukkausten ilmoitusvelvollisuuden toteutumista ja toimivat yhteyshenkilönä Siun soten ja viranomaisten välillä henkilötietojen käsittelyyn liittyvissä kysymyksissä. Tietosuojavastaavat myös toteuttavat lakisääteistä raportointia Siun soten johtoryhmälle tietosuojan tilasta ja kehittämistarpeista.

2.12 Tietosuojavaltuutetun toimisto

Tietosuojavaltuutetun toimisto on kansallinen valvontaviranomainen, joka valvoo tietosuojalainsäädännön noudattamista ja muiden henkilötietojen käsittelyä koskevien lakien noudattamista. Tietosuojavaltuutetun toimisto on itsenäinen ja riippumaton viranomainen. Tietosuojavaltuutetun toimistossa työskentelee tietosuojavaltuutetun sekä apulaistietosuojavaltuutettujen lisäksi asiantuntijoita. Tietosuojavaltuutetun toimiston verkkosivuilta[1] voi lukea lisää tietosuojavaltuutetun tehtävistä sekä hyödyntää sivuilta löytyvää tietosuojaan liittyvää tietoa.

2.13 Tietosuojaa koskeva vaikutustenarviointi (DPIA)

Tietosuojan vaikutustenarviointi auttaa tunnistamaan ja hallitsemaan henkilötietojen käsittelystä aiheutuvia riskejä. Arvioitavana ovat henkilötietojen käsittelyn vaikutukset henkilötietojen suojaan. Vaikutustenarviointi tulee tehdä aina, kun suunnitellaan asiakas- ja potilastietojen käsittelyä sekä muiden erityisiin henkilötietoryhmiin kuuluvien arkaluonteisten tietojen käsittelyä. Myös uuden teknologian käyttöönotto, geneettisten, biologisten tai sijaintitietojen käsittely ovat vaikutustenarvioinnin laatimiseen velvoittavia.

Vaikutustenarvioinnissa arvioidaan tietosuojaperiaatteiden toteutumista. Mikäli henkilötietojen käsittely todennäköisesti aiheuttaisi rekisteröidyn oikeuksille riskejä, on riskien hallitsemiseksi pyrittävä tunnistamaan ja määrittelemään tarvittavat toimenpiteet. Tarvittaessa rekisterinpitäjä voi pyytää tietosuojavaltuutetulta ennakkokuulemista, mikäli riski jää edelleen korkeaksi toteutetuista toimenpiteistä huolimatta.

Ota tietosuojan peruskäsitteet haltuun!

Älä epäröi kysyä, jos jokin on epäselvää.

[1] Tietosuojavaltuutetun toimisto (verkkosivut)

3 Tietosuoja- ja tietoturvatyön vastuunjako ja velvollisuudet hyvinvointialueella

Siun sote toimii rekisterinpitäjänä, kun se määrittelee toiminnassaan ja palveluissaan henkilötietojen käsittelyn tarkoitukset ja keinot, tai kun sille on laissa säädetty rekisterinpitoa koskeva tehtävä. Siun soten aluehallitus hyväksyy hyvinvointialueelle tietosuoja- ja tietoturvapolitiikan[2], joka kuvaa tietosuojan ja tietoturvallisuuden periaatteet, tavoitteet, organisointitavat ja vastuut.

Tietosuoja on osa sosiaali- ja terveydenhuollon sekä pelastustoimen palvelujen laatua[3] sekä asiakas- ja potilasturvallisuutta[4]. Tietosuoja takaa myös työelämän hyvää laatua, jonka toteutumisesta Siun sote työnantajana vastaa. Tietosuojan ja tietoturvan vastuut eivät kuitenkaan rajaudu vain organisaatioihin tai toiminnan johtamiseen, vastuut ulottuvat myös jokaiseen työntekijään, joka tukee ja toteuttaa omalta osaltaan palvelujen laatua ja turvallisuutta. Tietosuoja ja tietoturva ovat osa jokaisen Siun soten työntekijän työtä ja toiminnan arkea.

3.1 Henkilötietojen käsittelyssä on noudatettava tietosuojaperiaatteita

Tietosuojaperiaatteita on noudatettava aina käsiteltäessä henkilötietoja. Siun soten on rekisterinpitäjänä myös pystyttävä osoittamaan, että tietosuojaperiaatteet toteutuvat henkilötietojen käsittelyssä koko henkilötietojen käsittelyn elinkaaren ajan. Tietosuojaperiaatteet on huomioitava ja sisällytettävä kaikkiin henkilötietojen käsittelyn toimintoihin mahdollisimman varhaisessa vaiheessa, mm. suunniteltaessa henkilötietojen käsittelyä, hankittaessa uusia palveluja, tietojärjestelmiä tai hoitoa ja palvelua tukevia sovelluksia tai ohjelmistoja sekä kehitettäessä toimintaa ja prosesseja. Tietosuojaperiaatteet on kuvattu kuviossa 1.

[2] Siun sote – Tietosuoja- ja tietoturvapolitiikka (Siun sote intra)
[3] Siun sote – Laadunhallinta (Siun sote intra)
[4] Siun sote – Asiakas- ja potilasturvallisuus (Siun sote intra)

Lainmukaisuus, asianmukaisuus, läpinäkyvyys

Henkilötietojen käsittelyssä on noudatettava EU:n yleistä tietosuoja-asetusta tai muuta henkilötietojen käsittelyä koskevaa lainsäädäntöä. Henkilötietojen käsittelylle tulee olla aina käsittelyperuste. Henkilötietojen käsittelyn tulee olla asianmukaista ja kohtuullista suhteessa käsittelyn tarkoitukseen. Henkilötietojen käsittelystä tulee kertoa rekisteröidylle selkeästi ja ymmärrettävästi. Avoimuus ja ymmärrettävyys henkilötietojen käsittelyssä lisäävät luottamusta rekisterinpitäjään.

Käyttötarkoitussidonnaisuus

Henkilötietojen käsittelyn tarkoitus on suunniteltava ja määriteltävä selkeästi ennen käsittelyn aloittamista. Henkilötietoja saa kerätä vain tiettyä, nimenomaista ja laillista käyttötarkoitusta varten. Tietoja ei saa käsitellä alkuperäisten tarkoitusten kanssa yhteensopimattomalla tavalla myöhemmin. Käyttötarkoituksen määritteleminen auttaa rekisteröityä ymmärtämään, miksi hänen tietojaan tarvitaan ja päättämään, haluaako hän vaikuttaa henkilötietojensa käsittelyyn käyttämällä tietosuojaoikeuksiaan.

Tietojen minimointi

Käsiteltävien tietojen tulee olla asianmukaisia eli kerättyjen tietojen on oltava sellaisia, joilla kyetään täyttämään määritelty käyttötarkoitus. Käsiteltävien tietojen tulee olla olennaisia eli kerätyillä tiedoilla on oltava selkeä yhteys määriteltyyn käyttötarkoitukseen. Käsiteltävien tietojen tulee olla rajoitettuja eli välttämättömiä määritellyn käsittelytarkoituksen kannalta. Henkilötietoja ei saa kerätä tai käsitellä laajemmin kuin on välttämätöntä käyttötarkoituksen kannalta.

Tietojen täsmällisyys

Käsiteltävien henkilötietojen tulee olla täsmällisiä ja päivitettyjä. Epätarkat ja virheelliset henkilötiedot on oikaistava tai poistettava viipymättä. Epätäsmälliset ja virheelliset tiedot voivat vakavalla tavalla vaarantaa rekisteröityjen oikeuksia ja johtaa vääriin tulkintoihin ja toimenpiteisiin. Kun henkilötietoja luovutetaan tai niitä saadaan muualta, tiedon oheen tulee kirjata näkyviin tietolähde. Näin mahdollistetaan virheellisen tiedon korjaaminen myös alkuperäiselle tietolähteelle.

Säilytyksen rajoittaminen

Henkilötietoja saa säilyttää vain niin kauan kuin se on tarpeen tietojen käsittelytarkoitusta varten. Säilytysaika tulee suunnitella, perustella ja dokumentoida. Säilytysaikaa arvioidaan tilannekohtaisesti, huomioiden toimintaan vaikuttava lainsäädäntö sekä esimerkiksi asiakkaan reklamaatiomahdollisuus. Kun henkilötietoja ei enää tarvita, ne tulee anonymisoida tai poistaa, mikäli niille ei ole olemassa arkistointivelvoitetta.

Luottamuksellisuus ja turvallisuus

Henkilötietojen käsittelyn tulee olla luottamuksellista ja turvallista. Rekisterinpitäjän vastuulla on suojatoimin varmistaa järjestelmien, palvelujen ja tietojen luottamuksellisuus, eheys ja saatavuus sekä suojata henkilötietoja luvattomalta ja lainvastaiselta käytöltä tai esimerkiksi vahingossa tapahtuvalta häviämiseltä. Henkilötietoja on suojattava kaikissa niihin kohdistuvissa käsittelytoiminnoissa koko henkilötietojen käsittelyn elinkaaren ajan. Suojatoimia on ajoittain testattava ja niihin tulee tehdä tarvittavia parannuksia.

Kuva 1 Tietosuojaperiaatteet

3.2 Sisäänrakennettu ja oletusarvoinen tietosuoja

Sisäänrakennettu ja oletusarvoinen tietosuoja tarkoittaa, että Siun soten on otettava tietosuojaperiaatteet huomioon ja sisällytettävä ne kaikkiin henkilötietojen käsittelyn vaiheisiin mahdollisimman varhaisessa vaiheessa. Tietosuojaperiaatteet on otettava huomioon jo suunniteltaessa henkilötietojen käsittelyä sisältäviä toimintoja ja prosesseja tai kehitettäessä tietojärjestelmiä. Tietosuojaperiaatteiden lisäksi tärkeä osa sisäänrakennettua ja oletusarvoista tietosuojaa on riskienhallinta.

Tietosuojavaatimusten huomioon ottaminen ei ole vain Siun soten johtajien, lakimiesten tai tietosuojavastaavien tehtävä. Jokainen Siun soten työntekijä vastaa osaltaan siitä, että tietosuojan tarpeet tulee huomioiduksi henkilötietojen käsittelytoimissa, järjestelmissä ja palveluissa.

3.3 Tekniset ja organisatoriset toimenpiteet

Tietosuojaperiaatteiden toteuttamiseksi Siun soten tulee tehdä tarvittavat tekniset ja organisatoriset toimenpiteet. Tarvittavia toimenpiteitä arvioitaessa tulee huomioida henkilötietojen käsittelyn luonne ja laajuus. Mitä arkaluonteisimmista tiedoista ja mitä laajemmasta tietojen käsittelystä on kyse, sitä kattavampia toimenpiteitä edellytetään. Tekniset ja organisatoriset toimenpiteet ovat tietosuojaperiaatteiden mukaisia henkilötietojen suojatoimia.

Organisatorisia toimenpiteitä ovat mm. työntekijöiden tietosuoja- ja tietoturvaosaamisesta huolehtiminen koulutuksin sekä ohjein, työntekijöiden salassapitovelvoitteeseen liittyvät sitoumukset, työtehtävien mukaiset käyttöoikeudet henkilötietoja sisältävissä tietojärjestelmissä sekä fyysisten toimitilojen turvallisuus ja valvonta. Teknisiä toimenpiteitä ovat mm. henkilötietojen käsittelyyn käytettävien tietojärjestelmien tietoturvallisuudesta huolehtiminen (ml. auditoinnit, tietoturvapäivitykset, tietojen varmuuskopiointi), tietojen salaus ja pseudonymisointi sekä tietojärjestelmien ja palvelujen luottamuksellisuutta, eheyttä, käytettävyyttä ja vikasietoisuutta varmistavat toimenpiteet.

Teknisten ja organisatoristen toimenpiteiden tehokkuutta ja riittävyyttä on arvioitava säännöllisesti. Toimenpiteitä on tarvittaessa lisättävä ja vahvistettava. Esimerkiksi pseudonymisoinnin osalta on huomioitava, että pseudonymisoidut tiedot ovat edelleen henkilötietoja, vaikka henkilön suora tunnistetieto on korvattu jollain tunnisteella (mm. koodilla). Tunnisteen avulla tiedot ovat kuitenkin edelleen myöhemmin palautettavissa ja yhdistettävissä taas henkilöön. Pseudonymisointia ei siis voida pitää yksistään riittävänä toimenpiteenä, ellei ole riittävällä tasolla huolehdittu myös esimerkiksi koodiavainten säilytyksestä, käyttöoikeuksista ja hallinnasta.

Teknisten ja organisatoristen toimenpiteiden määrittelyssä tulee lisäksi huomioida teknologinen kehitys mm. markkinoilla saatavilla olevien tietojärjestelmien ja muiden tietoturvaa tukevien teknisten ratkaisujen osalta. Teknisessä toimintaympäristössä on myös arvioitava riskejä, joita valittu tekniikka voi käsittelytoimelle aiheuttaa. Tästä syystä teknisen kehityksen seuraaminen ja ajan tasalla pysyminen on tärkeää, jotta voidaan varmistua siitä, että aikanaan riittävän suojan tason antanut toimenpide antaa henkilötiedoille suojan myös muuttuvassa toimintaympäristössä ja tietojärjestelmien kehityksessä jatkossakin. Lisäksi on huomioitava, että yksikään

tietojärjestelmä ei yksin takaa henkilötietojen suojaa, vaan myös tietojärjestelmän käyttäjien tulee omalla toiminnallaan tukea turvallista tietojen käsittelyä ja toimia annettujen ohjeistusten mukaisesti.

3.4 Tietosuoja ja -turva hankinnoissa ja sopimuksissa

Siun sote voi halutessaan ulkoistaa henkilötietojen käsittelyyn liittyviä tehtäviä palveluntuottajille. Henkilötietojen käsittelyä koskevia tehtäviä annettaessa sopimusperusteisesti palveluntuottajalle, on välttämätöntä huolehtia siitä, että henkilötietojen käsittelyn roolit ja vastuut määritellään rekisterinpitäjän ja henkilötietojen käsittelijän välillä. Siun sote toimii monissa tilanteissa rekisterinpitäjänä hankkiessaan ja ostaessaan palveluja ulkopuolisilta palveluntuottajilta. Mikäli palveluun tai ostoon liittyy henkilötietojen käsittelyä, palveluntuottaja tulee toimimaan oletettavasti henkilötietojen käsittelijän roolissa. Tietosuoja-asetus velvoittaa näissä tilanteissa sopimaan sopimuksella henkilötietojen käsittelystä rekisterinpitäjän ja henkilötietojen käsittelijän välillä.

Siun sotessa käytetään ensisijaisesti aluehallituksen hyväksymiä henkilötietojen käsittelyn ehtoja[5], mikäli palveluntuottaja tulee henkilötietojen käsittelijänä käsittelemään sopimusperusteisesti henkilötietoja Siun soten lukuun, puolesta ja hyväksi. Henkilötietojen käsittelyn ehdot liitetään sopimukseen ja niiden tavoitteena on sitouttaa Siun sote sekä palveluntuottaja käsittelemään henkilötietoja tietosuojalainsäädännön mukaisella tavalla. Olennaisena osana ehtoja on lisäksi henkilötietojen käsittelytoimien kuvaus, joka määrittää mm. tietojen käsittelyn tarkoituksen, luonteen sekä henkilötietojen tyypit sekä tarvittavat tekniset ja organisatoriset toimenpiteet, tietojen käsittelyn sijainnin sekä huomioiden myös palveluntuottajan mahdollisesti käyttämät alihankkijat.

Huomioitavaa on, ettei edellä mainitut henkilötietojen käsittelyn roolit ja vastuut välttämättä päde kaikkiin hankintoihin ja sopimuksiin. Tästä syystä on ensiarvoisen tärkeää pohtia ja määritellä huolellisesti hankinnan suunnitteluvaiheessa, mitä palvelua olemme hankkimassa, millaista henkilötietojen käsittelyä palveluihin liittyy ja onko esimerkiksi ulkoisella palveluntuottajalla itsenäistä päätösvaltaa henkilötietojen käsittelyn, säilytyksen ja käyttämisen suhteen. Palveluntuottajat voivat siis joissakin tilanteissa toimia myös itsenäisinä rekisterinpitäjinä, vaikka tuottavatkin hankintasopimuksen mukaista palvelua Siun sotelle. Tällöin rekisterinpitäjän vastuut koskevat molempia tahoja ja sopimuksissa sekä ehdoissa on määriteltävä tarkoin.

Tietosuojavastaavan vinkit!

- Lue lisää henkilötietojen käsittelystä sopimisesta Siun soten intrasta[6] ja tutustu henkilötietojen käsittelyn ehtojen toimintaohjeeseen[7]!

[5] Siun sote – Henkilötietojen käsittelyn ehdot (Siun sote intra)
[6] Siun sote – Henkilötietojen käsittelystä sopiminen (Siun sote intra)
[7] Siun sote – Toimintaohje: Henkilötietojen käsittelyn ehdot ja henkilötietojen käsittelytoimien kuvaus (Siun sote intra)

- Tutustu henkilötietojen käsittelyn ehtoihin[8] sekä niiden liitteenä olevaan henkilötietojen käsittelytoimien kuvauslomakkeeseen!
- Huomioi, että hankintoihin voi liittyä salassa pidettävää tietoa sekä liikesalaisuuksia, jotka ovat yleensä luonteeltaan teknisiä ja kaupallisia. Hankinta-asiakirjojen julkisuudesta voi saada lisätietoja mm. Julkisten hankintojen neuvontayksikön (JHNY) verkkosivuilta[9]
- **Lukuvinkki:** Julkisten hankintojen käsikirja 2023 (Valtiovarainministeriön julkaisuja)[10]

3.5 Riskienhallinta

Siun sotessa henkilötietojen käsittelyyn liittyviä riskejä tulee arvioida aina, ennen kuin ryhdytään käsittelemään henkilötietoja. Riskienarvion avulla tulee tunnistaa jo suunnitteluvaiheessa ne toimenpiteet, joihin on ryhdyttävä riskien hallitsemiseksi ja henkilötietojen asianmukaisen käsittelyn turvaamiseksi. Riskienarvio tulee aina toteuttaa rekisteröidyn näkökulmasta, jolloin arvioidaan mitä rekisteröidyn vapauksia ja oikeuksia käsittely voi mahdollisesti vaarantaa ja mitä vahinkoja rekisteröidylle voi aiheutua suunnitellusta henkilötietojen käsittelystä. Vahingot voivat olla fyysisiä, aineellisia tai aineettomia. Vahinko voi olla mm. petoksen kohteeksi joutuminen, taloudellinen menetys tai sosiaalinen vahinko kuten maineen menetys.

Riskienarviossa on huomioitava henkilötietojen käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset. Kun henkilötietojen käsittelystä aiheutuvat riskit rekisteröidyn oikeuksille ja vapauksille on tunnistettu, on arvioitava riskien ja niistä aiheutuvan haitan vakavuutta ja toteutumisen todennäköisyyttä. Riskien tunnistamisen merkitys korostuu erityisesti silloin, kun Siun sotessa määritetään teknisiä ja organisatorisia toimenpiteitä (mm. ohjeistus, tietojärjestelmien tietoturva, tietojen salaus), joilla varmistetaan tietosuojan toteutuminen henkilötietojen käsittelyssä.

Riskienarviointi on jatkuvaa toimintaa eli toimenpiteiden riittävyyttä on arvioitava suhteessa käsittelyyn liittyvään riskiin jatkuvasti ja riskienarviointia päivitettävä tarvittaessa. Siun sotella on myös osoitusvelvollisuus riskiperusteisen lähestymistavan noudattamisesta. Riskiperusteinen lähestymistapa ei sulje pois parhaiden käytäntöjen, standardien tai laatutyökalujen käyttöä, vaan ne voivat osaltaan tukea riskienhallintaa ja toimenpiteiden suunnittelua.

Tietosuojaan liittyviä riskejä tulee myös hallita osana Siun soten kokonaisvaltaista riskienhallintaa. Tietosuojariskit eivät siis ole koskaan irrallisia, vaan ne ovat osa toiminnan ja palvelujen muita mahdollisia riskejä. Yksi työkalu riskienarviointiin on tietosuojaa koskeva vaikutustenarviointi (DPIA).

[8] Siun sote – Henkilötietojen käsittelyn ehdot (Siun sote intra)
[9] Julkisten hankintojen neuvontayksikkö
[10] Valtiovarainministeriö – Julkisten hankintojen käsikirja 2023 (julkaisu 2023:60)

3.5.1 Tietosuojaa koskeva vaikutustenarviointi (DPIA)

Vaikutustenarvioinnista yleisesti käytetty lyhenne DPIA tulee sen englanninkielisestä nimestä Data Protection Impact Assessment. EU:n yleisen tietosuoja-asetuksen mukaan rekisterinpitäjän on tehtävä DPIA silloin, kun suunnitellaan henkilötietojen käsittelyä, joka todennäköisesti aiheuttaa korkean riskin rekisteröidyn oikeuksille ja vapauksille.

DPIA tulee tehdä aina, kun suunnitellaan asiakas- ja potilastietojen käsittelyä sekä muiden erityisiin henkilötietoryhmiin kuuluvien (arkaluonteisten) tietojen käsittelyä. DPIA on tehtävä mm. myös silloin, kun henkilötietojen käsittelyssä otetaan käyttöön uutta teknologiaa, käsitellään geneettisiä, biometrisiä tai sijaintitietoja tai henkilötietoja käsitellään laajamittaisesti. DPIAn tarve on arvioitava myös silloin, kun suunnitellaan merkittäviä muutoksia olemassa oleviin palveluihin ja järjestelmiin. Samoin merkittävissä muutostilanteissa tulee päivittää jo aiemmin tehtyä DPIAa, koska käsittelytoimista aiheutuvat riskit voivat tällöin muuttua.

DPIAn tekeminen on aloitettava mahdollisimman aikaisin henkilötietojen käsittelyn valmistelu- ja suunnitteluvaiheessa. Prosessiin on hyvä varata riittävästi aikaa. Vastuu vaikutustenarvioinnin tekemisestä ja etenemisestä on henkilötietojen käsittelytoimen, palvelun tai järjestelmän vastuuhenkilöllä, joka yhdessä rekisterinpitäjän edustajan kanssa hyväksyy valmiin arvioinnin. Arviointiin osallistetaan käsittelytoimen mukaan asiantuntijoita, tietosuojavastaava sekä henkilötietojen käsittelijän roolissa toimiva taho esimerkiksi järjestelmätoimittaja tai Meita.

Tietosuojavastaavan vinkit!

- Lue lisää DPIAsta Siun soten intrasta[11]! Intrasta löydät myös vaikutustenarvioinnin kartoitusohjeen, arvioinnin laadinnan ohjeen sekä Siun soten oman vaikutustenarvioinnin työkalun (Excel).

3.6 Henkilötietojen käsittelyn peruste

Henkilötietojen käsittely edellyttää aina laista löytyvää käsittelyperustetta. Peruste on määritettävä ennen käsittelyn aloittamista. Kun henkilötietojen käsittelyperuste on sidottu johonkin käsittelyperusteeseen, perustetta ei voi enää vaihtaa toiseen. Käsittelyperuste vaikuttaa merkittävästi myös siihen, mitä oikeuksia rekisteröidyllä on eri tilanteissa suhteessa rekisterinpitäjään.

[11] Siun sote – Tietosuojaa koskeva vaikutustenarviointi (DPIA) (Siun soten intra)

Tietosuoja-asetuksessa on kuusi eri perustetta, joilla henkilötietojen käsittely on mahdollista:

- rekisteröidyn antama suostumus
- sopimus
- rekisterinpitäjän lakisääteinen velvoite
- elintärkeiden etujen suojaaminen
- yleistä etua koskeva tehtävä tai julkinen valta
- rekisterinpitäjän tai kolmannen osapuolen oikeutettu etu.

Siun sotessa henkilötietojen käsittelyn yleisimmät käsittelyperusteet ovat Siun sotelle kuuluvat lakisääteiset velvoitteet (mm. sosiaali- ja terveydenhuollon sekä pelastustoimen palvelujen järjestäminen), yleinen etu tai julkisen vallan käyttäminen. Tällöin henkilötietojen käsittelyyn ei tarvita erikseen niiden henkilöiden antamaa suostumusta, joiden tietoja käsitellään. Siun sotessa on kuitenkin myös sellaisia henkilötietojen käsittelytoimia, jotka perustuvat henkilöiden antamaan suostumukseen. Näiden osalta on erittäin tärkeää huomioida, että suostumuksen on aina oltava vapaaehtoinen, yksilöity, tietoinen ja yksiselitteinen tahdonilmaisu, jolla rekisteröity hyväksyy henkilötietojensa käsittelyn. Suostumus on myös voitava peruuttaa yhtä helposti kuin sen on voinut antaa ja Siun soten tulee rekisterinpitäjänä pystyä osoittamaan, että lainmukainen suostumus on henkilötietojen käsittelyyn olemassa.

3.7 Henkilötietojen käsittelystä kertominen rekisteröidylle

Siun soten tulee rekisterinpitäjänä toimittaa rekisteröidylle henkilötietojen käsittelyä koskevat tiedot tiiviisti esitetyssä, läpinäkyvässä ja helposti ymmärrettävässä muodossa selkeällä kielellä ja tietojen tulee olla helposti saatavilla.

Siun soten henkilötietojen käsittelyä on kuvattu Siun soten verkkosivuilla, jossa rekisteröidyille on saatavilla yleinen informaatio henkilötietojen käsittelystä sekä kerrottu heidän oikeuksistaan ja niiden toteuttamisesta. Verkkosivuilta ovat saatavilla myös tietosuojavastaavien yhteystiedot, joihin rekisteröidyt voivat tarvittaessa olla yhteydessä.

Henkilötietojen käsittelystä on laadittu tietosuojaselosteet. Tietosuojaselosteet ovat saatavilla myös Siun soten intran Tiedostopankissa. Tiedostopankista löytyvät myös Siun soten työntekijöiden tietojen käsittelyä koskevat tietosuojaselosteet.

3.8 Henkilötietojen käsittelyn osoitusvelvollisuus

Siun soten tulee rekisterinpitäjänä pystyä osoittamaan noudattavansa henkilötietojen käsittelyssä EU:n tietosuoja-asetusta sekä kansallista tietosuojalainsäädäntöä, huomioiden sosiaali- ja terveydenhuoltoon, pelastustoimeen sekä ympäristöterveydenhuoltoon liittyvät erityislainsäädännöt. Osoitusvelvollisuuden tarkoituksena on myös näyttää, miten rekisterinpitäjä kunnioittaa henkilötietojen käsittelyn kohteena olevien henkilöiden tietosuojaa ja osoitusvelvollisuuden toteuttaminen lisää luottamusta rekisterinpitäjän toimintaan.

Siun soten on toteutettava tarpeelliset tekniset ja organisatoriset toimenpiteet täyttääkseen osoitusvelvollisuuden vaatimukset. Osoitusvelvollisuus tarkoittaa myös dokumentointivelvollisuutta, käytännössä tehtyjen toimenpiteiden tekemistä ja kirjaamista. Siun sote toteuttaa osoitusvelvollisuutta tuottamalla mm. seuraavia dokumentteja tai sisältöjä:

- **Tietosuoja- ja tietoturvapolitiikkaan**[12] on kuvattu periaatteet, tavoitteet, organisointitavat ja vastuut, joita Siun sote noudattaa tietosuojan ja tietoturvallisuuden toteuttamisessa ja kehittämisessä.
- **Tietosuoja- ja tietoturvasuunnitelmaan**[13] on kuvattu menettelyt ja toimintatavat, joilla Siun sotessa toimeenpannaan ja toteutetaan aluehallituksen hyväksymän tietosuoja- ja tietoturvapolitiikan mukaiset tietosuojan ja tietoturvan periaatteet ja tavoitteet. Suunnitelma täyttää sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetun lain (784/2021; 1.1.2024 alkaen laki sosiaali- ja terveydenhuollon asiakastietojen käsittelystä 703/2023, jatkossa asiakastietolaki) sekä sitä täydentävän Terveyden ja hyvinvoinnin laitoksen (THL) määräyksen 3/2021 mukaiset tietoturvasuunnitelman laatimisen velvoitteet ja kokoaa yhteen näiden edellyttämät omavalvonnan kohteen selvitykset ja kuvaukset.
- **Tietosuojan valvontasuunnitelmaan**[14] on kuvattu Siun sotessa tapahtuvan henkilötietojen käsittelyn, terveydenhuollon potilasrekisterin, sosiaalihuollon asiakasrekisterin sekä Kanta-palvelujen tietojen käsittelyn seurannan ja valvonnan periaatteet, valvontakohteet, valvonnan dokumentoinnit sekä väärinkäytösten seuraamukset.
- **Seloste käsittelytoimista**[15] on sisäinen kirjallinen kuvaus Siun soten tekemästä henkilötietojen käsittelystä, joka vastaa tietosuoja-asetuksen (30 artikla) velvoitteeseen. Selostetta ylläpidetään ensisijaisesti valvontaviranomaisia varten. Tarkemmat tiedot eri palveluissa toteutettavasta henkilötietojen käsittelystä ovat ARC-ohjelmiston Henkilötietovarannoissa, johon selosteen liitteellä viitataan. Henkilötietovaranto-taulukkoa ei säilytetä tai ylläpidetä erillisesti ko. selosteen liitteenä.
- **Tietosuoja- ja tietoturvakäsikirjan** tavoitteena on ohjata Siun soten henkilöstöä toimimaan tietosuojalainsäädännön mukaisesti ja täyttämään tietosuojalainsäädännön velvoitteet Siun soten toiminnassa, kunnioittaen rekisteröityjen yksityisyyttä sekä heidän oikeuksiaan henkilötietojen käsittelyssä.
- **Tietotilinpäätöksen** tavoitteena on antaa kokonaiskuva Siun soten tiedonhallinnan, tietosuojan ja tietoturvallisuuden tilasta. Osoitusvelvollisuuden lisäksi tarkoituksena on kuvata viranomaisen

[12] Siun sote - Tietosuoja- ja tietoturvapolitiikka (Siun sote intra)
[13] Siun sote – Tietosuoja- ja tietoturvasuunnitelma (luottamuksellinen)
[14] Siun sote – Tietosuojan valvontasuunnitelma (Siun sote intra)
[15] Siun sote – Seloste käsittelytoimista (Siun sote intra)

toiminnan julkisuudesta annetun lain (621/1999) mukaista hyvän tiedonhallintatavan noudattamista.

- **Tietosuojan tilanneraportti** tuottaa kolmesti vuodessa tilannetietoa tietosuojan tilasta Siun soten johdolle.
- **Tietosuojan omavalvontaraportti** tuottaa kolmesti vuodessa tilannetietoa Siun soten asiakas- ja potilastietojen käsittelyn omavalvonnasta. Asiakas- ja potilastietojärjestelmien tuottamien asiakas- ja käyttäjälokien avulla valvotaan tietojen asianmukaista käsittelyä ja valvonta sisältää myös Kanta-palvelujen käytön valvonnan Mediatri-tietojärjestelmän Medikanta-katselimen osalta.
- **Kyberturvallisuuskatsauksien** tavoitteena on tuottaa viikoittaista tilannekuvaa kyberturvallisuuden tilasta, joka perustuu Kyberturvallisuuskeskuksen viikkokatsauksiin sekä Huoltovarmuuskeskuksen tilannekatsauksiin. Lisäksi tuotetaan tilannekuvaa Siun soten ja Meitan havainnoista sekä poikkeamista.
- **Tietosuojaa koskevien vaikutustenarviointien (DPIA)**[16] tavoitteena on tunnistaa, arvioida ja hallita henkilötietojen käsittelystä aiheutuvia riskejä.
- **Henkilötietojen tietoturvaloukkaukset**[17] ilmoitetaan Siun sotessa Miunpalvelujen kautta sähköisellä lomakkeella[18] ja käsittely dokumentoidaan asianhallintajärjestelmään.
- **Henkilötietojen tietosuojavalvonnat** dokumentoidaan asianhallintajärjestelmässä.
- **Rekisteröityjen oikeuksiin liittyvät pyynnöt** dokumentoidaan asianhallintajärjestelmässä.
- **Tietosuojaselosteiden**[19][20] tavoitteena on kuvata henkilötietojen käsittelyn kohteena olevalle henkilölle, mitä hänen henkilötietojaan tullaan käsittelemään ja miten. Tietosuojaselosteissa kerrotaan myös, mitä rekisteröidyn oikeuksia käsittelyyn liittyy ja kuinka rekisteröity voi käyttää oikeuksiaan.
- **Henkilötietojen käsittelyn ehdot**[21] liitetään osaksi Siun soten ja palveluntuottajan välistä sopimusta silloin, kun palveluntuottaja käsittelee henkilötietoja Siun soten lukuun, puolesta ja eduksi. Ehtoja sovelletaan myös palvelusetelipalvelujen tuottajaksi hakeutuvien palveluntuottajien osalta. Ehtojen käytöstä on laadittu erillinen toimintaohje[22].

[16] Siun sote – Tietosuojaa koskeva vaikutustenarviointi (DPIA) (Siun sote intra)
[17] Siun sote – Tietoturvaloukkauksesta ilmoittaminen (Siun sote intra)
[18] Miunpalvelut – Ilmoitus henkilötietojen tietoturvaloukkauksesta Siun sotelle (Siun sote intra)
[19] Siun sote – Tietosuojaselosteet (Siun sote intra)
[20] Siun sote – Henkilötietojen käsittely
[21] Siun sote – Henkilötietojen käsittelyn ehdot (Siun sote intra)
[22] Siun sote – Toimintaohje: Henkilötietojen käsittelyn ehdot ja henkilötietojen käsittelytoimien kuvaus (Siun sote intra)

- **Tietosuojaan ja tietoturvaan liittyvät koulutukset**[23] on tarkoitettu henkilöstön osaamisen kehittämiseksi. Henkilöstö suorittaa koulutukset Siun soten määrittelemällä tavalla ja suoritetut koulutukset dokumentoidaan henkilöstön osaamisen kehittämiseen ja -hallintaan tarkoitetussa järjestelmässä.

3.9 Tietosuojavastaavat hyvinvointialueen asiantuntijoina

Siun sote on nimittänyt tietosuoja-asetuksen mukaisesti hyvinvointialueelle tietosuojavastaavat. Siun sotessa on kaksi nimettyä tietosuojavastaavaa, jotka toimivat tietosuojan asiantuntijoina.

Tietosuojavastaavan asema ja tehtävät määräytyvät tietosuoja-asetuksen mukaisesti (38–39 artiklat). Tietosuojavastaavan asema on riippumaton ja puolueeton ja heitä sitoo tehtävien suorittamista koskeva salassapitovelvollisuus. Tietosuojavastaava ei ota vastaan ohjeita tietosuoja-asetuksen mukaisten tehtävien hoitamisessa. Tietosuojavastaavan tehtäviin kuuluu mm.:

- seurata tietosuojasäädösten noudattamista koko organisaatiossa ja tuoda esiin havaitsemiaan puutteita
- antaa tietoja ja neuvoja tietosuojasäädösten mukaisista velvollisuuksista johdolle ja henkilötietoja käsitteleville työntekijöille
- antaa pyydettäessä neuvoja tietosuojan vaikutustenarvioinnin tekemisestä ja valvoa vaikutustenarvioinnin toteutusta
- olla rekisteröityjen yhteyshenkilö henkilötietojen käsittelyyn liittyvissä asioissa
- olla tietosuojavaltuutetun toimiston yhteyshenkilö ja tehdä yhteistyötä tietosuojavaltuutetun toimiston kanssa.

Siun sotessa tietosuojavastaavien tehtäviin kuuluvat tietosuoja-asetuksen mukaisten tehtävien lisäksi tietosuojavalvonnan toteuttamisen sekä henkilötietojen tietoturvaloukkausten ilmoitusvelvollisuuden toteutumisen seuranta. Tietosuojavastaavat raportoivat säännöllisesti tietosuojan tilasta ja kehittämistarpeista Siun soten johtoryhmälle.

[23] Siun sote – Tietosuoja- ja tietoturvakoulutus (Siun sote intra)

Tietosuojavastaavat eivät ole sosiaali- ja terveydenhuoltoon, pelastustoimeen tai ympäristöterveydenhuoltoon liittyvien lainsäädännöllisten asioiden asiantuntijoita. Näiden asioiden käsittely tehdään aina yhteistyössä Siun soten eri toimialueiden kanssa, jotta substanssilainsäädännön asiantuntemus varmistetaan ja tietosuojavastaavat tuovat käsiteltävään asiaan näkemyksensä tietosuojalainsäädännön osalta. Tarvittaessa asian käsittelyyn hyödynnetään myös Siun soten lakimiehen asiantuntemusta. Tietosuojaa rakennetaan ja ylläpidetään Siun sotessa siis vahvalla yhteistyöllä, käsitellen asioita monialaisesti ja eri näkökulmista.

Tavoitat Siun soten tietosuojavastaavat osoitteesta tietosuoja@siunsote.fi
Tietosuojavastaaviin voit olla aina yhteydessä matalalla kynnyksellä!

3.10 Henkilöstön osaamisen kehittäminen

Jokaisella työntekijällä on oikeus hyvään perehdytykseen ja työnantajalla on velvollisuus huolehtia perehdyttämisestä. Hyvä perehdytys on suunnitelmallista, tavoitteellista ja sitä arvioidaan perehdytyksen loputtua. Siun sotelle on laadittu strategiaan pohjautuva osaamisen kehittämisen suunnitelma sekä perehdytysohjelma. Siun soten yleisperehdytykseen kuuluvat myös olennaisena osana tietosuoja ja tietoturva. Perehdytyksen päätavoitteita tietosuojan ja tietoturvan näkökulmasta ovat:

- työntekijät sitoutuvat lakien, asetusten ja määräysten lisäksi noudattamaan Siun soten Tietosuoja- ja tietoturvapolitiikan toteuttamiseen liittyviä määräyksiä, ohjeita ja toimintatapoja
- työntekijä perehtyy Siun soten tietoturva- ja tietosuojaohjeisiin
- työntekijä ymmärtää, että hän vastaa omalta osaltaan henkilötietojen käsittelystä sekä tietoturvan ja tietosuojan huomioimisesta työtehtävissään
- työntekijä soveltaa oppimaansa omassa työssään, arvioi työhön liittyviä riskejä sekä nostaa esille havaitsemansa puutteet ja ilmoittaa epäkohdista.

Kaikki Siun soten työntekijät suorittavat tietosuoja- ja tietoturvakoulutukset Duodecim Oppiportin verkkokursseina[24] viiden vuoden välein. Koulutusten suorittaminen on kohdennettu seuraavasti:

- Kaikki hyvinvointialueen työntekijät suorittavat *Tietoturva sosiaali- ja terveydenhuollossa* -verkkokurssin (ml. pelastuslaitos ja ympäristöterveydenhuolto)
- Lisäksi terveydenhuollossa työskentelevät suorittavat *Tietosuoja terveydenhuollossa* -verkkokurssin

[24] Siun sote – Tietosuoja- ja tietoturvakoulutus (Siun sote intra)

- Johtajat ja esihenkilöt suorittavat *Johdon ja esimiesten tietoturvakoulutus* -verkkokurssin.

Esihenkilöt kirjaavat tietosuoja- ja tietoturvakoulutusten suoritukset osaamisen kehittämisen ja henkilöstöhallinnon järjestelmään ja seuraavat koulutusten säännöllistä toteutumista.

Hyvinvointialueen luottamushenkilöille suositellaan suoritettavaksi Digi- ja väestötietoviraston ja eOppivan *Digiturvallisuus hyvinvointialueiden luottamushenkilöille* -verkkokoulutusta[25]. eOppivan koulutustarjonnassa on tarjolla muitakin tietosuojaan ja tietoturvaan liittyviä koulutuksia, jotka ovat kaikkien saatavilla ja joilla henkilöstö voi vahvistaa omaa tietosuojaosaamistaan[26][27][28][29][30].

Siun soten tietosuoja- ja tietoturvaohjeistus on koottu intraan henkilöstön saataville[31]. Siun soten tietosuojavastaavat julkaisevat lisäksi tietosuojan liittyviä tietoiskuja Siun soten intrassa. Tietoiskut ovat tarkoitettu koko Siun soten henkilöstölle ja ne sisältävät ajankohtaisia aiheita tietosuojaan ja henkilötietojen käsittelyyn liittyen. Tietoiskujen tarkoituksena on kehittää ja lisätä tietosuojaosaamista.

Siun soten tietosuojavastaavat voivat osallistua myös toimintayksiköiden esihenkilöiden pyynnöstä yksiköiden järjestämiin koulutus- ja infotilaisuuksiin sekä yhteistyötahojen pyynnöstä myös muihin erilaisiin tilaisuuksiin, joissa toivotaan tietosuojaan liittyvää koulutusta, ohjausta ja neuvontaa.

Tietosuojavastaavan vinkit!

- Tutustu huolellisesti tietosuojaan ja tietoturvaan liittyviin ohjeisiin ja materiaaleihin!
- Huomioi, että ohjeistukset ja tämä käsikirja päivittyvät jatkuvasti, sillä toimintaympäristömme myös muuttuu jatkuvasti!
- Mikäli jokin asia askarruttaa tietosuojan osalta, ota asia esille rohkeasti esihenkilösi kanssa. Tietosuojavastaaviin voi myös olla yhteydessä matalalla kynnyksellä!

[25] eOppiva – Digiturvallisuus hyvinvointialueiden luottamushenkilöille
[26] eOppiva - Tietosuojan ABC julkishallinnon henkilöstölle
[27] eOppiva - Tietosuojan ABC 2 – Syvemmälle tietosuojaan
[28] eOppiva- Digiturvallinen työelämä
[29] eOppiva – Tietosuoja hankinnoissa
[30] eOppiva – Tietosuojan vaikutustenarvioinnin osana hankintaa
[31] Siun sote – Tietosuoja ja tietoturva (Siun sote intra)

Tietosuoja- ja tietoturvaosaaminen on valttikortti sosiaali- ja terveydenhuollon toiminnassa. Henkilöstön tietoturvallisista toimintatavoista rakentuu luotettava ja laadukas hyvinvointialue!

4 Tietosuoja-asetuksen mukaiset rekisteröityjen oikeudet

Siun soten käsitellessä rekisterinpitäjänä henkilötietoja, sen on toteutettava asianmukaiset toimenpiteet rekisteröityjen tietosuojaoikeuksien toteuttamiseksi. Tietosuojaoikeuksilla tarkoitetaan niitä rekisteröityjen oikeuksia, jotka on säädetty EU:n yleisessä tietosuoja-asetuksessa. Rekisterinpitäjän on myös osaltaan helpotettava oikeuksien käyttämistä ja annettava ohjausta rekisteröidyille tarvittaessa. Siun sotessa jokainen työntekijä ja viranhaltija on velvollinen ohjaamaan ja neuvomaan rekisteröityjä. Ohjausta ja neuvontaa rekisteröidyille antavat myös Siun soten tietosuojavastaavat.

Rekisteröity ei voi käyttää kaikkia tietosuojaoikeuksiaan kaikissa tilanteissa. Oikeuksiin vaikuttaa henkilötiedoille määritetty käsittelyperuste. Oikeuksien käyttäminen on rekisteröidylle lähtökohtaisesti maksutonta. Tietyin poikkeuksin maksu voidaan periä esimerkiksi tilanteissa, jos pyydetään tiedoista useampia jäljennöksiä tai jos rekisteröidyn esittämät pyynnöt toistuvat.

Rekisterinpitäjän on pystyttävä vahvistamaan tietosuojaoikeuksiaan käyttävän henkilön henkilöllisyys. Henkilön tunnistamisessa noudatetaan Siun soten ohjeistuksia ja rekisteröityjen pyynnöt pyydetään toimittamaan ensisijaisesti sähköisen asiointipalvelun (Miunpalvelut) kautta, jolloin käytössä on palvelun osalta henkilön vahva tunnistautuminen.

Rekisteröidyn käyttäessä oikeuksiaan, hänelle on vastattava ilman aiheetonta viivytystä, mutta viimeistään kuukauden kuluessa pyynnön vastaanottamisesta. Vastauksessa on kerrottava toimenpiteistä, joihin pyynnön vuoksi on ryhdytty. Jos pyyntöjä on useita tai ne ovat monimutkaisia, voi käsittely vaatia normaalia pidemmän vastausajan. Tällöin määräaikaa voidaan jatkaa enintään kahdella kuukaudella ja määräajan jatkaminen on perusteltava sekä ilmoitettava rekisteröidylle.

Joistakin rekisteröidyn esittämistä pyynnöstä voi kieltäytyä. Kieltäytymisestä on ilmoitettava rekisteröidylle viimeistään kuukauden kuluessa pyynnön vastaanottamisesta ja kieltäytyminen on perusteltava.

4.1 Oikeus saada tietoa henkilötietojen käsittelystä

Rekisteröidyllä on oikeus saada tietoa hänen henkilötietojensa keräämisestä sekä käsittelystä. Rekisterinpitäjän on annettava rekisteröidylle kaikki henkilötietojen käsittelyä koskevat tiedot tiiviissä, läpinäkyvässä, helposti ymmärrettävässä ja selkeässä muodossa. Tavoitteena on, että rekisteröity saa kattavan ja selkeän kuvan henkilötietojen käsittelyn kokonaisuudesta.

Rekisteröidylle on kerrottava mm.

- mikä taho toimii rekisterinpitäjänä ja tarjottava rekisterinpitäjän yhteystiedot
- mihin tarkoitukseen henkilötietoja käsitellään
- mikä on henkilötietojen käsittelyperuste
- mitkä ovat henkilötietojen käsittelyajat
- mihin henkilötietoja mahdollisesti luovutetaan
- siirretäänkö henkilötietoja EU:n tai ETA-alueen ulkopuolelle
- mistä käsiteltävät henkilötiedot on saatu, kun ne on saatu muualta kuin rekisteröidyltä itseltään.

Rekisteröidyille annetaan tieto henkilötietojen käsittelystä yleensä kirjallisesti, esimerkiksi tietosuojaselosteen muodossa.

Tietosuojavastaavan vinkit!

- Kun suunnittelet henkilötietojen käsittelyä kuvaavaa tiedotetta tai tietosuojaselostetta, tunnista kohderyhmä, jolle henkilötietojen käsittelystä kerrotaan. Huomioi erityisesti mm. lapset ja iäkkäät henkilöt ja arvioi, onko annettu tieto kohderyhmän keskivertoedustajan ymmärrettävissä.
- Lisätietoa tietosuojaselosteiden laadinnasta Siun soten intrasta[32], josta löydät myös valmiin mallipohjan tietosuojaselosteesta[33].
- Huomioithan lisäksi, että tietosuojavastaavat eivät ylläpidä tietosuojaselosteita tai laadi niitä valmiiksi pyynnöstä. Tarvittavien tietosuojaselosteiden laatiminen ja niiden ylläpito on käsittelytoimen vastuuhenkilöllä ja viimekädessä rekisterinpitäjän edustajalla!

4.2 Oikeus saada tutustua tietoihin

Rekisteröidyllä on oikeus saada rekisterinpitäjältä vahvistus siitä, käsitteleekö tämä häntä koskevia henkilötietoja. Näin rekisteröidyllä on mahdollisuus arvioida ja varmistaa käsittelyn lainmukaisuus. Jos rekisteröidyn tietoja käsitellään, rekisterinpitäjän on toimitettava hänelle jäljennös käsiteltävistä henkilötiedoista. Pyyntö tulee käsitellä kuukauden kuluessa.

Oikeus voidaan evätä laissa säädetyin perustein, jolloin rekisteröity saa kieltäytymistodistuksen. Mikäli rekisteröity on tähän tyytymätön, on hänellä oikeus saattaa asia tietosuojavaltuutetun käsiteltäväksi tai hakea päätökseen muutosta hallinto-oikeudelta.

[32] Siun sote – Tietosuojaselosteet (Siun sote intra)
[33] Siun sote – Tietosuojaselosteen mallipohja (Siun sote intra)

Tietosuojavastaavan vinkit!

- Ohjaa asiakkaita katsomaan hoitoon ja palveluun liittyviä tietoja OmaKanta-palvelusta mahdollisuuksien mukaan.
- Asiakkaita voi ohjeistaa tekemään tarvittaessa asiakas- ja/tai potilasrekisteritietojen tarkastuspyynnön sähköisesti Miunpalveluissa[34] tai Siun soten verkkosivuilta löytyvällä tulostettavalla lomakkeella[35].
- Tutustu asiakas- ja potilasrekisteriin tallennetun tiedon luovuttaminen ja tarkastaminen toimintaohjeeseen[36]!

4.3 Oikeus oikaista tietoja

Rekisteröidyllä on oikeus vaatia, että rekisterinpitäjä oikaisee häntä koskevat epätarkat ja virheelliset henkilötiedot. Rekisteröidyllä on myös oikeus saada puutteelliset henkilötiedot täydennettyä. Pyyntö tehdään kirjallisesti ja se käsitellään kuukauden kuluessa.

Oikeus voidaan evätä rekisterinpitäjän arvioinnin perusteella, jolloin rekisteröity saa kieltäytymistodistuksen. Mikäli rekisteröity on tähän tyytymätön, on hänellä oikeus saattaa asia tietosuojavaltuutetun käsiteltäväksi tai hakea päätökseen muutosta hallinto-oikeudelta.

Tietosuojavastaavan vinkit!

- Muista tarkastaa asiakkaasi yhteystiedot aina asiakkaan asioidessa Siun soten palveluissa!
- Asiakkaita voi ohjeistaa tekemään tarvittaessa asiakas- ja/tai potilasrekisteritietojen korjauspyynnön sähköisesti Miunpalveluissa[37] tai Siun soten verkkosivuilta löytyvällä tulostettavalla lomakkeella[38].

4.4 Oikeus poistaa tiedot

Rekisteröidyllä on oikeus saada rekisterinpitäjä poistamaan itseään koskevat tiedot. Oikeus tunnetaan myös nimellä oikeus tulla unohdetuksi. Pyyntö tehdään kirjallisesti ja se tulee käsitellä kuukauden kuluessa.

[34] Miunpalvelut – Asiakas- ja/tai potilasrekisteritietojen tarkastuspyyntö
[35] Siun sote – Henkilötietojen tarkastuspyyntö (asiakas- ja potilastiedot)
[36] Siun sote – Toimintaohje: Asiakas- ja potilasrekisteriin tallennetun tiedon luovuttaminen ja tarkastaminen (Siun sote intra)
[37] Miunpalvelut – Asiakas- tai potilasrekisteriin tallennetun henkilötiedon korjaamisvaatimus
[38] Siun sote – Asiakas- tai potilasrekisteriin tallennetun henkilötiedon korjaamisvaatimus

Oikeus voidaan evätä rekisterinpitäjän arvioinnin perusteella, jolloin rekisteröity saa kieltäytymistodistuksen. Mikäli rekisteröity on tähän tyytymätön, on hänellä oikeus saattaa asia tietosuojavaltuutetun käsiteltäväksi tai hakea päätökseen muutosta hallinto-oikeudelta. Oikeutta tietojen poistamiseen ei ole mm. silloin, kun tietoja käsitellään rekisterinpitäjän lakisääteisen tehtävän suorittamiseksi (mm. asiakas- ja potilastietojen lakisääteinen käsittely asiakas- ja potilastietojärjestelmissä).

Mikäli henkilötietojen käsittely on perustunut rekisteröidyn antamaan suostumukseen, hänellä on oikeus perua antamansa suostumus ja tähän perustuen pyytää rekisterinpitäjää poistamaan itseään koskevat tiedot. Mikäli henkilö peruuttaa antamansa suostumuksen, tulee henkilötietojen käsittely päättää siltä osin, kuin käsittely on perustunut suostumukseen.

Tietosuojavastaavan vinkit!

- Asiakkaita voi ohjeistaa tekemään tarvittaessa asiakas- ja/tai potilasrekisteritietojen poistopyynnön sähköisesti Miunpalveluissa[39] tai Siun soten verkkosivuilta löytyvällä tulostettavalla lomakkeella[40].

4.5 Oikeus rajoittaa tietojen käsittelyä

Rekisteröidyllä on tietyissä tilanteissa oikeus pyytää rekisterinpitäjää rajoittamaan häntä koskevien henkilötietojen käsittelyä. Rekisteröity voi käyttää kyseistä oikeutta esimerkiksi tilanteissa, jos rekisteröity kiistää henkilötietojen paikkansapitävyyden. Tällöin käsittelyä on rajoitettava ja varmistuttava tietojen paikkansapitävyydestä. Pyynnöt käsitellään tapauskohtaisesti.

4.6 Oikeus siirtää tiedot järjestelmästä toiseen

Rekisteröidyllä on tietyissä tilanteissa oikeus saada rekisterinpitäjälle toimittamansa henkilötiedot jäsennellyssä, yleisesti käytetyssä ja koneellisesti luettavassa muodossa sekä halutessaan siirtää kyseiset tiedot toiselle rekisterinpitäjälle. Oikeutta sovelletaan vain henkilötietojen automaattiseen käsittelyyn tilanteissa, joissa tiedot koskevat rekisteröityjä, tiedot ovat hänen itsensä toimittamia ja tietojen käsittely on perustunut suostumukseen tai sopimukseen. Oikeutta ei voi soveltaa esimerkiksi Siun soten sosiaalihuollon asiakasrekisterin tai terveydenhuollon potilasrekisterin tietoihin. Pyynnöt käsitellään tapauskohtaisesti.

[39] Miunpalvelut – Asiakas- tai potilasrekisteriin tallennetun henkilötiedon korjaamisvaatimus (myös poisto)
[40] Siun sote – Asiakas- tai potilasrekisteriin tallennetun henkilötiedon korjaamisvaatimus (myös poisto)

4.7 Oikeus vastustaa tietojen käsittelyä

Rekisteröidyllä on tietyissä tilanteissa oikeus vastustaa henkilötietojensa käsittelyä eli pyytää, ettei tietoja käsiteltäisi ollenkaan. Oikeus vastustaa tietojen käsittelyä on mm. suoramarkkinointitarkoituksiin liittyvissä käsittelytoimissa. Oikeutta tietojen käsittelyn vastustamiseen ei ole mm. silloin, kun tietoja käsitellään rekisterinpitäjän lakisääteisen tehtävän suorittamiseksi. Pyynnöt käsitellään tapauskohtaisesti.

4.8 Oikeus olla joutumatta automaattisen päätöksenteon kohteeksi

Rekisteröidyllä on oikeus vaatia, että häntä koskevat päätökset tekee ihminen. Tällöin päätös ei perustu pelkästään automaattiseen henkilötietojen käsittelyyn tai rekisteröidyn henkilökohtaisia ominaisuuksia arvioivaan käsittelyyn (profilointiin).

Mikäli automaattista päätöksentekoa tai profilointia suoritetaan, tulee rekisteröidyille kertoa siitä tietosuojaselosteessa, kuvaten päätöksenteon toimintaperiaatteet, päätöksenteossa painotettavat tekijät sekä se, kuinka toiminta vaikuttaa rekisteröityyn. Mikäli rekisteröity vastustaa automaattisen päätöksenteon käyttöä henkilötietojen käsittelyssä, rekisteröity voi ottaa yhteyttä tietosuojaselosteeseen merkittyyn rekisterinpitäjän edustajaan tai Siun soten tietosuojavastaaviin. Pyynnöt käsitellään tapauskohtaisesti.

4.9 Oikeus tehdä ilmoitus valvontaviranomaiselle

Rekisteröidyllä on oikeus tehdä ilmoitus tietosuojavaltuutetun toimistoon, mikäli hän katsoo, että hänen tietosuojaoikeuksiaan on loukattu, henkilötietojen käsittelyssä on toimittu tietosuojalainsäädännön vastaisesti tai hän on havainnut epäkohdan henkilötietojen käsittelyssä. Tietosuojavaltuutettu ei lähtökohtaisesti ota kantaa sellaisiin tapauksiin, joissa rekisterinpitäjään ei ole oltu itse yhteydessä. Rekisteröityjä tulee siis ohjata ensisijaisesti olemaan yhteydessä Siun soteen tai tietosuojavastaaviin.

Tietosuojavastaavan vinkit!

- Asiakkaita voi ohjeistaa olemaan yhteydessä Siun sotentietosuojavastaaviin, mikäli he tarvitsevat lisätietoja tietosuojaoikeuksistaan tai haluavat keskustella henkilötietojensa käsittelyyn liittyvistä asioista tai niissä tapahtuneista poikkeamista!

5 Julkisuuslain mukaiset oikeudet

Viranomaisille kohdennettujen tietopyyntöjen osalta noudatetaan julkisuuslakia (laki viranomaisen toiminnan julkisuudesta 621/1999). Julkisuuslain tarkoituksena on korostaa ja toteuttaa julkisuusperiaatteita kaikkien viranomaisten toiminnassa. Julkisuusperiaatteiden tarkoituksena on parantaa kansalaisten mahdollisuuksia osallistua yhteiskunnalliseen toimintaan sekä valvoa julkisen vallan käyttöä ja viranomaisten toimintaa. Julkisuuslaki sääntelee lisäksi viranomaisten asiakirjojen ja muiden tietoaineistojen julkisuutta ja salassapitoa sekä tiedon antamista asiakirjasta ja siihen liittyvää menettelyä. Suomessa julkisuusperiaatteella on vahva asema ja sen mukaan viranomaisten asiakirjat ovat julkisia, ellei niiden salassapidosta ole nimenomaisesti säädetty.

Henkilön käyttäessä oikeuksiaan, hänelle on vastattava ilman aiheetonta viivytystä, mutta viimeistään kahden viikon kuluessa pyynnön vastaanottamisesta. Jos tiedon antaminen vaatii tavanomaista suuremman työmäärän, tieto annetaan viimeistään kuukauden kuluessa tietopyynnön tekemisestä. Jos tiedon antaminen edellyttää erityistoimenpiteitä, siitä voidaan julkisuuslain nojalla periä korvaus.

Jos tietopyynnön mukaisia tietoja ei voida luovuttaa, viranomaisen on aina perusteltava kieltäytyminen tiedon antamisesta ja kerrottava lakiperuste, jonka mukaisesti tieto on salassa pidettävä tai ei-julkinen. Pyynnön esittäjälle on tarvittaessa annettava kieltäytymisestä valituskelpoinen päätös.

Tietosuojavastaavan vinkit!

- Tutustu Siun soten asiakirjajulkisuuskuvaukseen[41] sekä sen ohessa oleviin lisätietoihin tietopyyntöjen tekemisestä, toimittamisesta ja niiden käsittelystä!
- Tutustu Siun soten tiedonohjaussuunnitelmaan[42], jossa on kuvattu mm. tietojärjestelmissä käsiteltävien tietojen säilytysajat (pois luettuna asiakas- ja potilastiedot, joiden pysyvästä sähköisestä säilyttämisestä vastaa valtakunnallinen Kanta-arkisto).
- Tunnista julkisuuslakiin perustuvan tietopyynnön ja tietosuoja-asetuksen mukaisen tarkastuspyynnön erot!
- Muista, että julkisuuslaissa käytetty salassapidon käsite sisältää asiakirjasalaisuuden, vaitiolovelvollisuuden ja salassa pidettävien tietojen hyväksikäyttökiellon. Julkisuuslaissa määritellyt viranomaiset tai niiden henkilöstö ei saa paljastaa salassa pidettäviä tietoja sivullisille ja viranomaistoiminnan yhteydessä saatuja salassa pidettäviä tietoja ei saa käyttää omaksi tai toisen hyödyksi tai toisen vahingoksi!

5.1 Viranomaisen asiakirja

Viranomaisen asiakirja tarkoittaa asiakirjaa, joka on viranomaisen hallussa, jonka viranomainen on laatinut tai joka on toimitettu viranomaiselle jonkin asian käsittelyä varten. Jos asiakirja on laadittu viranomaisen antaman toimeksiannon takia, se kuuluu viranomaisen asiakirjoihin. Viranomaiselle toimitettuja asiakirjoja ovat sellaiset asiakirjat, jotka on annettu viranomaiselle jonkin tehtävän suorittamista varten. Viranomaisten asiakirjoista voi ilmetä myös henkilötietoja, joka ei automaattisesti tarkoita sitä, etteikö asiakirjaa voisi luovuttaa. Tällöin kuitenkin tulee arvioida, onko tietoja pyytävällä taholla tietosuojalainsäädännön mukainen oikeus käsitellä henkilötietoja. Pääsääntöisesti viranomaisen asiakirjoja eivät ole mm.:

[41] Siun sote - Asiakirjajulkisuuskuvaus
[42] Siun sote – Tiedonohjaussuunnitelma (Siun sote intra)

- viranomaiselle tai luottamushenkilölle toimitetut asiakirjat, jotka on lähetetty hänelle muun tehtävänsä tai asemansa vuoksi
- muistiinpanot, jotka viranomaisen palveluksessa oleva tai viranomaisen toimeksiannosta toimiva henkilö on laatinut
- asiakirjat, jotka on hankittu viranomaisen sisäistä koulutusta, tiedonhakua tai muuta vastaavaa syytä varten
- asiakirjat, jotka ovat päätyneet viranomaisen haltuun löytötavaroina tai -asiakirjoina.

Tietosuojavastaavan vinkit!

- Muista, että kansalaisilla on viranomaistoiminnan asianosaisina mahdollisuus saada oman oikeusturvansa kannalta itseä koskevaa tietoa viranomaisten ratkaisuista sekä saada tieto itseään koskevasta asiakirjasta!

5.2 Oikeus saada tieto julkiseksi määritellystä viranomaisen asiakirjasta

Jokaisella on oikeus saada tieto julkiseksi määritellystä julkisesta asiakirjasta sekä oikeus saada tieto henkilöä itseään koskevasta asiakirjasta. Tällöin on huomioitava, että jos asia on keskeneräinen, on tiedon antaminen viranomaisen harkinnassa. Viimeistään asian valmistuttua, tiedonsaantioikeutta ei voi rajoittaa. Kun tietopyyntö koskee julkista asiakirjaa, tietopyyntöä ei tarvitse perustella eikä tiedon pyytäjällä ole velvoitetta kertoa, mihin hän tulee pyydettävää tietoa käyttämään.

Tietosuojavastaavan vinkit!

- Huomioi, että journalismi on osin tietosuojalainsäädännön vaatimusten soveltamisen ulkopuolella. Toimittajilla on yleisen tiedonsaannin pohjalta mahdollisuus valvoa ja arvioida omassa työssään julkisuuden kautta virnaomaisten toimintoja. Journalismissa on kyse enemmän yksityisyydensuojasta kuin tietosuojasta, mikäli pohditaan, mitä kaikkea yksityishenkilöä koskevaa tietoa voidaan julkaista esimerkiksi sanomalehdessä.

5.3 Oikeus saada tieto salassa pidettävästä tai osin salassa pidettävästä asiakirjasta

Salassa pidettävästä viranomaisen asiakirjasta tai sen sisällöstä saa antaa tiedon vain, jos niin julkisuuslaissa säädetään. Jos vain osa asiakirjasta on salassa pidettävä, asiakirjan julkisesta osasta voidaan antaa tietoa. Julkisesta osasta annetaan tietoa kuitenkin vain silloin, jos tiedon antaminen on mahdollista siten, ettei salassa pidettävä osa tule tietoon sivullisille.

Tietosuojavastaavan vinkit!

- Jos jokin asiakirja on säädetty salassa pidettäväksi, se on salainen jokaisen viranomaisen hallussa! Ehdottoman salassapidon piiriin kuuluvat mm. sosiaali- ja terveydenhuollon asiakkaaseen ja hänen saamansa etuuteen, palveluun tai hänen terveydentilaansa liittyvät tiedot!

5.4 Oikeus saada tieto asiasta, joka koskee henkilöä itseään tai jossa henkilö on asianosaisena

Jokaisella on oikeus saada tieto viranomaisen asiakirjaan sisältyvistä tiedoista, jotka koskevat häntä itseään. Oikeutta saada tietoa itseään koskevasta asiakirjasta rajoittaa vain esimerkiksi se, että tiedon antaminen olisi vastoin erittäin tärkeää yksityistä tai yleistä etua:

- Erittäin tärkeä yksityinen etu voi tarkoittaa yksityiselämän suojaamista, kuten tietoa asianosaisen sairaudesta, tai yksilön turvallisuuden varmistamista. Yksityisen edun suojaaminen voi tarkoittaa myös liikesalaisuuden suojaamista.
- Erittäin tärkeä yleinen etu puolestaan voi liittyä esimerkiksi valtion ulkoiseen turvallisuuteen.
- Lisäksi asiakirjasta ei välttämättä voida antaa tietoa siinä vaiheessa, kun asian käsittely ei ole vielä päättynyt viranomaisen taholta. Tällöin viranomainen voi antaa asiasta tiedon harkintansa mukaan.

Jos tietoja pyytävä henkilö on asiassa asianosaisen asemassa, hänellä on oikeus saada asiaa käsittelevältä tai käsitelleeltä viranomaiselta tieto muunkin kuin julkisen asiakirjan sisällöstä, joka voi tai on voinut vaikuttaa hänen asiansa käsittelyyn. Asianosaisella tarkoitetaan hakijaa, valittajaa tai muuta henkilöä, jonka oikeutta, etua tai velvollisuutta asia koskee. Asianosainen voi olla luonnollisen henkilön lisäksi oikeushenkilö, kuten yhdistys, yhtiö tai muu yhteisö. Myös julkisyhteisö tai sen toimielin voi olla asianosainen, jos asia koskee julkisyhteisön tai sen toimielimen etua, oikeutta tai velvollisuutta.

Asianosaisen henkilön tiedonsaantioikeutta ei kuitenkaan ole esimerkiksi asiakirjaan, josta tiedon antaminen olisi vastoin erittäin tärkeää yleistä etua taikka lapsen etua tai muuta erittäin tärkeätä yksityistä etua. Lisäksi asianosaisella henkilöllä ei ole tiedonsaantioikeutta esittelymuistioon, ratkaisuehdotukseen tai vastaavaan asian valmistelua varten tehtyyn asiakirjaan, ennen kuin asian käsittely viranomaisen taholta on päättynyt.

6 Henkilötietojen käsittelyssä huomioitavia asioita

Henkilötietojen käsittely tarkoittaa henkilötietoihin kohdistettua toimintaa. Käsittely voi olla joko automaattista tietojärjestelmällä tapahtuvaa tai paperisten asiakirjojen manuaalista käsittelyä. Tiedon käsittelyä on tietojen kerääminen, tallentaminen, järjestäminen, jäsentäminen, säilyttäminen, muokkaaminen tai muuttaminen, kysely, käyttö, tietojen luovuttaminen tai asettaminen saataville, tietojen yhteensovittaminen tai yhdistäminen, käytön rajoittaminen, tulostaminen, poisto tai tuhoaminen. Myös tiedon haku ja lataaminen sähköisestä järjestelmästä tai tietokannasta on henkilötietojen käsittelyä. Henkilötiedon käsittelyksi on myös hyvä tunnistaa pelkkä tietojen katselu eli lukeminen tai tietojen selaaminen.

Henkilötietojen käsittely edellyttää aina laista löytyvää käsittelyperustetta. Peruste on määritettävä ennen käsittelyn aloittamista. Henkilötietojen käsittely perustuu ennalta määriteltyyn käyttötarkoitukseen, jolloin tätä kyseistä käyttötarkoitusta varten kerättyjä tietoja ei saa käyttää muihin käyttötarkoituksiin. Henkilötietojen käsittelyä ohjaavat tietosuojaperiaatteet.

Siun soten asiakas- ja potilasrekistereihin merkityt tiedot ovat myös henkilötietoja. Lisäksi sosiaali- ja terveydenhuollon asiakas- ja potilastiedot ovat salassa pidettäviä ja niiden käsittelyä ohjaa tietosuojalainsäädännön lisäksi vahva kansallinen sosiaali- ja terveydenhuoltoa koskeva erityislainsäädäntö.

Tietosuojavastaavan vinkit!

- Tunnista millaista henkilötietojen käsittelyä työtehtäviisi kuuluu ja pohdi millaisia riskejä käsittelytoimeen mahdollisesti kohdistuu. Toimintayksiköissä tulee arvioida säännöllisesti, onko käsittelytoimiin tai vaikkapa tietojärjestelmien käyttöön liittyvät ohjeistukset ajan tasalla ja että henkilökunta saa perehdytyksen työtehtäviinsä.

6.1 Tietoaineistoturvallisuus

Tietoaineistoturvallisuuden keinoin pyritään turvaamaan asiakirjojen, tiedostojen ja muiden tietoaineistojen luottamuksellisuuden, eheyden, saatavuuden ja käytettävyyden toteutuminen. Tietoaineistoturvallisuuden toteutumisen edellytyksenä on, että

- tunnistetaan, mitä tietoja organisaatiossa käsitellään, missä tietoja säilytetään ja miten niitä käsitellään
- tunnistetut tiedot luokitellaan (julkinen, sisäinen ja salassa pidettävä tieto)
- tietoihin kohdistuvat käsittelytoimet määräytyvät luokituksen mukaisesti
- tietojen suojaamisesta huolehditaan kaikissa tiedon elinkaaren vaiheissa tietojen keräämisestä tietojen tuhoamiseen.

Tietoaineistoturvallisuuden toteutuminen edellyttää myös, että muista tietoturvallisuuden osa-alueista on huolehdittu asianmukaisesti, esimerkiksi tietojärjestelmien ja laitteiden tietoturvaominaisuudet on mitoitettu niissä käsiteltävien tietojen luokittelun mukaisesti ja henkilöstöä on ohjeistettu luokittelun mukaisesta tietojen käsittelystä. Pääsääntöisesti tietoaineistoja Siun sotessa käsitellään niissä tietojärjestelmissä, jotka on tarkoitettu kyseisten tietojen käsittelyyn. On kuitenkin tilanteita, joissa tietoa joudutaan käsittelemään tietojärjestelmien ulkopuolella ja useassa eri sijainnissa, esimerkiksi verkkolevyillä, ulkoisilla tallennusvälineillä, eri viestintävälineissä ja paperilla.

Siun soten toiminnasta kertyvien asiakirjojen ja tietoaineistojen säilyttämisestä ohjeistetaan tiedonohjaussuunnitelmassa[43], joka sisältää sähköisissä tietojärjestelmissä olevat käsittely- ja säilytysaikatiedot.

[43] Siun sote – Tiedonohjaussuunnitelma (Siun sote intra)

Siun sotessa tietojärjestelmien ulkopuolella käsiteltävät tietoaineistot luokitellaan tietoaineiston luokittelu- ja käsittelyohjeen[44] mukaisesti.

Tietosuojavastaavan vinkit!

- Tunnista, mihin luokkaan käsittelemäsi tietoaineisto kuuluu. Jos olet epävarma, selvitä!

6.2 Salassapito, vaitiolovelvollisuus ja hyväksikäyttökielto

Jokainen Siun soten työntekijä ja viranhaltija on salassapito- ja vaitiolovelvollinen. Velvollisuus koskee myös alan opiskelijoita sekä harjoittelijoita sekä muita Siun sotessa työskenteleviä ammattilaisia ja luottamushenkilöitä. Siun sotessa on käytössä salassapito- ja käyttäjäsitoumus[45], jonka mm. uudet työntekijät ja viranhaltijat allekirjoittavat palvelussuhteen alussa. Salassapito- ja käyttäjäsitoumuksesta ja sen käytöstä on annettu erillinen toimintaohje[46].

Palvelus- tai virkasuhteen aikana tai muun työtehtävän aikana tai sen päätyttyä, sivulliselle ei saa ilmaista työn vuoksi tietoon saatuja Siun soten asiakkaita ja potilaita, henkilöstöä, sopimuskumppaneita tai muita yhteistyötahoja koskevia salassa pidettäviä tietoja.

Salassapitovelvoite koostuu kolmesta toisiaan täydentävästä osa-alueesta –asiakirjasalaisuudesta, vaitiolovelvollisuudesta ja hyväksikäyttökiellosta:

- Asiakirjasalaisuudella tarkoitetaan sitä, että asiakirjaa tai sen kopiota tai tulostetta ei saa näyttää, luovuttaa tai antaa muulla tavoin sivullisen nähtäväksi tai käytettäväksi.
- Vaitiolovelvollisuus jatkuu vielä senkin jälkeen, kun virka- tai palvelussuhde taikka toimeksianto on päättynyt ja pitää sisällään kaikki muut tiedon luovuttamistavat kuin edellä mainitut ja koskee myös tallentamattomia tietoja.
- Hyväksikäyttökielto tarkoittaa sitä, ettei tietoa saa käyttää omaksi tai toisen hyödyksi tai toisen vahingoksi.

Tietosuojavastaavan vinkit!

- Muista, että henkilön sosiaali- tai terveydenhuollon asiakkuus on myös salassa pidettävä tieto!

[44] Siun sote – Tietoaineiston luokittelu- ja käsittelyohje (Siun sote intra)
[45] Siun sote – Salassapito- ja käyttäjäsitoumus (Siun sote intra)
[46] Siun sote – Salassapito- ja käyttäjäsitoumus ja siihen liittyvät hyvinvointialueen tietosuoja- ja tietoturvakoulutukset ja ohjeistukset (Siun sote intra)

- Huolehdi, että salassapito- ja käyttäjäsitoumus[47] on laadittu aina palvelussuhteen alussa uusilta työntekijöiltä. Sitoumus laaditaan kahtena kappaleena, joista toinen jää sitoumuksen tekijälle ja toinen arkistoitavaksi Siun sotelle!
- Työntekijän vastuulla on perehtyä salassapito- ja käyttäjäsitoumuksen velvoittavuuteen ja sisältöön. Työnantajan on annettava työntekijälle kaikki tarpeellinen informaatio sitoumuksesta, sen käyttötarkoituksesta ja merkittävyydestä. Työntekijälle kerrotaan lisäksi työnantajan toimesta, että mahdollisiin työntekijän rikkomuksiin puututaan ja rikkomuksista voi aiheutua työ-, vahingonkorvaus- ja rikoslainsäädännön mukaisia seuraamuksia työntekijälle!
- Muista, että salassapito- ja vaitiolovelvollisuus on voimassa pysyvästi, eikä se pääty mm. palvelussuhteen päätyttyä!

6.3 Käyttöoikeudet henkilötietoihin

Käyttöoikeuksien määrittely, hallinta ja säännöllinen katselmointi ovat henkilötietojen suojauksen oleellinen osa. Siun sotessa käyttövaltuuksien hallinnan ja tunnistamisen käytäntöjen periaatteet ja toimintatavat on kuvattu tarkemmin Tietosuoja- ja tietoturvasuunnitelmassa[48]. Suunnitelmassa kuvatut periaatteet ja toimintatavat ovat yhteisesti määriteltyjä, jotka ohjaavat käyttöoikeuksien käytänteitä koko Siun soten alueella.

Esihenkilöiden vastuulla on määritellä työntekijöiden käyttöoikeudet vastaamaan työtehtävän mukaista tietojen käyttötarkoitusta ja laajuutta. Tarvittaessa käyttöoikeuksien määrittely ja pohdinta tulee tehdä palvelu- ja toimialueella. Suunniteltaessa uusia toimintoja, käytänteitä tai otettaessa käyttöön uusia tietojärjestelmiä tai ohjelmistoja, käyttöoikeuksien määrittely tulee tehdä osana muuta suunnittelutyötä ja niiden määrittelylle kannattaa varata riittävästi aikaa.

Sosiaali- ja terveydenhuollon asiakastietojen käyttöoikeudesta säädetään Sosiaali- ja terveysministeriön asetuksella (825/2022, nk. käyttöoikeusasetus). Asetus säätelee, mitä tietoja sosiaali- ja terveydenhuollon ammattihenkilöt ja muut asiakas- ja potilastietoja käsittelevät henkilöt saavat enintään käsitellä, perustuen työtehtävään ja annettavaan palveluun.

Tietosuojavastaavan vinkit!

- Muista, että jokainen työntekijä vastaa omalla käyttäjätunnuksellaan järjestelmien, ohjelmistojen ja sovellusten sekä laitteiden käytöstä sekä asiakirjoihin tehdyistä merkinnöistä ja tietojen

[47] Siun sote – Salassapito- ja käyttäjäsitoumus
[48] Siun sote – Tietosuoja- ja tietoturvasuunnitelma (luottamuksellinen)

katselusta! Älä luovuta käyttäjätunnusta, salasanaa tai toimikorttiasi kenellekään! Ne ovat henkilökohtaisia ja jokainen vastaa itse niiden huolellisesta säilytyksestä sekä käytöstä!
- Tutustu Siun soten käyttövaltuuksien hallinnan ja tunnistautumisen käytäntöihin[49]!

6.4 Henkilötietojen sekä luottamuksellisten ja salassa pidettävien tietoaineistojen suojaaminen sivullisilta

Henkilötiedot sekä luottamukselliseksi tai salassa pidettäväksi luokitellut tiedot ja tietoaineistot on suojattava niin, ettei niihin pääse käsiksi henkilöt, joilla ei ole tietoihin käyttöoikeutta.

Henkilötietojen osalta on varmistuttava siitä, ettei niitä voida vahingossa tai laittomasti hävittää, muuttaa, luovuttaa, siirtää tai muutoin laittomasti käsitellä. Tietojen suojausvelvollisuus koskee sekä paperimuodossa että sähköisessä muodossa olevia tietoja. Paperimuotoisia henkilötietoja sisältäviä tietoja on säilytettävä esimerkiksi lukitussa kaapissa tai lukitussa huoneessa siten, etteivät niitä näe ulkopuoliset. Asiakkaan tai potilaan asioista ei pidä myöskään puhua tai keskustella niin, että sen kuulisivat muut asiakkaat tai sellaiset työntekijät, jotka eivät asiakkaan tai potilaan asioita hoida tai osallistu heidän palveluunsa. Myös toimitilat ja asiakasprosessit tulee suunnitella siten, että käytännön työssä pystytään käsittelemään asiakkaiden ja potilaiden asioita niin, etteivät sivulliset niitä näe tai kuule.

Kenelläkään sivullisella ei ole oikeutta esimerkiksi asiakas- ja potilastietojen käsittelyyn. Sivullisella tarkoitetaan muita kuin asiakkaan tai potilaan hoitoon tai palveluun tai niihin liittyviin tehtäviin osallistuvia henkilöitä. Sivullisia ovat myös esimerkiksi yksikössä hoidettavat tai yksikön palvelujen piirissä olevat muut asiakkaat.

Henkilö- sekä asiakas- ja potilastietoja käsitellään Siun sotessa sähköisten asiakas- ja potilastietojärjestelmien avulla, jolloin niiden tekninen ja toiminnallinen toteutus ja tietoarkkitehtuuri on suunniteltava niin, että kussakin tehtävässä voidaan käyttää vain kyseisen tehtävän edellyttämiä tietoja ja vain siinä laajuudessa kuin tehtävien hoito edellyttää. Kullakin työntekijällä on oikeus nähdä vain sellaisia asiakkaita tai potilaita koskevia tietoja, joita hän työtehtävissään tarvitsee. Tämä koskee myös sosiaalihuollon ja terveydenhuollon toimintayksiköissä työskenteleviä harjoittelijoita tai opiskelijoita.

Tietosuojavastaavan vinkit!

- Kirjaudu ulos tietojärjestelmistä ja lukitse työasema aina käytön jälkeen ja poistuessasi työpisteeltäsi! Tiesithän, että työaseman voi lukita näppäimistöltä *Windows-näppäin+L-kirjain-komennolla*!

[49] Siun sote – Toimintaohje: Käyttövaltuuksien hallinnan ja tunnistautumisen käytännöt (Siun sote intra)

- Sijoita käytössäsi olevan työaseman näyttö siten, etteivät sivulliset pääse näkemään näytön tietoja. Tarvittaessa työasemien näytöille voi asentaa näytönsuojakalvon, jonka hankkimisesta voit keskustella esihenkilösi kanssa.

6.5 Henkilötunnuksen käsittely

Henkilötunnus on yksilöimiskeino, joka yksilöi henkilön vielä tarkemmalla tasolla kuin esimerkiksi nimi. Kahta saman henkilötunnuksen omaavaa henkilöä ei voi Suomessa olla. Henkilötunnus on tarkoitettu pysyväksi ja sitä muutetaan vain perustellusta syystä.

Henkilötunnus kertoo muutakin tietoa henkilöstä, kuin vain syntymäpäivän, -kuukauden ja -vuoden. Henkilötunnuksen jälkimmäisellä osalla eli yksilönumerolla, erotetaan toisistaan henkilöt, joilla on sama syntymäaika. Numeron toiseksi viimeinen merkki on miehillä pariton ja naisilla parillinen. Käytännössä yksilönumeroksi annetaan jokin luku väliltä 002–899. Henkilötunnuksen viimeinen merkki on tarkistusmerkki (numero tai kirjain), joka muodostuu erillisen kaavan mukaisesti. Syntymäajan jäljessä oleva merkki kertoo syntymävuosisadan:

- yhdysmerkki (-) tarkoittaa, että henkilö on syntynyt 1900-luvulla
- A-kirjain tarkoittaa, että henkilö on syntynyt 2000-luvulla
- plusmerkki (+) tarkoitti, että henkilö oli syntynyt 1800-luvulla.

Henkilötunnusta saa käsitellä rekisteröidyn suostumuksella tai jos käsittelystä säädetään laissa. Lisäksi henkilötunnusta saa käsitellä, jos rekisteröidyn yksiselitteinen yksilöiminen on tärkeää:

- laissa säädetyn tehtävän suorittamiseksi
- rekisteröidyn tai rekisterinpitäjän oikeuksien ja velvollisuuksien toteuttamiseksi
- historiallista tai tieteellistä tutkimusta tai tilastointia varten.

Henkilötunnusta saa käsitellä mm. luotonannossa tai saatavan perimisessä, vakuutus-, luottolaitos-, maksupalvelu-, vuokraus- ja lainaustoiminnassa, luottotietotoiminnassa, terveydenhuollossa, sosiaalihuollossa ja muun sosiaaliturvan toteuttamisessa tai virka-, työ- ja muita palvelussuhteita ja niihin liittyviä etuja koskevissa asioissa. Henkilötunnusta ei saa merkitä tarpeettomasti henkilörekisterin perusteella tulostettuihin tai laadittuihin asiakirjoihin. Lisäksi tietosuojavaltuutetun toimisto on suositellut, että henkilötunnusta tai sen osaa ei käytettäisi myöskään laskun viitenumerossa tai osana viitenumeroa. Laskut voidaan yksilöidä muullakin tunnuksella, mm. erillisellä asiakasnumerolla tai koodilla. Yleinen hyvän tietojenkäsittelytavan periaate on, ettei kenenkään yksityisyyttä perusteettomasti vaaranneta.

Tietosuojavastaavan vinkit!

- Muista, että pelkästään henkilötunnuksen kysyminen asiakkaalta ei ole luotettava tapa selvittää mm. puhelimessa asioivan henkilön henkilöllisyyttä. Henkilötunnus voi olla tiedossa myös muilla

kuin asianomaisella itsellään, eikä henkilötunnusta ole tarkoitettu henkilöiden tunnistamiseen vaan yksilöimiseen!

- Henkilötunnuksen sijaan voidaan asiakas yksilöidä esimerkiksi asiakas-/potilasnumerolla (mm. Mediatrinumero). Huomioitavaa kuitenkin on, ettei esimerkiksi suojaamattomassa sähköpostiliikenteessä tai Teams-viesteissä Mediatrinumeroa tule yhdistää asiakas- tai potilastietoon! Mediatrinumero on myös henkilötieto.
- Henkilötunnuksen sijaan voidaan työntekijä yksilöidä henkilönumerolla (mm. HR-järjestelmässä oleva henkilönumero). Huomioitavaa kuitenkin on, että henkilönumeron käsittelyssä tulee myös huolehtia tietojen suojaamisvelvoitteesta. Henkilönumero on myös henkilötieto.
- Hae aina tietoja tietojärjestelmästä pelkästään henkilötunnuksella! Mikäli esimerkiksi asiakasta haetaan asiakastietojärjestelmästä vain nimellä, riski henkilön virheelliseen yksilöintiin kasvaa ja tietojärjestelmästä avautuvat käsittelyyn väärän henkilön tiedot. Tällainen poikkeama täyttää henkilötietojen tietoturvaloukkauksen määritelmän!

6.6 Henkilön tunnistaminen

Henkilöllisyys ja identiteetti kuvaavat sitä, keitä olemme. Erilaiset tunnisteet ovat vain yksi osa henkilön identiteettiä. Tyypillisin tunniste on henkilön nimi, jonka rinnalle Suomessa on asetettu jokaiselle yksiköllinen henkilötunnus. Näiden ohella käytössä on myös biometrisia tunnisteita, joista tunnetuin on sormenjälki.

Henkilön tunnistamiseen on valikoima keinoja. Tunnistaminen voidaan jakaa kahteen ryhmään: tunnistetaan fyysisesti läsnä oleva henkilö ja tunnistetaan sähköisesti asioiva henkilö digitaalisessa toimintaympäristössä. Fyysisessä toimintaympäristössä henkilön tunnistaminen tapahtuu tunnistusasiakirjoista ja/tai niiden sähköisestä lukemisesta (mm. Kela-kortista). Tunnistamisen jälkeen tieto tulee todentaa.

Digitaalisessa toimintaympäristössä henkilö usein tunnistautuu järjestelmään tai sähköiseen palveluun. Tunnistautuminen sähköisesti tapahtuu usein varmentamalla henkilöllisyys kirjautumisen yhteydessä mm. pankkitunnuksilla. Tällöin puhutaan vahvasta tunnistusmenetelmästä. Suomessa sähköisen julkishallinnollisten asiointipalvelujen tunnistaminen on keskitetty pääsääntöisesti Suomi.fi-tunnistukseen.

Asiakkaille Siun soten työntekijöiden tunnistaminen on tärkeää ja se on osa asiakkaiden kohtaamista. Siun soten ammattilaisten ja opiskelijoiden tunnistamista asiakasnäkökulmasta helpottaa yhtenäiset työasut. Lisäksi ammattilaisten on käytettävä kuvallista henkilökorttia. Henkilökortilla henkilö osoittaa kuuluvansa Siun soten henkilökuntaan ja hänellä on oikeus liikkua Siun soten tiloissa. Henkilökortissa tulee olla näkyvillä työntekijän nimi ja ammattinimike. Henkilökorttien käyttö on suositeltavaa myös yhteistyökumppaneiden kanssa tai edustettaessa Siun sotea esimerkiksi erilaisissa koulutustilaisuuksissa ja verkostotapaamisissa. Myös opiskelijoilla tulee olla näkyvillä nimikyltti, josta käy ilmi opiskelijan nimi ja se, että hän on opiskelija (mm. sairaanhoitajaopiskelija, sosionomiopiskelija).

Henkilön tunnistamisen menetelmien lisäksi on hyvä varautua myös tilanteisiin, jossa jostakin syystä henkilö haluaa tai on päätynyt yrittämään esiintymistä väärillä henkilötiedoilla. Tällaisen tilanteen havaitessaan, jokainen

Siun soten työntekijä on velvollinen ilmoittamaan siitä viipymättä Siun soten turvallisuuspäällikölle tai hänen varahenkilölleen. Väärän nimen tai muutoin henkilöllisyydestään väärän tai harhaanjohtavan tiedon antaminen viranomaisille erehdyttämistarkoituksessa on rikoslain (39/1889) mukaan rangaistava teko.

Tietosuojavastaavan vinkit!

- Tutustu asiakkaan tunnistamiseen liittyviin ohjeisiin Siun soten intrassa[50]!
- Muista, että tunnistamiseen käytetty menetelmä on oltava todennettavissa jälkikäteen. Välttämättä tähän ei löydy omaa kirjaamispaikkaa asiakas- ja potilastietojärjestelmästä. Kirjaamispaikka ja tapa on sovittava muiden kirjaamiskäytäntöjen ohella, riippuen siitä, mihin palveluun tai hoitoon liittyvät merkinnät kyseisessä asioinnissa normaalisti kirjattaisi.
- Muista, että tunnistaminen ei saa koskaan tapahtua siten, että ammattihenkilö kertoo asiakkaan nimen ja henkilötunnuksen, jonka jälkeen asiakas hyväksyy ne.
- Älä jätä asiakasta yksin ammattilaisen omalle työasemalle vastaanoton tai tutkimuksen ajaksi, mikäli työasema ei ole tähän käyttöön tarkoitettu! Asiakkaille tarjottavat etäpalveluun käytettävät työasemat tulee olla sellaisia, joista asiakas ei pääse esimerkiksi Siun soten intraan tai avaamaan mm. työntekijän sähköpostia tai Teams-keskusteluja!
- Riskienhallinnan näkökulmasta on hyvä ymmärtää, että asiakas saattaa tallentaa käydyn etäpalvelun keskustelun! Huomioi myös, että asiakkaan kotona voi olla muita sivullisia paikalla, jolle asiakkaan asiat eivät kuulu. Varmista, että asiakas ymmärtää, että hän itse vastaa siitä, keitä paikalla on ja ketkä voivat kuulla ammattilaisen kanssa käydyn keskustelun hänen asioistaan!
- Muista tunnistamisen merkitys ja menetelmät myös työhönottotilanteissa! Lisäksi tulee muistaa sosiaali- ja terveydenhuollon ammattihenkilöiden ammattioikeuden tarkastaminen Valviran ylläpitämästä keskusrekisteristä (JulkiTerhikki/JulkiSuosikki)[51].
- Tutustu Siun soten henkilöturvaohjeeseen Siun soten intrassa[52]! Muista, että kuvallista henkilökorttia tulee säilyttää huolellisesti ja jokainen työntekijä vastaa henkilökortistaan itse! Henkilökortin kuva ja sen tiedot (mm. nimen muutos, ammattinimikkeen/työtehtävän vaihtuminen) tulee päivittää tarvittaessa!
- Huomioi, että henkilökortissa näkyviä tietoja (mm. ammattilaisen etu- ja sukunimi) voidaan rajoittaa vain perustellusta syystä! Asiakkaalla on oikeus tietää, kuka ammattilainen tai opiskelija häntä hoitaa tai hänen asiaansa käsittelee. Mikäli asiakas siis kysyy ammattilaiselta nimeä esimerkiksi hoitotoimenpiteen tai palvelussa asioinnin yhteydessä, ammattilainen on velvollinen kertomaan oman nimensä asiakkaalle!

[50] Siun sote – Potilaan tai asiakkaan tunnistaminen (Siun sote intra)
[51] Valvira – Sosiaali- ja terveydenhuollon ammattihenkilöiden keskusrekisterit (JulkiTerhikki/JulkiSuosikki)
[52] Siun sote – Henkilöturvaohje (Siun sote intra)

6.7 Turvakielto

Turvakielto on poikkeuksellinen henkilötietojen turvaamistoimi, jolla rajoitetaan henkilön osoite-, asuinpaikka- ja kotikuntatiedon luovuttamista väestötietojärjestelmästä vain sellaisille viranomaisille, joilla on oikeus turvakiellon alaisten tietojen käsittelyyn. Turvakieltoa voi hakea henkilö, jolla on perusteltu ja ilmeinen syy epäillä itsensä tai perheensä terveyden tai turvallisuuden olevan uhattuna. Tällaisia tilanteita voivat olla esimerkiksi todistajansuojelutilanne, perheväkivaltatilanne tai toimiminen sellaisessa ammatissa, jossa henkilö joutuu kokemaan säännöllistä vakavan fyysisen väkivallan uhkaa.

Turvakieltoa haetaan kirjallisesti Digi- ja väestötietovirastolta (DVV)[53]. Turvakiellon myöntämisen jälkeen, henkilön osoite- ja kotikuntamerkintä piilotetaan viranomaisten käyttämästä väestötietojärjestelmästä ja estetään tiedon välittyminen. Turvakiellon alaiset tiedot eivät tällöin näy Siun soten asiakas- ja potilastietojärjestelmissä. Turvakiellon alaisia tietoja ei missään tilanteessa saa tallentaa Siun soten tietojärjestelmiin tai liittää osaksi asiakkaan tai potilaan asiakirjoja, kirjeitä tai muita hoitoon tai palveluun liittyviä paperisia aineistoja.

Siun sotessa on nimetyt turvakieltopostin käsittelijät, joille on anottu Väestörekisterikeskukselta suorakäyttöoikeudet väestötietojärjestelmään. He voivat tarvittaessa katsoa turvakieltohenkilön osoitteen. He eivät saa luovuttaa tietoja edelleen eivätkä antaa niitä sivullisen nähtäväksi tai käsiteltäväksi.

Tietosuojavastaavan vinkit!

- Tutustu turvakieltopostin käsittelyohjeeseen Siun soten intrassa[54]!
- Turvakiellon alaisia osoitetietoja ei saa tallentaa Siun soten tietojärjestelmiin, joten huomioi, ettei osoite näy missään asiakirjassa tai lomakkeella!
- Turvakieltohenkilölle lähetettävien viestien tai kirjeiden osoitekenttään ei saa merkitä *”Turvakielto”*-merkintää!

7 Sosiaalihuollon asiakastietojen käsittely

Siun soten sosiaalihuollon asiakasrekisterissä olevia tietoja käytetään ensisijaisesti asiakkaan sosiaalihuoltoon liittyvän asian käsittelyssä ja palvelussa. Asiakastietoja voidaan myös käyttää sosiaalihuollon ammattihenkilöiden

[53] Digi- ja väestötietovirasto - Turvakielto
[54] Siun sote – Turvakieltopostin käsittely (Siun sote intra)

toiminnan valvonnassa, toiminnan ohjauksessa, suunnittelussa ja johtamisessa, tutkimus- ja opetustoiminnassa sekä valtakunnallisten lakisääteisten tilastotietojen tuottamisessa sekä tietojohtamisessa.

Siun sote, sosiaalihuollon palvelunjärjestäjänä, toimii rekisterinpitäjänä sosiaalihuollon toiminnassa syntyneille ja käsitellyille asiakastiedoille. Sosiaalihuollon asiakasrekisteriin kuuluvat myös niiden yksityisten sosiaalihuollon palveluntuottajien tuottamat ja käsittelemät asiakastiedot, joiden kanssa Siun sote on tehnyt sopimuksen. Siun sote toimii rekisterinpitäjänä lisäksi palvelusetelillä järjestettävissä palveluissa syntyvien asiakastietojen osalta. Sosiaalihuollon asiakasrekisterin vastuuhenkilö (rekisterinpitäjän edustaja) Siun sotessa on perhe- ja sosiaalipalvelujen toimialuejohtaja.

Sosiaalihuollon asiakasrekisterin rekisteröidyksi kutsutaan sitä henkilöä, jota asiakastieto koskee. Sosiaalihuollossa rekisteröity on se henkilö, joka on hakenut sosiaalihuollon palvelua, käyttää sitä tai on omasta tahdostaan riippumatta sosiaalihuollon toimenpiteiden kohteena. Käytännössä tämä tarkoittaa sitä, että rekisteröity on henkilö, jonka nimiin sosiaalihuollon asiakkuus on kirjattu.

Siun soten sosiaalihuollon asiakasrekisterin muodostavat tietojärjestelmissä olevat tiedot ja paperiset asiakaskertomukset. Asiakasrekisteriin kuuluvat kaikki asiakkaan asian käsittelyssä ja sosiaalihuollon eri palvelutehtävissä syntyvät tiedot mukaan lukien päätökset. Sosiaalihuollon asiakasrekisterin tietojen käsittelyä valvotaan ja seurataan Siun soten valvontasuunnitelman mukaisesti. Lisäksi asiakkailla on oikeus saada pyydettäessä tieto siitä, kuka on käsitellyt ja kenelle on luovutettu häntä koskevia asiakastietoja sosiaalihuollon asiakasrekisterissä.

Tietosuojavastaavan vinkit!

- Tutustu sosiaalihuollon asiakirjojen käsittelyn ja arkistoinnin toimintaohjeeseen[55]!
- Siun soten sosiaalihuollon asiakasrekisterin tietosuojaseloste on saatavilla Siun soten verkkosivuilla[56].
- **Lukuvinkki:** Tietosuojavaltuutetun toimisto on julkaissut oppaan Sosiaalihuollon asiakastietojen käsittelystä[57].
- Tutustu yksityisten palveluntuottajien Siun soten lukuun tuottamissa palveluissa muodostuneiden asiakirjojen käsittelyn ja arkistoinnin ohjeeseen[58]!

[55] Siun sote – Toimintaohje: Sosiaalipalvelujen asiakirjojen käsittely ja arkistointi (Siun sote intra)
[56] Siun sote – Tietosuojaseloste: Sosiaalihuollon asiakasrekisteri
[57] Tietosuojavaltuutetun toimisto – Sosiaalihuollon asiakastietojen käsittely (opas)
[58] Siun sote - Yksityisten palveluntuottajien Siun soten lukuun tuottamissa palveluissa muodostuneiden asiakirjojen käsittely ja arkistointi (Siun sote intra)

- Huomioithan, että tietosuojavastaavat ovat henkilötietojen käsittelyn erityisasiantuntijoita! Sosiaalihuollon asiakastietojen käsittelyyn ja kirjaamiseen liittyvät ohjeet ovat ensisijaisesti toimialueiden vastuulla ja tämä käsikirja ei kata kaikkia asiakastietojen käsittelyyn liittyviä tilanteita tai toimialueella sovittuja toimintamalleja!

7.1 Sosiaalihuollon asiakastietojen käsittelyä ohjaava lainsäädäntö

Sosiaalihuoltoa ja siihen liittyvää asiakastietojen käsittelyä ohjaavat mm. seuraavat lait ja asetukset:

- Sosiaalihuoltolaki (1301/2014)
- Laki sosiaalihuollon asiakasasiakirjoista (254/2015, nk. asiakasasiakirjalaki, joka kumoutuu 1.1.2024 alkaen uuden asiakastietolain tullessa voimaan)
- Laki sosiaalihuollon asiakkaan asemasta ja oikeuksista (812/2000, jatkossa asiakaslaki)
- Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (784/2021, 1.1.2024 alkaen laki sosiaali- ja terveydenhuollon asiakastietojen käsittelystä 703/2023, jatkossa asiakastietolaki)
- Sosiaali- ja terveysministeriön asetus käyttöoikeudesta asiakastietoon (825/2022, jatkossa käyttöoikeusasetus)
- Laki viranomaisen toiminnan julkisuudesta (621/1999, jatkossa julkisuuslaki).

Lisäksi sosiaalihuoltoa ohjaa palvelutehtäväkohtainen lainsäädäntö (mm. lastensuojelulaki 417/2007). Sosiaalihuoltoa koskevan erityislainsäädännön lisäksi asiakkaan yksityiselämän suojaa sääntelee Suomen perustuslaki (731/1999). Asiakkaiden henkilötietojen käsittelyn osalta noudatetaan ja sovelletaan EU:n yleistä tietosuoja-asetusta (679/2016) sekä tietosuojalakia (1050/2018).

Jokaisen sosiaalihuollon ammattihenkilön ja Siun soten sosiaalihuollossa työskentelevän työntekijän velvollisuus on perehtyä sosiaalihuollon lainsäädäntöön sekä erityislainsäädäntöön sekä on velvollinen ylläpitämään ja kehittämään ammattitaitoaan. Työntekijän velvollisuuksia tukevat myös Siun soten sosiaalihuollon asiakastietojen käsittelystä annetut ohjeet sekä työnantajan velvoite tukea ammattihenkilöiden osaamisen kehittämistä. Jokaisen ammattihenkilön velvollisuutena on lisäksi ilmoittaa, mikäli havaitsee työssään poikkeaman tai annetut ohjeet ovat puutteellisia tai toiminnassa ei noudateta lainsäädäntöä.

7.2 Sosiaalihuollon asiakastiedot ovat salassa pidettäviä

Kansallisessa lainsäädännössä on useassa kohtaa nimenomaisesti erikseen säädetty sosiaalihuollon tietojen salassapitovelvoitteesta. Myös julkisuuslaissa sosiaalihuollon asiakkuus on säädetty salassa pidettäväksi. Asiakaslain mukaan sosiaalihuollon asiakirjat, jotka sisältävät tietoa sosiaalihuollon asiakkaasta tai muusta yksityisestä henkilöstä, ovat salassa pidettäviä. Asiakirjaa tai sen kopiota tai tulostetta ei saa näyttää eikä luovuttaa sivulliselle, eikä antaa sitä teknisen käyttöyhteyden avulla tai muulla tavoin sivullisen nähtäväksi tai käytettäväksi. Lisäksi asiakaslain mukaan on kiellettyä paljastaa

- asiakirjan salassa pidettävää sisältöä

- tietoja, jotka asiakirjaan merkittynä olisi salassa pidettävä
- muuta sosiaalihuollon tehtävissä toimiessaan tietoonsa saamansa seikkaa, josta on laissa säädetty vaitiolovelvollisuus.

7.3 Asiakastiedot tulee suojata sivullisilta

Asiakastiedot on säilytettävä ja suojattava niin, etteivät ulkopuoliset pääse niihin käsiksi. Kenelläkään sivullisella ei ole oikeutta asiakastietojen käsittelyyn. Sivullisella tarkoitetaan muita kuin asiakkaan palveluun tai niihin liittyviin tehtäviin osallistuvia henkilöitä. Sivullisia ovat myös esimerkiksi palvelujen piirissä olevat muut asiakkaat.

Asiakastietojen osalta tulee varmistua siitä, ettei niitä voida vahingossa tai laittomasti hävittää, muuttaa, luovuttaa, siirtää tai muutoin laittomasti käsitellä. Tietojen suojausvelvollisuus koskee sekä paperimuodossa että sähköisessä muodossa olevia tietoja. Paperimuotoisia asiakastietoja on säilytettävä esimerkiksi lukitussa kaapissa tai lukitussa huoneessa siten, etteivät niitä näe ulkopuoliset. Asiakkaan asioista ei pidä myöskään puhua tai keskustella niin, että sen kuulisivat muut asiakkaat tai sellaiset työntekijät, jotka eivät asiakkaan asioita hoida. Myös toimitilat ja asiakasprosessit tulee suunnitella siten, että käytännön työssä pystytään käsittelemään asiakkaiden asioita niin, etteivät sivulliset niitä näe tai kuule.

Asiakastietoja käsitellään Siun sotessa sähköisten asiakastietojärjestelmien avulla, jolloin niiden tekninen ja toiminnallinen toteutus ja tietoarkkitehtuuri on suunniteltava niin, että kussakin tehtävässä voidaan käyttää vain kyseisen tehtävän edellyttämiä tietoja ja vain siinä laajuudessa kuin tehtävien hoito edellyttää. Asiakastietoja käsittelevillä työntekijöillä tulee tietojen käsittelytapahtumien todentamiseksi olla henkilökohtaiset käyttäjätunnukset tietojärjestelmiin. Kullakin työntekijällä on oikeus nähdä vain sellaisia asiakkaita koskevia tietoja, joita hän työtehtävissään tarvitsee. Tämä koskee myös sosiaalihuollon toimintayksiköissä työskenteleviä tai siellä opintojaan suorittavia harjoittelijoita tai opiskelijoita.

Tietosuojavastaavan vinkit!

- Asiakastietojärjestelmiin määritellyt käyttöoikeudet suojaavat asiakastietoja asiattomalta käsittelyltä. Vaikka käyttöoikeuksin jokin tieto olisi ammattilaisten saatavilla, jokainen sosiaalihuollon ammattilainen saa käsitellä vain välttämättömiä sosiaalihuollon asiakastietoja työtehtävänsä edellyttämässä laajuudessa!
- Sosiaalihuollon ammattilaisella on lähtökohtaisesti käyttöoikeus asiakastietoihin siinä sosiaalihuollon palvelutehtävässä, johon hänen omat työtehtävänsä kohdistuvat. Poikkeuksena voivat olla ne ammattilaiset, joille on työtehtävässä välttämätöntä muodostaa laaja kokonaiskuva sosiaalihuollon asiakkuudesta sekä palveluista (mm. palveluntarpeen arviointi, sosiaalipäivystys).

7.4 Asiakastietojen kirjaaminen

Asiakastietojen laadukas kirjaaminen ja niiden käsittely lainmukaisesti kuuluvat olennaisena osana asiakkaalle annettavaan hyvään palveluun. Oikeus lainmukaisiin asiakaskirjauksiin on myös sosiaalihuollon asiakkaalle lainsäädännössä turvattu perusoikeus. Lisäksi Siun soten työntekijöiden oman oikeusturvan kannalta on tärkeää

tuntea henkilötietojen käsittelyä koskeva yleinen sääntely, kuten myös sosiaalihuollon asiakastietojen käsittelyä koskeva kansallinen erityissääntely.

Jokainen sosiaalihuollon ammattilainen, joka osallistuu asiakastyöhön, on velvollinen kirjaamaan sosiaalihuollon järjestämisen, suunnittelun, toteuttamisen, seurannan ja valvonnan kannalta tarpeelliset ja riittävät tiedot sekä tallentamaan ne käytössä olevaan asiakastietojärjestelmään. Kirjaamisvelvollisuus alkaa, kun hyvinvointialue on saanut tiedon henkilön palveluntarpeesta tai on ryhtynyt toteuttamaan sosiaalihuollon palvelua. Asiakkuuden päättyminen on myös kirjattava asiakastieto. Sosiaalihuollon ammattilaisten ohella myös opiskelijoilla sekä muulla avustavalla henkilöstöllä on kirjaamisvelvoite, mikäli he osallistuvat asiakastyöhön. Opiskelijoiden tai avustavan henkilöstön kirjaamisvelvoitteesta voidaan myös sopia muutoin, huomioiden henkilön työtehtävän.

Lähtökohta on, että asiakkaasta kirjattavan tiedon on oltava tarpeellista siihen käyttötarkoitukseen, mitä varten tietoa kerätään sosiaalihuollon asiakkaasta. Tässä sosiaalihuollon ammattilaisen harkinta ja kokemus omasta alastaan on tärkeässä roolissa. Sosiaalihuollon ammattilainen tekee tietojen kirjaamishetkellä arvion siitä, mikä hänen käsityksensä mukaan on tarpeellista. Tietojen tarpeellisuus vaihtelee eri sosiaalihuollon asiakkaiden välillä, eli kirjattavien tietojen tarpeellisuutta tulee harkita aina yksilökohtaisesti. Lainsäädännöstä tulevat tietyt määräykset tiedoista, jotka kaikista asiakkaista tulee kirjata.

Asiakastietojen kirjaaminen on tehtävä viipymättä, kun asiakkaan asiaa on käsitelty sosiaalihuollossa. Kirjauksessa käytetyn kielen tulisi olla niin sanottua hyvää yleiskieltä, jolloin väärinymmärrysten mahdollisuus vähenee. Hyvä lähtökohta on pyrkiä mahdollisimman konkreettiseen asioiden kuvaamiseen, jotta toinen henkilö ymmärtää tekstin samoin kuin alkuperäisen kirjauksen tekijä on tarkoittanut. Hyvällä yleiskielellä minimoidaan sitä mahdollisuutta, että hyvää tarkoittavasta puhekielen ilmauksesta voi toisen silmissä tulla päinvastainen vaikutelma kuin mitä kirjoittaja on alun perin tarkoittanut.

Tietosuojavastaavan vinkit!

- Jo sosiaalihuollon asiakastietoja kirjatessa on hyvä pitää mielessä, että asiakkaalla on oikeus saada nähdä itseään koskevat tiedot, saada niistä jäljennökset sekä vaatia tietojen korjaamista tarvittaessa!
- Muista, että kirjatun tiedon lähteellä on merkitystä! Kirjaa siis selkeästi, kenen kertomasta asiasta tai näkemyksestä kulloinkin on kyse, mikäli asiakkaan asiaan liittyy muiden henkilöiden kuulemista tai perheen kanssa keskustelua. Myös sosiaalihuollon ammattihenkilön omat arviot tulee kirjauksesta erottua selkeästi!
- Asiakastiedoista tulee ilmetä, millaisten tietojen ja käsitysten varassa milloinkin on toimittu. Vaikka myöhemmin ilmenisi muuta, asia voidaan jälkikäteenkin arvioida kirjaamishetken näkemykseksi eikä sitä voi vaatia korjattavaksi tai muutettavaksi jälkikäteen.

- Tutustu Sosmetan sosiaalihuollon asiakirjarakenteiden ja metatietojen palveluun[59] ja Kanta-palvelujen käsikirjaan sosiaalihuollon toimijoille[60]!

7.4.1 Terveyttä koskevien tietojen käsittely sosiaalihuollossa

Sosiaalihuollon palveluissa voi olla tarve käsitellä ja kirjata myös asiakkaan terveyteen liittyviä tietoja. Terveydentilatietojen kirjaamista sosiaalihuollon asiakastietoihin voidaan pitää tietyissä tilanteissa tarpeellisina. Tällaisia tilanteita ovat mm. lastensuojeluasian käsittely, jos esimerkiksi lastensuojeluilmoituksen perusteena on ollut epäily lapseen kohdistuneesta pahoinpitelystä tai jos vammaispalvelujen yhteydessä joudutaan käsittelemään asiakkaan sairautta tai terveydentilaa koskevia arkaluonteisia tietoa. Tietoja ei kuitenkaan tällöinkään tule kirjata tarpeettoman laajasti. Kirjauksissa tulee kiinnittää huomiota siihen, että asiakastietoihin kirjataan vain sellaisia terveyteen liittyviä tietoja, jotka ovat tarpeen kyseessä olevan etuuden tai palvelun myöntämisedellytysten arvioimiseksi tai kyseisen palvelun antamisessa.

Mikäli sosiaalihuollon toimintayksikössä työskentelee terveydenhuollon ammattihenkilö, jonka työtehtäviin kuuluu antaa asiakkaille tutkimusta tai hoitoa, heidän tekemänsä kirjaukset asiakkaasta ovat potilastietoja. Näiden tietojen käsittelyyn kohdentuu potilastietojen laatimista ja säilyttämistä koskevaa lainsäädäntöä, joka on huomioitava tietojen käsittelyssä. Potilastiedot tulee pitää erillään sosiaalihuollon asiakastiedoista.

Tietosuojavastaavan vinkit!

- Huomioi, että sosiaalihuoltoon muualta saadut lääkärintodistukset tai potilastietojen jäljennökset ovat sosiaalihuollon asiakastietoja.
- Huomioitavaa on, että myös sosiaalihuollossa työskentelevien ammattilaisten työtehtäviin voi kuulua mm. asiakkaan verenpaineen tai verensokerin mittaaminen sekä muita terveydenhuoltoon liittyviä tehtäviä, mutta joiden hoitaminen ei kuitenkaan edellytä terveydenhuollon ammattihenkilön pätevyyttä. Tästä syystä myös sosiaalihuollon asiakastiedoissa on usein terveydentilaa koskevia merkintöjä, mutta niissä ei silti ole kyseessä potilastietojen kirjaaminen!

7.4.2 Monialainen yhteistyö

Monialaisessa yhteistyössä joudutaan lähes poikkeuksetta tilanteeseen, jossa luovutetaan asiakas- tai potilastietoja toisille asiakkaan asian hoitamiseen osallistuville tahoille. Tällöin tietoja luovutetaan sellaiseen

[59] THL – Sosmeta – Sosiaalihuollon asiakirjarakenteiden ja metatietojen palvelu
[60] Kanta – Kanta-palvelujen käsikirja sosiaalihuollon toimijoille

tarkoitukseen, jota ei ole kyseisille tiedoille määritelty käyttötarkoitukseksi. Tietojen luovutuksista tulee tehdä asianmukaiset luovutusmerkinnät.

Velvoite monialaiseen yhteistyöhön koskee sekä sosiaalihuoltoa että terveydenhuoltoa. Sosiaalihuoltolain mukaan asiakkaan palvelutarpeen arvioimiseksi, päätösten tekemiseksi ja sosiaalihuollon toteuttamiseksi on sosiaalihuollossa huolehdittava siitä, että käytettävissä on asiakkaan yksilöllisiin tarpeisiin nähden riittävästi asiantuntemusta ja osaamista. Mikäli sosiaalihuollon ammattihenkilö pyytää, muiden tahojen on osallistuttava asiakkaan palvelutarpeen arviointiin sekä asiakassuunnitelman laatimiseen. Terveydenhuoltolaissa asetetaan puolestaan terveydenhuollon ammattihenkilölle velvollisuus hoidon tarpeen arvioinnin yhteydessä arvioida myös sitä, onko asiakkaalla ilmeinen sosiaalihuollon tarve.

Kun monialaisen yhteistyön tarve on tunnistettu, asiakkaan asiaa hoitava taho kutsuu koolle asiantuntijoita sen perusteella, mitä tuen ja hoidon tarpeita asiakas on ilmaissut. Ennen koolle kutsumista, asiakkaan asiaa hoitava taho sopii asiakkaan kanssa, miten laajaa yhteistyötä asiakkaan kokonaisvaltainen tukeminen edellyttää ja keitä sosiaali- ja terveydenhuollon ammattihenkilöitä ja mahdollisesti asiakkaan läheisiä työntekijä voi kutsua yhteistyöhön.

Asiakkaan edun ollessa kyseessä, monialainen yhteistyö tarkoittaa sitä, että eri ammattihenkilöt ovat yhteydessä keskenään ja tarvittavissa määrin vaihtavat tietoja asiakkaan tilanteesta. Asiakkaan antamasta suostumuksesta tulee olla asianmukainen merkintä asiakas- ja potilastiedoissa. Mikäli asiakas haluaa rajoittaa tai kieltää joidenkin toimijoiden osallistumisen tai hän haluaa rajoittaa tiedonvaihtoa toimijoiden välillä, tulee myös tämä merkitä asiakas- ja potilastietoihin. Mikäli asiakas myöhemmin peruuttaa antamansa suostumuksen, tulee peruutuksen vastaanottaneen tahon huolehtia siitä, että suostumuksen peruutus tavoittaa kaikki monialaiseen yhteistyöhön osallistuneet tahot ja suostumuksen peruutus merkitään myös asiakas- ja potilastietoihin.

Monialaisen yhteistyön kirjaamiseen vaikuttaa se, kuinka monialainen yhteistyö on toteutettu. Mikäli esimerkiksi yhteistyö on toteutettu sosiaalihuollon toimintayksikön sisäisessä yhteistyössä, laadittavat sosiaali- ja terveydenhuollon yhteiset asiakirjat tallennetaan ja säilytetään sosiaalihuollon asiakasrekisterissä. Yhteistyössä laadittu asiakassuunnitelman kopio (jäljennös) voidaan kuitenkin tallentaa myös terveydenhuollon potilasrekisteriin tarvittaessa. Yhteistyössä laaditut terveyden- ja sairaanhoitoa koskevat potilastiedot tallennetaan ja säilytetään terveydenhuollon potilasrekisterissä. Mikäli taas yhteistyötä toteutetaan eri organisaatioiden välillä, kukin yhteistyöhön osallistuva taho tallentaa yhteiset asiakirjat oman organisaationsa rekistereihin, mikäli se on tarpeellista asiakkaan asian hoitamiseksi.

Tietosuojavastaavan vinkit!

- Muista, monialainen yhteistyö toteutetaan aina asiakkaan antamalla suostumuksella!

- Tutustu tarkemmin kirjaamiseen monialaisessa yhteistyössä[61]!
- Yhteisasiakasohjaus on yksi monialaisen yhteistyön muoto, tutustu Siun soten yhteisasiakasohjaukseen[62]!

7.5 Asiakaskertomukseen kuulumattomat tiedot

Kaikki sosiaalihuollossa käsiteltävä tieto ei kuulu osaksi sosiaalihuollon asiakasrekisteriä. Asiakkaan asiakirjoihin kirjataan lähtökohtaisesti vain asiakkaan asioiden hoitamiseen liittyviä asioita. Muiden kuin asiakaskertomukseen kuuluvien tietojen käsittely tapahtuu muualla kuin sosiaalihuollon asiakastietojärjestelmässä. Asiakkaan asiakaskertomukseen eivät kuulu mm. seuraavat tiedot:

- muistutusten ja kanteluiden käsittely
- adoptioneuvonnan asiakirjat
- perhehoidon hallinnolliset asiakirjat (mm. perhehoitajaksi hyväksyminen ja valvonta)
- omaishoidon hallinnolliset asiakirjat (mm. palkkiot, sopimukset)
- hyvinvointialueen verkkosivujen kautta saatu asiakaspalaute
- EU:n tietosuoja-asetuksen mukaiset rekisteröidyn oikeuksiin liittyvät pyynnöt
- lokivalvonta
- asiakasturvallisuusilmoitukset (Laatuportti)
- ammattilaisen toimesta tehty virheellinen tietojen käsittely (mm. väärän asiakkaan tietojen avaaminen vahingossa).

7.6 Asiakastietojen hankkiminen ja pyytäminen

Lähtökohtaisesti sosiaalihuollon asiakkaan tiedot saadaan asiakkaalta itseltään. Tietoja voidaan hankkia ja pyytää myös muilta tahoilta tarvittaessa. Tietojen hankkiminen ja pyytäminen tapahtuu lähtökohtaisesti aina asiakkaan antamalla suostumuksella. Sosiaalihuollossa on lisäksi tilanteita, joissa laissa säädetyn sosiaaliviranomaisen tiedonsaantioikeuden myötä voi olla mahdollista hankkia tarvittavia tietoja.

Sosiaalihuollon asiakkaan läheisverkoston kartoittaminen on myös luokiteltavissa tietojen hankkimiseksi. Asiakkaan läheisverkoston kartoittaminen on mahdollista vain asiakkaan antamalla suostumuksella. Lähiverkoston kartoittamisella tarkoitetaan selvitystä siitä, kuinka omaiset tai asiakkaalle muut läheiset henkilöt osallistuvat asiakkaan tukemiseen. Mikäli asiakas on kykenemätön vastaamaan omasta huolenpidostaan, terveydestään ja turvallisuudestaan, ja läheisverkoston tiedot ovat välttämättömiä palvelutarpeen selvittämiseksi

[61] THL – Kirjaaminen monialaisessa yhteistyössä
[62] Siun sote – Yhteisasiakasohjaus (Siun sote intra)

tai kun tiedot ovat tarpeen alaikäisen lapsen edun vuoksi, tiedonsaantioikeutta tulee tarkastella sosiaalihuollon palvelutehtävään liittyvästä lainsäädännöstä.

Tietosuojavastaavan vinkit!

- Muista, että tietojen hankkiminen ja pyytäminen tulee perustua asiakkaan palveluun liittyvään tarpeeseen. Pohdi siis hankittavien tietojen tarpeellisuutta, sillä asiakkaan palvelun kannalta tarpeettomia tietoja ei tule kerätä.
- Huomioi, että myös muilta viranomaisilta pyydettyjen tietojen ja selvitysten tulee olla sosiaalihuollon asiakassuhteeseen olennaisesti vaikuttavia ja viranomaiselle laissa säädetyn tehtävän vuoksi välttämättömiä asiakkaan sosiaalihuollon tarpeen selvittämiseksi, palvelujen järjestämiseksi ja siihen liittyvien toimenpiteiden toteuttamiseksi. Muista myös, että pyyntö tulee aina perustella (asiakkaan suostumus tai lainsäädäntö)!
- Tutustu tietopyyntöihin liittyviin ohjeistuksiin Siun soten intrasta[63]!

7.7 Asiakastietojen luovuttaminen

Sosiaalihuollon asiakastietoja voidaan luovuttaa, jos tietojen luovuttamiselle on asiakkaan antama suostumus tai siihen on oikeutus lainsäädännön nojalla. Mikäli tietojen luovutus perustuu asiakkaan suostumukseen, tulee suostumuksen olla vapaaehtoinen, yksilöity ja tietoinen tahdonilmaus. Suostumuksessa tulee ilmetä mm. mitä tietoja luovutus koskee, kenelle tietoja luovutetaan ja mitä käyttötarkoitusta varten. Suostumusperusteisessa tietojen luovuttamisessa tulee aina huomioida, että asiakas voi myöhemmin perua antamansa suostumuksen

Jos asiakkaalla ei ole edellytyksiä arvioida annettavan suostumuksen merkitystä, tietoja voidaan luovuttaa asiakkaan laillisen edustajan antamalla suostumuksella. Alaikäisen lapsen laillinen edustaja on pääsääntöisesti hänen huoltajansa. Huoltaja ei kuitenkaan voi antaa suostumusta lapsen puolesta siinä tilanteessa, jos hänellä itsellään ei ole oikeutta tiedonsaantiin. Edunvalvojien ja edunvalvontavaltuutettujen toimivalta puolestaan määräytyy heidän tehtävänsä mukaisesti.

Mikäli asiakas ei itse kykene antamaan suostumusta tietojen luovuttamiseen, eikä hänellä ole laillista edustajaa, tietoja ei voi luovuttaa perustuen suostumukseen. Tällaisissa tilanteissa luovuttaminen on mahdollista vain, jos jokin lainsäännös siihen oikeuttaa. Yksityiskohtaiset tietojen luovuttamisen edellytykset tulee katsoa asianomaisesta lainsäädännöstä (mm. asiakaslaki, asiakastietolaki, rikoslaki, lastensuojelulaki, julkisuuslaki).

[63] Siun sote – Tietojen luovuttaminen ja tietopyynnöt (Siun sote intra)

Kaikki tietojen luovutukset tulee merkitä asianmukaisin tiedoin, perustuipa tietojen luovutus suostumukseen tai lainsäädäntöön. Suostumukset tulee myös arkistoida. Myös asiakkaan ilmoittamat tietojen luovutus- tai hankkimiskiellot tulee merkitä asiakastietoihin.

Tietosuojavastaavan vinkit!

- Muista, että tietojen luovuttaja on aina velvollinen tarkistamaan tietojen luovutuksen perusteen. Tietojen luovuttaja on myös vastuussa siitä, että tietojen luovutus tapahtuu oikeutetusti ja että tiedot vastaanottava taho on tiedonsaantioikeutettu!
- Tutustu tietopyyntölomakkeeseen Siun soten intrassa[64], jota käytetään pyydettäessä tietoja Siun soten toimintayksikön käyttöön asiakkaan palvelun tai hoidon järjestämiseksi!
- Merkitse toteutuneet tietojen luovutukset huolellisesti! Jos salassa pidettävää tietoa sisältäviä asiakirjoja luovutetaan paperisina, luovutettaviin asiakirjoihin tulee tehdä julkisuuslain mukainen salassapitomerkintä!
- Lue lisää tietojen luovuttamisesta ja tietopyynnöistä Siun soten intrasta[65]!

7.8 Asiakastietojen korjaaminen

Asiakkaalla on oikeus pyytää itseään koskevien asiakastietojen korjaamista, jos ne ovat olleet hänen mielestään virheellisiä, tarpeettomia, puutteellisia tai vanhentuneita. Siun soten on myös rekisterinpitäjänä oikaistava ja korjattava virheelliseksi havaitsemansa asiakastiedot oma-aloitteisesti.

Sosiaalityön asiakasprosesseille on tyypillistä, että asiakastiedot tarkentuvat ja täydentyvät ajan kuluessa. Asiakastietoihin kirjattua tietoa ei voida jälkikäteen oikaista virheellisenä, jos se on kirjaamishetkellä näyttänyt asianmukaiselta ja vasta asiakkuusprosessin edetessä osoittautunut virheelliseksi.

Asiakastietojen korjaaminen on toteutettava siten, että alkuperäinen merkintä on myöhemmin osoitettavissa. Korjauksesta on lisäksi käytävä ilmi korjauksen tekijän nimi, virka-asema sekä korjauksen ajankohta ja peruste. Myös tietojen täydentäminen on yksi tietojen korjaamistapa. Mikäli esimerkiksi sosiaalihuollon asiakkaana olevan lapsen vanhemmalla ja sosiaalityöntekijällä on erilainen käsitys perheen tilanteesta, tietoja voidaan korjata täydentämällä niitä vanhemman kertomuksella siitä, mitä hän on sanonut tai mitä on tapahtunut, jos tietoja ei kokonaisuudessaan voida korjata.

Siun sote rekisterinpitäjänä päättää tiedon korjaamisesta. Korjaamisvaatimukset käsitellään yhden kuukauden kuluessa pyynnön saapumisesta. Mikäli korjausvaatimukseen suostutaan, asiakastiedot korjataan ja asiakas saa

[64] Siun sote – Tietopyyntö asiakkaan palvelua tai potilaan hoitoa varten (Siun soten intra)
[65] Siun sote – Tietojen luovuttaminen ja tietopyynnöt

tiedon korjatuista tiedoista. Mikäli korjauspyynnöstä kieltäydytään, korjausvaatimuksen pyytäjälle lähetetään kieltäytymistodistus, jossa kieltäytymisen syy on perusteltu. Asiakkaalla on lisäksi oikeus saattaa asia käsittelyyn tietosuojavaltuutetun toimistoon, mikäli hän katsoo kieltäytymispäätöksen perusteettomaksi.

Tietosuojavastaavan vinkit!

- Mikäli asiakastiedoissa on selkeä todennettavissa oleva virhe (mm. virheellinen päivämäärä tai henkilön nimi), työntekijä voi korjata asiakastiedon itse. Mikäli kirjauksen tehnyt työntekijää ei tavoiteta, yksikön esihenkilö tekee kyseisen korjauksen.
- Sosiaalihuollon asiakastietojärjestelmän osalta, tietojen korjaamiseen voi tarvita Siun soten järjestelmäpääkäyttäjien tai jopa tietojärjestelmätoimittajan toimenpiteitä. Pyydä tarvittaessa apua Siun soten tietojärjestelmien pääkäyttäjiltä!
- Asiakastietojen korjaamisessa on lisäksi arvioitava, onko tapahtumassa ollut kyse henkilötietojen tietoturvaloukkauksesta. Mikäli näin on, loukkauksesta on ilmoitettava viipymättä yksikön esihenkilölle tai Siun soten tietosuojavastaavalle[66]!
- Huomioitavaa on, ettei tietosuojavaltuutettu voi yleisen tietosuoja-asetuksen mukaisena tiedon oikaisemista koskevana asiana määrätä korjattavaksi sosiaaliviranomaisen päätöksiin tai lausuntoihin merkittyjä seikkoja. Näin ollen tietosuojavaltuutettu ei voi määrätä oikaistavaksi esimerkiksi toimeentulotukipäätöksen tai sosiaaliviranomaisen käräjäoikeudelle antaman, lapsen huoltoa koskevan lausunnon tietoja. Viranomainen voi itse oikaista päätöksensä hallintolain mukaisesti.

7.9 Asiakastietojen säilyttäminen ja hävittäminen

Siun sote vastaa rekisterinpitäjänä asiakastietojen säilyttämisestä ja niiden asianmukaisesta hävittämisestä, mikäli niille määritelty säilytysaika päättyy tai tiedoilla ei ole arkistointivelvoitetta. Sosiaalihuollon asiakastietojen säilytysajat on määritelty sosiaalihuollon lainsäädännössä, palvelutehtävittäin. Kanta-palvelujen sosiaalihuollon asiakastiedon arkiston säilytyksestä vastaa Kela. Kansallisarkisto määrää lisäksi arkistolain nojalla joidenkin asiakirjojen arkistoinnista.

Tietosuojavastaavan vinkit!

- Lue lisää asiakirjojen säilytysajoista ja arkistoinnista Siun soten intrasta[67]!

[66] Siun sote – Tietoturvaloukkauksesta ilmoittaminen (Siun sote intra)
[67] Siun sote – Säilytysajat ja arkistointi (Siun sote intra)

8 Terveydenhuollon potilastietojen käsittely

Siun soten terveydenhuollon potilasrekisterissä olevia tietoja käytetään ensisijaisesti potilaan tutkimuksen ja hoidon järjestämiseen, suunnitteluun sekä toteutukseen liittyvissä tehtävissä. Potilastietoja voidaan myös käyttää terveydenhuollon ammattihenkilöiden toiminnan valvonnassa, toiminnan ohjauksessa, suunnittelussa ja johtamisessa, tutkimus- ja opetustoiminnassa sekä valtakunnallisten lakisääteisten tilastotietojen tuottamisessa sekä tietojohtamisessa.

Siun sote terveydenhuollon palvelunjärjestäjänä toimii myös rekisterinpitäjänä terveydenhuollon toiminnassa syntyneille ja käsitellyille potilastiedoille. Terveydenhuollon potilasrekisteriin kuuluvat myös niiden yksityisten terveydenhuollon palveluntuottajien tuottamat ja käsittelemät potilastiedot, joiden kanssa Siun sote on tehnyt sopimuksen. Siun sote toimii rekisterinpitäjänä lisäksi palvelusetelillä järjestettävissä palveluissa syntyvien potilastietojen osalta. Terveydenhuollon potilasrekisterin vastuuhenkilö (rekisterinpitäjän edustaja) Siun sotessa on terveys- ja sairaanhoitopalvelujen toimialuejohtaja.

Terveydenhuollon potilasrekisterin rekisteröidyksi kutsutaan sitä henkilöä, jota potilastieto koskee. Siun soten terveydenhuollon potilasrekisterin muodostavat erikoissairaanhoidon ja perusterveydenhuollon potilastiedot sekä kaikki potilaan hoidossa syntyvät tiedot mukaan lukien kuvantamis- ja tutkimustulokset sekä muut potilaan hoidon kannalta merkittävät materiaalit (mm. videot ja valokuvat). Terveydenhuollon potilasrekisterin muodostavat tietojärjestelmissä olevat tiedot ja paperiset potilaskertomukset.

Terveydenhuollon potilasrekisterin tietojen käsittelyä valvotaan ja seurataan Siun soten valvontasuunnitelman mukaisesti. Lisäksi potilailla on oikeus saada pyydettäessä tieto siitä, kuka on käsittelyt ja kenelle on luovutettu häntä koskevia potilastietoja terveydenhuollon potilasrekisterissä.

Tietosuojavastaavan vinkit!

- Tutustu terveydenhuollon asiakirjojen käsittelyn ja arkistoinnin toimintaohjeeseen[68]!
- Siun soten terveydenhuollon potilasrekisterin tietosuojaseloste on saatavilla Siun soten verkkosivuilla[69].
- Tutustu yksityisten palveluntuottajien Siun soten lukuun tuottamissa palveluissa muodostuneiden asiakirjojen käsittelyn ja arkistoinnin ohjeeseen[70]!

[68] Siun sote – Toimintaohje: Terveydenhuollon asiakirjojen käsittely ja arkistointi (Siun sote intra)
[69] Siun sote – Tietosuojaseloste: Terveydenhuollon potilasrekisteri
[70] Siun sote – Toimintaohje: Yksityisten palveluntuottajien Siun soten lukuun tuottamissa palveluissa muodostuneiden asiakirjojen käsittely ja arkistointi (Siun sote intra)

- Huomioithan, että tietosuojavastaavat ovat henkilötietojen käsittelyn erityisasiantuntijoita! Terveydenhuollon potilastietojen käsittelyyn ja kirjaamiseen liittyvät ohjeet ovat ensisijaisesti toimialueiden vastuulla ja tämä käsikirja ei kata kaikkia potilastietojen käsittelyyn liittyviä tilanteita tai toimialueella sovittuja toimintamalleja!

8.1 Terveydenhuollon potilastietojen käsittelyä ohjaava lainsäädäntö

Terveydenhuoltoa ja siihen liittyvää potilastietojen käsittelyä ohjaavat mm. seuraavat lait ja asetukset:

- Terveydenhuoltolaki (1326/2010)
- Sosiaali- ja terveysministeriön asetus potilasasiakirjoista (94/2022, jatkossa potilasasiakirja-asetus)
- Laki potilaan asemasta ja oikeuksista (785/1992, jatkossa potilaslaki)
- Laki sosiaali- ja terveydenhuollon asiakastietoen sähköisestä käsittelystä (784/2021, 1.1.2024 alkaen laki sosiaali- ja terveydenhuollon asiakastietojen käsittelystä 703/2023, jatkossa asiakastietolaki)
- Sosiaali- ja terveysministeriön asetus käyttöoikeudesta asiakastietoon (825/2022, jatkossa käyttöoikeusasetus)
- Laki viranomaisten toiminnan julkisuudesta (621/1999, jatkossa julkisuuslaki).

Lisäksi terveydenhuoltoa ohjaa palvelukohtainen lainsäädäntö (mm. mielenterveyslaki 1116/1990, tartuntatautilaki 1227/2016). Terveydenhuoltoa koskevan erityislainsäädännön lisäksi potilaan yksityiselämän suojaa sääntelee Suomen perustuslaki (731/1999). Potilaiden henkilötietojen käsittelyn osalta noudatetaan ja sovelletaan EU:n yleistä tietosuoja-asetusta (679/2016) sekä tietosuojalakia (1050/2018).

Jokaisen terveydenhuollon ammattihenkilön ja Siun soten terveydenhuollossa työskentelevän työntekijän velvollisuus on perehtyä terveydenhuollon lainsäädäntöön sekä erityislainsäädäntöön sekä on velvollinen ylläpitämään ja kehittämään ammattitaitoaan. Työntekijän velvollisuuksia tukevat myös Siun soten terveydenhuollon potilastietojen käsittelystä annetut ohjeet sekä työnantajan velvoite tukea ammattihenkilöiden osaamisen kehittämistä. Jokaisen ammattihenkilön velvollisuutena on lisäksi ilmoittaa, mikäli havaitsee työssään poikkeaman tai annetut ohjeet ovat puutteellisia tai toiminnassa ei noudateta lainsäädäntöä.

8.2 Terveydenhuollon potilastiedot ovat salassa pidettäviä

Yleisessä tietosuoja-asetuksessa terveydentilaa koskevat tiedot kuuluvat niin sanottuihin erityisiin henkilötietoryhmiin. Kansallisessa lainsäädännössäkin on useassa kohtaa nimenomaisesti erikseen säädetty terveydenhuollon potilastietojen salassapitovelvoitteesta.

Potilaslain mukaan terveydenhuollon asiakirjat, jotka sisältävät terveydenhuollon potilaasta, ovat salassa pidettäviä. Terveydenhuollon ammattihenkilöitä sitoo salassapitovelvollisuus, joka säilyy ammatinharjoittamisen ja palvelussuhteen päättymisen jälkeenkin. Salassapitovelvollisuus sisältää asiakirjasalaisuuden, vaitiolovelvollisuuden ja hyväksikäyttökiellon.

Terveydenhuollon ammattihenkilöllä on kuitenkin joissakin tilanteissa lakisääteinen velvollisuus tehdä salassapitosäännösten estämättä ilmoitus viranomaisille. Näitä velvollisuuksia on mm. lastensuojelullisissa tai liikenneterveyteen liittyvissä asioissa.

Tietosuojavastaavan vinkit!

- Perehdy terveydenhuollon ammattihenkilön ilmoitusvelvollisuuksiin ja -oikeuksiin Valviran sivulta [71]
- Potilastietojen käsittely hoitosuhteen päättymisen jälkeen ammattihenkilön oman osaamien kehittämiseksi ei ole sallittua, mikäli se on tietojen käsittelyn ainoa tarkoitus!
- Omien potilastietojen katselu potilastietojärjestelmästä on kielletty, sillä tietojen käyttöoikeus tulee perustua hoitosuhteeseen! Siun soten työntekijän on tarvittaessa pyydettävä omat potilastietonsa hoitavasta yksiköstä tai katsottava niitä OmaKanta-palvelun kautta.
- Siun soten työntekijöiden omaisten tai läheisten potilastietojen käsittelyssä tulee käyttää erityistä harkintaa. Mikäli työntekijällä ei ole olemassa olevaa hoitosuhdetta omaiseen tai läheiseen, potilastietojen käsittely on kiellettyä. Potilastietojärjestelmässä esimerkiksi huollettavien tietojen katselu tai puolison ajanvaraustietojen katselu myös henkilöiden omasta pyynnöstä on kielletty! Omaisten tai läheisten hoitoon osallistumista kannattaa myös harkita tarkoin ja mahdollisuuksien mukaan heidän hoitonsa tulee ohjata toiselle ammattihenkilölle.
- Siun sote toimii opetusorganisaationa ja tarjoaa minipuolisen oppimisympäristön eri koulutusalojen opiskelijoille. On kuitenkin hyvä huomioida, että potilaalta tulee tiedustella, suostuuko hän olemaan ns. opetuksen kohteena. Mikäli potilas kieltäytyy, ei myöskään häntä koskevia potilastietoja saa käsitellä potilastietojärjestelmässä opetukseen liittyen.

8.3 Potilastiedot tulee suojata sivullisilta

Potilastiedot on säilytettävä ja suojattava niin, etteivät ulkopuoliset pääse niihin käsiksi. Kenelläkään sivullisella ei ole oikeutta potilastietojen käsittelyyn. Sivullisella tarkoitetaan muita kuin potilaan hoitoon tai siihen muutoin liittyviin tehtäviin osallistuvia henkilöitä. Sivullisia ovat myös esimerkiksi yksikössä hoidettavat tai yksikön palvelujen piirissä olevat muut potilaat.

Potilastietojen osalta tulee varmistua siitä, ettei niitä voida vahingossa tai laittomasti hävittää, muuttaa, luovuttaa, siirtää tai muutoin laittomasti käsitellä. Tietojen suojausvelvollisuus koskee sekä paperimuodossa että sähköisessä muodossa olevia tietoja. Paperimuotoisia potilastietoja on säilytettävä esimerkiksi lukitussa kaapissa tai lukitussa huoneessa siten, etteivät niitä näe ulkopuoliset. Potilaiden asioista ei pidä myöskään puhua tai

[71] Valvira – Sosiaali- ja terveydenhuollon ammattihenkilön ilmoitusvelvollisuudet ja -oikeudet

keskustella niin, että sen kuulisivat muut potilaat tai sellaiset työntekijät, jotka eivät osallistu potilaan hoitoon. Myös toimitilat ja asiakasprosessit tulee suunnitella siten, että käytännön työssä pystytään käsittelemään potilaiden asioita niin, etteivät sivulliset niitä näe tai kuule.

Potilastietoja käsitellään Siun sotessa sähköisten potilastietojärjestelmien avulla, jolloin niiden tekninen ja toiminnallinen toteutus ja tietoarkkitehtuuri on suunniteltava niin, että kussakin tehtävässä voidaan käyttää vain kyseisen tehtävän edellyttämiä tietoja ja vain siinä laajuudessa kuin tehtävien hoito edellyttää. Potilastietoja käsittelevillä työntekijöillä tulee tietojen käsittelytapahtumien todentamiseksi olla henkilökohtaiset käyttäjätunnukset tietojärjestelmiin. Kullakin työntekijällä on oikeus nähdä vain sellaisia potilaita koskevia tietoja, joita hän työtehtävissään tarvitsee. Tämä koskee myös terveydenhuollon toimintayksiköissä työskenteleviä tai siellä opintojaan suorittavia harjoittelijoita tai opiskelijoita.

Tietosuojavastaavan vinkit!

- Potilastietojärjestelmiin määritellyt käyttöoikeudet suojaavat potilastietoja asiattomalta käsittelyltä. Vaikka käyttöoikeuksin jokin tieto olisi ammattilaisten saatavilla, jokainen terveydenhuollon ammattilainen saa käsitellä vain välttämättömiä potilastietoja työtehtävänsä edellyttämässä laajuudessa!
- Toimitiloissa on kiinnitettävä huomiota siihen, ettei sivulliset pääse kuulemaan tai näkemään potilastietoja. Huomiota kannattaa kiinnittää mm. tietokoneiden näyttöjen sijoitteluun, lääkärinkierroilla käytyihin keskusteluihin sekä kierroilla käytössä oleviin siirreltäviin kiertokärryihin! Työasemia ei tule jättää lukitsematta poistuttaessa työpisteeltä!
- Vastaanottojen odotustiloissa kannattaa kiinnittää huomiota potilaiden yksityisyyden suojaan, mm. kutsuttaessa potilas vastaanottohuoneeseen tai mikäli potilaalle annetaan hoito-ohjeita suullisesti vielä vastaanottohuoneesta poistumisen jälkeen!
- Potilastietojärjestelmästä kannattaa tulostaa potilasasiakirjoja vain harkiten! Tulosteet ja asiakirjojen manuaalinen käsittely on merkittävä riski potilaiden tietosuojan ja salassa pidettävien terveystietojen näkökulmasta. Tulosteita tulee käsitellä huolellisesti ja tulostaa kannattaa lähtökohtaisesti vain ne asiakirjat, joiden tulostamiselle on todellinen tarve! Tarpeettomat tulosteet tulee hävittää tietoturvallisesti tietosuojajätteenä!
- Potilaan tiedot tulee hakea aina tietojärjestelmästä potilaan henkilötunnuksella, jolloin voidaan varmistua siitä, että avataan oikean henkilön tiedot. Mikäli huomataan, että tietojärjestelmästä on avattu erheellisesti väärän potilaan tiedot, virhekäynnistä ei tule tehdä merkintää potilastietoihin! Esimerkiksi Mediatrissa em. virhekäynti merkitään tietojen käytön perusteluksi *Palvelutapahtuma*-riville, josta valitaan *Potilastietojen käytön peruste (Muu erityinen syy > 99 Muu syy > kirjoita ”Virhekäynti”*). Huomioithan, että virhekäyntien merkitsemisessä voi olla tietojärjestelmäkohtaisia eroja, järjestelmien pääkäyttäjät ohjaavat ja neuvovat tarvittaessa merkinnän tekemisessä!

8.4 Potilastietojen kirjaaminen

Potilastietojen laadukas kirjaaminen ja niiden lainmukainen käsittely kuuluvat olennaisena osana potilaalle annettavaan hyvään palveluun ja hoitoon. Oikeus lainmukaisiin kirjauksiin on myös terveydenhuollon potilaille lainsäädännössä turvattu perusoikeus. Lisäksi Siun soten työntekijöiden oman oikeusturvan kannalta on tärkeää tuntea tietosuojalainsäädäntö, kuten myös terveydenhuollon potilastietojen käsittelyä koskeva kansallinen sääntely.

Potilastietoihin tulee kirjata potilaan hoidon järjestämisen, suunnittelun, toteuttamisen ja seurannan turvaamiseksi tarpeelliset sekä laajuudeltaan riittävät tiedot. Kirjausten tulee olla selkeitä sekä ymmärrettäviä. Mikäli kirjattu tieto ei perustu ammattihenkilön omaan tutkimushavaintoon, tulee aina kirjata tiedon lähde. Lausunnot ja todistukset, jotka esitetään muulle organisaatiolle tai taholle, tulee varustaa laatijan allekirjoituksella. Potilastietojen, kuten käyntikirjauksien, lähetteiden ja loppuyhteenveden kirjaaminen tulee tehdä viiveettä, kuitenkin viiden vuorokauden kuluessa siitä, kun potilaan palvelutapahtuma on päättynyt.

Potilastietoja saavat kirjata potilaan hoitoon osallistuvat terveydenhuollon ammattihenkilöt ja heidän ohjeidensa mukaisesti myös muut henkilöt, siltä osin kuin he potilaan hoitoon osallistuvat. Terveydenhuollon opiskelijat saavat tehdä potilaan hoitoon osallistuessaan kirjauksia, kun he toimivat laillisen ammattihenkilön tehtävässä työsuhteessa. Terveydenhuollon opiskelijan ollessa työharjoittelussa, tulee hänen tekemät kirjaukset hyväksyä hänen ohjaajansa, esihenkilönsä tai tämän valtuuttama henkilön toimesta.

Tietosuojavastaavan vinkit!

- Jo terveydenhuollon potilastietoja kirjatessa on hyvä pitää mielessä, että potilaalla on oikeus saada nähdä itseään koskevat tiedot, saada niistä jäljennökset sekä vaatia tietojen korjaamista tarvittaessa!
- **Lukuvinkki:** THL on julkaissut Potilastiedon kirjaamisen yleisoppaan [72] ja Ensihoidon kirjaamisoppaan[73]
- Muista, että sairaalahoidossa olevasta pitkäaikaispotilaasta on laadittava hoitavan lääkärin toimesta vähintään kolmen kuukauden välein seurantayhteenveto, huolimatta siitä, onko potilaan tilassa tapahtunut oleellista muutosta.
- Mikäli potilaan itsemääräämisoikeutta joudutaan perustellusta syystä rajoittamaan, on rajoittamisesta tehtävä aina merkintä potilastietoihin. Merkinnöistä tulee käydä ilmi rajoittamistoimenpiteen syy, luonne ja kesto sekä arvio toimenpiteen vaikutuksesta potilaan

[72] THL - Potilastiedon kirjaamisen yleisopas (versio 5.0.)
[73] THL - Kirjaamisopas: Ensihoito

hoitoon. Myös toimenpiteen määrännen lääkärin ja toimenpiteen suorittajien nimet on merkittävä potilastietoihin.

- Puhelinneuvotteluista ja konsultaatioista on tehtävä merkintä potilastietoihin, mikäli se on potilaan hoidon tai taudinmäärityksen kannalta merkittävä. Mikäli konsultoiva lääkäri saa potilaan tunnistetietoja, myös hänen on merkittävä antamansa vastaus potilasasiakirjoihin tai hänelle on jäätävä antamansa vastauksen tiedot.
- Mediatrin ajanvarauskirjaan voi tulosyyn kirjata, jos sille löytyy toiminnan luonteen kannalta perusteet. Arkaluontoisen tiedon osalta tulosyy kirjataan ikään kuin viittauksena toiseen lähteeseen (esim. ”katso HOI-PTH).

8.4.1 Potilastietojen kopiointi

Potilastietojen kopiointi kertomuslomakkeelta toiselle on lähtökohtaisesti kielletty. Potilastietojen kopiointi voi sisältää riskejä esimerkiksi asiakirjojen eheyden, muuttumattomuuden ja kiistämättömyyden näkökulmassa. Mikäli esimerkiksi alkuperäisessä tekstissä havaittaisiin myöhemmin asiavirhe, on tieto voinut kopioitua eteenpäin ja kopioinnin vuoksi asiavirheitä voi olla mahdotonta jäljittää ja korjata luotettavasti. Osittain potilastietojen kopioinnin tarve on vähentynyt potilastietojen rakenteisuuden myötä.

Käytössä olevista potilastietojärjestelmistä riippuen, potilastietojen kopiointia on mahdollista teknisin toimenpitein estää tai rajoittaa. Järjestelmät voivat sisältää myös sellaisia toimintoja tai tietokenttiä, joiden osalta tietojärjestelmän käyttäjien tulee noudattaa erityistä huolellisuutta ja vältettävä tietojen kopiointia. Esimerkiksi Mediatrissa ns. ydintieto-otsikoiden (mm. diagnoosi, käyntisyy, fysiologiset mittaukset) kopiointi on kielletty, sillä ko. tietoja kopioitaessa otsikoiden rakenne ei kopioidu mukana ja tästä syystä kirjaus ei arkistoituisi oikein ja diagnoosin ja kertomuksen linkitys voi vääristyä.

Joissakin tilanteissa potilastietojen kopiointi on perusteltua, huomioiden kuitenkin turvallisen tietojen käsittelytavan ja menetelmät. Kopiointi on esimerkiksi sallittua niissä tilanteissa, kun lääkärin sanelun pohjalta kirjataan saman sisältöinen lausunto tai todistus sanelusta muodostuvan potilastietomerkinnän lisäksi. Tällöin saneluja purkavilla sihteereillä on oikeus kopioida potilastietomerkintä lausuntoon tai todistukseen. Kopioitaessa tietoja tulee kuitenkin varmistua siitä, että tieto säilyy eheänä, varmistaen tiedon alkuperäisen muodon.

8.5 Potilastietoihin kuulumattomat tiedot

Kaikki terveydenhuollossa käsiteltävä tieto ei kuulu osaksi terveydenhuollon potilasrekisteriä. Potilastietoihin kirjataan lähtökohtaisesti vain potilaan tutkimuksen ja hoidon kannalta tarpeelliset ja välttämättömät tiedot. Potilaan potilastietoihin eivät kuulu mm. seuraavat tiedot:

- muistutusten ja kanteluiden käsittely
- potilaslaskutukseen liittyvät asiakirjat
- tilastot, tutkimusluvat tai terveydenhuollon toiminnan kehittämiseksi laaditut selvitykset
- hyvinvointialueen verkkosivujen kautta saatu asiakaspalaute

- EU:n tietosuoja-asetuksen mukaiset rekisteröidyn oikeuksiin liittyvät pyynnöt
- lokivalvonta
- potilasturvallisuusilmoitukset (Laatuportti)
- ammattilaisen toimesta tehty virheellinen tietojen käsittely (mm. väärän potilaan tietojen avaaminen vahingossa).

Tietosuojavastaavan vinkit!

- Potilastietoihin kuulumattomia lausuntoja tai selvityksiä ei lähtökohtaisesti käsitellä potilastietojärjestelmissä!
- Mikäli on tarpeen laatia sanelemalla selvitys tai lausunto esimerkiksi potilasvahingosta, muistutuksesta tai kantelusta, Mediatrissa tulee käyttää ns. *Hallinnollista sanelua*. Tällöin potilasasiakirjoihin kuulumatonta tietoa ei tallennu osaksi potilastietoja! Tutustu hallinnollisten sanelujen saneluohjeeseen[74] sekä ko. sanelujen purkuohjeeseen Siun soten intrassa[75]! Em. ohjeisiin huolellinen perehtyminen on tärkeää, sillä hallinnollisten sanelujen prosessi sisältää monta käyttäjän muistettavaa ja huolehdittavaa asiaa, jotta sanelu ja sen purku tapahtuvat tietoturvallisesti!

8.6 Potilastietojen hankkiminen ja pyytäminen

Lähtökohtaisesti terveydenhuollon potilaan tiedot saadaan potilaalta itseltään. Tietoja voidaan hankkia ja pyytää myös muilta tahoilta tarvittaessa. Tietojen hankkiminen ja pyytäminen tapahtuu lähtökohtaisesti kuitenkin aina potilaan tai tämän laillisen edustajan antamalla suostumuksella. Mikäli potilas on kykenemätön vastaamaan omasta huolenpidostaan, terveydestään ja turvallisuudestaan, ja läheisverkoston tiedot ovat välttämättömiä hoidon tarpeen selvittämiseksi tai kun tiedot ovat tarpeen alaikäisen lapsen edun vuoksi, tiedonsaantioikeutta tulee tarkastella terveydenhuollon lainsäädännöstä.

Tietosuojavastaavan vinkit!

- Muista, että tietojen hankkiminen ja pyytäminen tulee perustua potilaan hoitoon liittyviin tarpeisiin. Pohdi siis hankittavien tietojen tarpeellisuutta, sillä potilaan hoidon kannalta tarpeettomia tietoja ei tule kerätä.
- Potilastietoihin kuulumattomia lausuntoja tai selvityksiä ei lähtökohtaisesti käsitellä potilastietojärjestelmissä!

[74] Meita – Hallinnollisten sanelujen sanelu
[75] Meita – Hallinnollisten sanelujen purku

- Tutustu tietopyyntöihin liittyviin ohjeistuksiin[76]!

8.7 Potilastietojen luovuttaminen

Terveydenhuollon potilastietoja voidaan luovuttaa, jos tietojen luovuttamiselle on potilaan antama suostumus tai siihen on oikeutus lainsäädännön nojalla. Mikäli tietojen luovutus perustuu potilaan suostumukseen, tulee suostumuksen olla vapaaehtoinen, yksilöity ja tietoinen tahdonilmaus. Suostumuksessa tulee ilmetä mm. mitä tietoja luovutus koskee, kenelle tietoja luovutetaan ja mitä käyttötarkoitusta varten. Suostumusperusteisessa tietojen luovuttamisessa tulee aina huomioida, että potilas voi perua myöhemmin antamansa suostumuksen.

Jos potilaalla ei ole edellytyksiä arvioida annettavan suostumuksen merkitystä, tietoja voidaan luovuttaa asiakkaan laillisen edustajan antamalla suostumuksella. Alaikäisen lapsen laillinen edustaja on pääsääntöisesti hänen huoltajansa. Huoltaja ei kuitenkaan voi antaa suostumusta lapsen puolesta siinä tilanteessa, jos hänellä itsellään ei ole oikeutta tiedonsaantiin. Edunvalvojien ja edunvalvontavaltuutettujen toimivalta puolestaan määräytyy heidän tehtävänsä mukaisesti.

Mikäli potilas ei itse kykene antamaan suostumusta tietojen luovuttamiseen, eikä hänellä ole laillista edustajaa, tietoja ei voi luovuttaa perustuen suostumukseen. Tällaisissa tilanteissa luovuttaminen on mahdollista vain, jos jokin lainsäännös siihen oikeuttaa. Yksityiskohtaiset tietojen luovuttamisen edellytykset tulee katsoa asianomaisesta lainsäädännöstä (mm. potilaslaki, asiakastietolaki, rikoslaki, julkisuuslaki).

Kaikki tietojen luovutukset tulee merkitä asianmukaisin tiedoin, perustuipa tietojen luovutus suostumukseen tai lainsäädäntöön. Suostumukset tulee myös arkistoida. Myös potilaan ilmoittamat tietojen luovutus- tai hankkimiskiellot tulee merkitä asiakastietoihin.

Tietosuojavastaavan vinkit!

- Huomioi, että potilaan laillinen edustaja ei voi tehdä tietojen luovutuskieltoa potilaan puolesta eikä perua potilaan aiemmin antamaa suostumusta tietojen luovuttamiseen.
- Tutustu asiakas- tai potilasrekisterin tallennettujen tietojen luovuttaminen ohjeeseen Siun soten intrassa[77] ja Tiedonhallinnan intra-sivuun[78].

[76] Siun sote – Tietojen luovuttaminen ja tietopyynnöt (Siun sote intra)
[77] Siun sote - Toimintaohje: Asiakas- ja potilasrekisteriin tallennetun tiedon luovuttaminen ja tarkastaminen (Siun sote intra)
[78] Siun sote - Tietojen luovuttaminen ja tietopyynnöt (Siun sote intra)

8.7.1 Alaikäinen henkilö terveydenhuollon palveluissa

Terveydenhuollon palveluissa tulee selvittää alaikäisen lapsen ja nuoren mielipide hoitoonsa aina, kun se hänen ikäänsä ja kehitystasoonsa nähden on mahdollista. On tärkeää, että lapsi ja nuori saa sanoa oman mielipiteensä ja näkemyksensä sekä esittää kysymyksiä silloinkin, kun hän ei vielä voi itse päättää hoitoon liittyvistä asioistaan. Terveydenhuollon ammattilaisilla on velvollisuus informoida alaikäistä hänen oikeuksistaan.

Kun alaikäinen ei kykene päättämään hoidostaan, hoidetaan häntä yhteistyössä vanhempien, muun huoltajan tai muun laillisen edustajan kanssa. Lapsen tai nuoren ollessa yhdessä vanhemman kanssa vastaanotolla, tulee ammattilaisen arvioida lapsen kykyä tehdä päätöksiä erityisesti silloin, kun vanhempi ja lapsi ovat eri mieltä hoidosta. Yleensä se edellyttää ammattilaisen ja lapsen keskustelua kahden kesken, eli silloin vanhempaa pyydetään poistumaan vastaanottohuoneesta kahdenkeskisen keskustelun ajaksi.

Alaikäinen voi päättää hoidostaan silloin, kun terveydenhuollon ammattihenkilö arvioi, että hän ikänsä ja kehitystasonsa perusteella on kykenevä asian vaatimaan päätöksentekoon. Laki ei tunne mitään päätöskykyisyyden ikärajaa, vaan ammattilainen tekee arvion aina tapauskohtaisesti huomioiden asian laadun. Silloin, kun lapsi tai nuori arvioidaan kykeneväksi käyttämään itsemääräämisoikeuttaan, saa hän päättää myös yhteydenotosta ja tietojen antamisesta vanhemmille, muulle huoltajalle tai muulle lailliselle edustajalle. Velvoitteena on tarjota lapselle ja nuorelle terveydenhuollon ammattilaisen hoitoa ja tukea silloinkin, kun hän ei halua asiaa jostakin syystä vanhemmilleen jakaa. Tällöin voi olla hedelmällistä avata keskustelu lapsen tai nuoren suhteesta vanhempiinsa: voi kysyä miksi hän ei halua asiaa vanhemman tietoon tai mitä hän ajattelee tapahtuvan, jos vanhempi saa tietää jostakin terveyteen liittyvästä asiasta.

Terveydenhuollon palveluissa on ajoittain myös tilanteita, joissa lapsi on lastensuojelulain (417/2007) mukaisesti huostaanotettuna ja hänen huoltonsa on vanhempien sijaan annettu sijaisvanhemmille perhehoitolain (263/2015) nojalla. Näissä tilanteissa lapselle on määrätty lapsen asioista vastaava sosiaalityöntekijä, jonka vastuulla on ensisijaisesti vastata lapsen hoitoon ja huoltoon liittyvistä asioista ja jolla on asiakaslain mukainen tiedonsaantioikeus lapsen terveydentilaan liittyvistä asioista. Vastaavan sosiaalityöntekijän vastuulla on myös antaa tietoja lapsesta tarvittaville yhteistyötahoille (mm. koulu, päiväkoti ja sijaisvanhemmat), mikäli he tietoja tarvitsevat. Terveydenhuollon ammattilaisten tulee huolehtia siitä, että vastaavan sosiaalityöntekijän kanssa on sovittu tietojen luovutuksesta ja luovutusmerkinnät tehdään lapsen potilastietoihin. Sijaisvanhemmilla ei siis ole oikeutta kuin lapsen hoidon ja huollon kannalta välttämättömiin lapsen terveyttä koskeviin tietoihin. Heillä ei ole myöskään oikeutta allekirjoittaa tietojen luovutuksiin liittyviä suostumuksia. Näissäkin tilanteissa lapsen päätöskyky arvioidaan edellä kuvatun mukaisesti. Mikäli lapsi ei kykene päättämään hoidostaan, sijaisvanhempien tulee olla yhteydessä vastaavaan sosiaalityöntekijään, joka pyytää tarvittavat lapseen liittyvät terveystiedot. On lisäksi huomioitava, että lapsen huoltajalla on tiedonsaantioikeus lapsen terveyttä koskeviin tietoihin. Huoltajan tiedonsaantioikeutta lapsi voi rajoittaa päätöskykyarvioon perustuen, mikäli lapsi on todettu päätöskykyiseksi ja hän päättäisi kieltää tietojen luovutuksen huoltajalle.

Tietosuojavastaavan vinkit!

- On hyvä huomioida, että hoidolla tarkoitetaan myös terveyden edistämiseen liittyvä toimintaa.

- Alaikäinen henkilö voi päättää hoidostaan silloin, kun terveydenhuollon ammattihenkilö arvioi, että hän ikänsä ja kehitystasonsa perusteella on kykenevä asian vaatimaan päätöksentekoon. Laki ei siis tunne mitään päätöskykyisyyden ikärajaa, vaan ammattilainen tekee arvion aina tapauskohtaisesti huomioiden asian laadun.
- Alaikäisen päätöskykyyn liittyvät merkinnät tulee tehdä potilastietojärjestelmään!
- **Lukuvinkki:** THL Alaikäisen itsenäisen päätöskyvyn arviointi terveydenhuollossa[79]. Tutustu lisäksi Siun soten intrasta löytyvään materiaaliin[80] aiheeseen liittyen!

8.8 Potilastietojen korjaaminen

Rekisterinpitäjän on oma-aloitteisesti oikaistava, poistettava tai täydennettävä rekisterissään oleva, käsittelytarkoituksen kannalta virheellinen, tarpeeton, puutteellinen tai vanhentunut tieto. Virheellisen tiedon korjaaminen tulee tehdä läpinäkyvästi ja ohjeiden mukaisesti. Myös potilaalla on oikeus pyytää virheellisten rekisteritietojen korjaamista.

Rekisterinpitäjä päättää aina tiedon korjaamisesta. Mikäli korjauspyynnöstä kieltäydytään, potilaalle on annettava perusteltu kieltäytymistodistus. Tällöin potilaalla on oikeus pyytää asiaan tietosuojavaltuutetun kannanottoa. Huomioitavaa on, ettei tietosuojavaltuutetun toimivaltaan kuulu arvioida lääketieteellisen arvion oikeellisuutta ja tästä syystä tietosuojavaltuutettu ei voi määrätä esimerkiksi diagnoositietoja korjattavaksi. Tietosuojavaltuutettu ei voi myöskään määrätä oikaistavaksi potilastietoihin merkittyä lääketieteellistä arviota muualta saadun lääkärinlausunnon perusteella.

Mikäli potilaan esittämään korjauspyyntöön suostutaan, rekisterinpitäjä ryhtyy tarvittaviin toimenpiteisiin. Potilastietojen korjaamisessa on huomioitava, että alkuperäiset tiedot tulee olla kuitenkin jälkikäteen löydettävissä. Korjauksesta on käytävä ilmi korjauksen tekijän nimi, työtehtävä, korjauksen ajankohta ja peruste tietojen korjaamiselle.

Tietosuojavastaavan vinkit!

- Huomioithan, että esimerkiksi virheellisesti väärälle potilaalle Mediatri-potilastietojärjestelmässä tehdystä ajanvarauksesta muodostuu palvelutapahtumaa, jota ammattilainen ei voi poistaa järjestelmästä itse. Korjauspyyntö asiasta on osoitettava Siun soteen nimetyille tekstinkorjaajille, jolloin voidaan varmistaa, että henkilön tietoihin ei jää virheellisiä palvelutapahtumia taustalle, jotka näkyisivät myös henkilölle itselleen OmaKanta-palvelussa!

[79] THL – Alaikäisen itsenäisen päätöskyvyn arviointi terveydenhuollossa
[80] Siun sote - Alaikäisen itsenäisen päätöskyvyn arviointi ja puolesta-asiointi (Siun sote intra)

- Muistathan osoittaa korjauspyynnöt nimetyille tekstinkorjaajille aina suojatulla sähköpostilla (korjaukset@siunsote.fi.s)!
- Huolehdithan, että laadit korjauspyynnön tekstinkorjaajille aina riittävillä tiedoilla! Pyynnössä tulee olla mainittuna mm. seuraavat asiat: potilasnumero, Mediatri-kanta (ESH/PTH/SOS), Mediatri-yksikkö, lomake, jossa poistettava tieto on, kirjauksen pääotsikko, kirjauksen päivämäärä ja kellonaika. Lisäksi pyyntöön tulee kirjata, kuka on kirjannut tekstin (Mediatri-käyttäjätunnus), poistosyy, pyytäjän yhteystiedot (nimi ja puhelinnumero). Lisäksi on hyvä kirjoittaa muut mahdolliset tiedot, esim. kuvapankkiin siirretyt kuvat.
- Muista, että saat lisätietoja eri tietojärjestelmien korjauspyynnöistä ja niiden käsittelystä aina tietojärjestelmien pääkäyttäjiltä!

8.9 Potilastietojen säilyttäminen ja hävittäminen

Siun sote vastaa rekisterinpitäjänä potilastietojen säilyttämisestä ja niiden asianmukaisesta hävittämisestä, mikäli niille määritelty säilytysaika päättyy tai tiedoilla ei ole arkistointivelvoitetta. Terveydenhuollon potilastietojen säilytysajat on määritelty terveydenhuollon lainsäädännössä. Kanta-palvelujen terveydenhuollon potilastiedon arkiston säilytyksestä vastaa Kela. Arkistolaitos määrää lisäksi arkistolain nojalla joidenkin asiakirjojen säilytyksestä

Tietosuojavastaavan vinkit!

- Perehdy Terveydenhuollon asiakirjojen arkistointi ja käsittelyohjeeseen Siun soten intrassa[81]!
- Lue lisää asiakirjojen säilytysajoista ja arkistoinnista Siun soten intrasta[82]!

9 Työntekijöiden henkilötietojen käsittely

Työntekijöiden henkilötietojen käsittelyyn sovelletaan työelämän tietosuojalakia eli laki yksityisyyden suojasta työelämässä (754/2004). Laki koskee yksityiselämän suojaa työntekijän ja työnantajan välisessä suhteessa. Lain soveltamisalaan kuuluvat mm. työsuhteiset työntekijät, virkasuhteiset virkamiehet ja viranhaltijat sekä soveltuvin osin myös työnhakijat ja virkaa hakevat.

Työntekijän henkilötietoja tulee käsitellä tietosuojaperiaatteiden mukaisesti ja työnantajan on toteutettava asianmukaiset toimenpiteet työntekijöiden tietosuojaoikeuksien toteutumiseksi. Työelämän henkilötietojen käsittelytilanteet ovat useimmiten lakisääteistä, joka vaikuttaa siihen, mitä tietosuoja-asetuksen mukaisia

[81] Siun sote - Terveydenhuollon asiakirjojen käsittely ja arkistointi (Siun sote intra)
[82] Siun sote – Säilytysajat ja arkistointi (Siun sote intra)

oikeuksia työntekijällä on. Työnantaja saa kuitenkin käsitellä vain välittömästi työntekijän työsuhteen kannalta tarpeellisia henkilötietoja, jotka liittyvät työsuhteen osapuolten oikeuksien ja velvollisuuksien hoitamiseen, työnantajan työntekijälle tarjoamiin etuuksiin tai jotka johtuvat työtehtävien erityisluonteesta. Tarpeellisuusvaatimuksesta ei voida poiketa työntekijän suostumuksella.

Lähtökohtaisesti työnantajan on kerättävä työntekijää koskevat henkilötiedot työntekijältä itseltään. Poikkeuksia tähän ovat mm. turvallisuusselvitykset (turvallisuusselvityslaki 726/2014), alaikäisten kassa työskentelevien henkilöiden rikostaustan selvittäminen (laki lasten kanssa työskentelevien rikostaustan selvittämisestä 504/2002) ja oikeus saada tietoja rikosrekisteristä (rikosrekisterilaki 779/1993). Mikäli työnantaja kerää henkilötietoja em. tarkoituksiin, tulee työntekijälle ilmoittaa etukäteen häntä koskevien tietojen hankkimisesta luotettavuuden selvittämistä varten.

Tietosuojavastaavan vinkit!

- Tutustu Työ- ja elinkeinoministeriön laatimaan esitteen työelämän tietosuojalaista[83] ja tietosuojavaltuutetun toimiston julkaisemaan työelämän tietosuojan käsikirjaan[84].
- Työnantaja ei saa ilmaista sivulliselle tietoja työntekijästä (mm. henkilöstöhallinnon tiedot). Sivulliseksi katsotaan myös ne työnantajan palveluksessa olevat muut työntekijät, joilla ei ole työtehtäviensä mukaista käsittelyoikeutta kyseisiin tietoihin.

9.1 Yhteistoimintamenettely

Työelämän tietosuojaan kuuluu vahvana osana yhteistoimintamenettely, jonka taustalla on laki työnantajan ja henkilöstön välisestä yhteistoiminnasta kunnassa ja hyvinvointialueella (449/2007). Siun sotessa Yhteistyötoimikunta[85] vastaa yhteistoimintajärjestelmästä ja seuraa yhteistoiminnan toteutumista. Yhteistoimintamenettelyssä käsitellään työelämän tietosuojaan liittyen mm. työntekijöiden henkilötietojen keräämistä työpaikalla sekä henkilötietojen käsittelyn valvontaa. Yhteistoimintamenettelyssä käsitellään lisäksi työntekijöihin kohdistuva tekninen valvonta.

Työntekijöihin liittyvistä henkilötietojen käsittelyistä tulee informoida työntekijöitä mm. toimintayksikön, palvelualueen ja toimialueen kokouksissa sekä kirjallisesti tietosuojaselosteilla. Tietosuojaselosteet ovat saatavilla Siun soten intrasta. Tietosuojaselosteiden laadinnasta, ajantasaisuudesta ja ylläpidosta vastaavat käsittelytoimien

[83] TEM – Työelämän tietosuojalaki
[84] Tietosuojavaltuutetun toimisto – Työelämän tietosuojan käsikirja
[85] Siun sote – Yhteistyötoimikunta (Siun sote intra)

vastuuhenkilöt ja/tai Siun soten henkilöstöjohtaja, joka toimii henkilöstöhallinnon tietovarannon rekisterinpitäjän edustajana.

Tietosuojavastaavan vinkit!

- Yhteistyömenettelyssä on sovittava myös siitä, mitkä työntekijöihin liittyvät henkilötiedot voidaan julkaista hyvinvointialueen verkkosivuilla tai sisäiseen käyttöön tarkoitetussa intrassa.
- Tutustu ilmoittajan suojelulain (1171/2022) mukaiseen Whistleblowing-ilmoituskanavaan Siun soten intrasta[86] tai tietosuojavaltuutetun toimiston oppaasta[87].

9.2 Oikeus käsitellä työntekijän henkilötietoja

Työnantajan on määriteltävä ne henkilöt, jotka työtehtäviensä perusteella saavat käsitellä työntekijöiden henkilötietoja. Käsittelyssä tulee huomioida työtehtävän lisäksi käsiteltävien tietojen laajuus.

9.3 Terveydentilaan liittyvien tietojen käsittely

Työntekijän terveydentilaan liittyvät tiedot ovat erityisiin henkilötietoryhmiin kuuluvia, arkaluonteisia ja salassa pidettäviä henkilötietoja. Myös näiden osalta työnantajan on määriteltävä ne henkilöt, joilla on työtehtäviensä perusteella oikeus käsitellä työntekijän terveydentilaan liittyviä tietoja. Terveydentilaa koskevia tietoja saavat käsitellä mm. henkilöt, jotka tietojen perusteella valmistelevat tai tekevät palvelussuhdetta koskevia päätöksiä tai laittavat niitä toimeen.

Työntekijän terveydentilaan liittyvien tietojen käsittely voi olla työnantajalle oikeutettua esimerkiksi työturvallisuuslain (738/2022) tai työterveyshuoltolain (1383/2001) perusteella. Hyväksyttävää käsittelyä voivat olla myös mm. sairausajan palkan maksaminen tai poissaolosyyn selvittäminen, tilanne, jossa työn tekeminen aiheuttaa sairastumisen vaaraa tai tilanne, jolloin työntekijä haluaa selvittää työkykyisyyttään. Työntekijöiden terveydentilaan liittyvistä tiedoista ei saa pitää työpaikalla rekisteriä. Rekisterinpito on sallittua vain terveydenhuollon toimijalla, kuten esimerkiksi työterveyshuollolla.

Tietosuojavastaavan vinkit!

- Työnantajalla ei ole yleistä oikeutta kertoa, muulla tavoin ilmaista tai luovuttaa työntekijää koskevaa sairauspoissaoloa tai sen syytä muille työntekijöille tai sivullisille. Mikäli työntekijän sairauspoissaololla on vaikutusta työyksikön muuhun toimintaan, sairauspoissaolosta tiedotetaan

[86] Siun sote – Ilmoittajan suojelu (Siun sote intra)
[87] Tietosuojavaltuutetun toimisto – Työelämän tietosuoja ns. Whistleblowing-ilmiantojärjestelmässä

ilmoittamalla ainoastaan henkilön olevan ”poissa”. Työntekijää ei voi velvoittaa ilmoittamaan nimenomaisesti sairauspoissaolosta esimerkiksi sähköpostin automaattisessa poissaoloviestissä. Poissaoloviestiin työntekijä voi ilmaista olevansa poissa, samoin kuten loma-aikoina.

- Työterveyshuollon käsittelemät potilastiedot ovat osa työterveyshuollon toimintaa. Työterveyshuollon potilasrekisterissä olevia tietoja voidaan luovuttaa työnantajalle vain työntekijän suostumuksella tai jos laissa on nimenomaisesti säädetty.
- Henkilöstöhallinnon tietojärjestelmiin ei ole sallittua tallentaa tietoja työntekijän sairauden tai vamman syytä osaksi työntekijän muita tietoja.
- Työkykyneuvottelujen kirjalliset raportit ja yhteenvedot muodostavat osan henkilöstöhallinnon rekisterinpitoa. Työkykyneuvotteluissa on suositeltavaa keskittyä työntekijän työkykyyn ja työjärjestelyihin liittyviin asioihin.

9.4 Henkilö- ja soveltuvuusarviointitestit

Työntekijää voidaan suostumukseen perustuen testata henkilö- ja soveltuvuusarvioinnein työtehtävien hoidon edellytysten tai koulutus- ja muun ammatillisen kehittämisen tarpeen selvittämiseksi. Työnantajan on varmistettava, että testeissä käytetään luotettavia testausmenetelmiä, niiden suorittajat ovat asiantuntevia ja testauksella saatavat tiedot virheettömiä.

Tietosuojavastaavan vinkit!

- Henkilö- ja soveltuvuusarvioinnit ovat mm. julkisuuslain mukaan salassa pidettäviä.
- Arviointeja koskee henkilötietojen suojaamisvelvoite ja vaitiolovelvollisuus.
- Työnantajan on annettava työntekijälle pyynnöstä henkilö- tai soveltuvuusarvioinnista laadittu kirjallinen lausunto. Jos lausunto on annettu työnantajalle suullisena, työntekijän tulee saada selvitys annetun lausunnon sisällöstä.

9.5 Tekninen valvonta, sähköpostit ja tietoverkot

Teknisellä valvonnalla tarkoitetaan mm. työntekijöihin kohdistuvaa kameravalvontaa, kulunvalvontaa ja muita teknisin menetelmin toteutettuja valvontoja. Valvontaa voidaan kohdistaa myös sähköpostiin sekä tietoverkon käyttöön. Valvontaan liittyvät asiat kuuluvat yhteistoimintamenettelyn piiriin.

Yhteistoimintamenettelyn lisäksi työnantajan on määriteltävä työntekijöihin kohdistuvan teknisen valvonnan käyttötarkoitus, siinä käytettävät menetelmät sekä tiedotettava työntekijöille valvonnan tarkoituksesta, käyttöönotosta ja siinä käytettävistä menetelmistä. Valvontaa voidaan käyttää, mikäli työnantaja haluaa valmistaa työntekijöiden ja muiden työnantajan tiloissa olevien henkilöiden turvallisuuden, suojata omaisuutta tai varmistaa em. vaarantavien tilanteiden ennalta estämisen tai selvittämisen. Siun sotessa valvontaa toteutetaan mm.

tallentavalla kameravalvontajärjestelmällä[88], lääkehuoneiden kameravalvonnalla[89] ja kulunvalvonnalla[90]. Kameravalvontaa voidaan käyttää turvallisuuden varmistamiseksi, omaisuuden suojaamiseksi tai tuotannon asianmukaisen toiminnan valvomiseksi ja niitä vaarantavien tilanteiden ennaltaehkäisemiseksi tai selvittämiseksi.

Viestinnän luottamuksellisuudesta säädetään Suomen perustuslaissa, jonka mukaan kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus on loukkaamaton. Työntekijän sähköpostiosoite, joka on esimerkiksi muotoa etunimi.sukunimi@siunsote.fi ja siihen tulleet henkilökohtaiset sähköpostit kuuluvat luottamuksellisen viestinnän piiriin. Työnantajalla on oikeus hakea esille ja avata työnantajalle kuuluvat sähköpostiviestit (saapuneet sekä lähetetyt). Sähköpostin avaamisen suorittaa Meita. Viesteihin kohdistuneet toimenpiteet tulee kirjata avauspöytäkirjaan ja avaukseen osallistuneita henkilöitä sitoo vaitiolovelvollisuus. Sähköpostien avaamisesta tulee antaa kirjallinen selvitys työntekijälle, jossa ilmenee perusteet viestien esiin hakemiselle ja ketkä sen ovat suorittaneet ja milloin.

Työnantajalla on oikeus määrittää mihin työaikaa käytetään. Työnantaja voi kieltää mm. henkilökohtaisen puhelimen käyttämisen tai verkkosivujen selaamisen (ns. verkkosurffailun) työajalla. Työnantajalla on oikeus myös määrittää omistamiensa laitteiden, kuten työpuhelinten ja työtietokoneiden käytöstä. Kyseessä voi olla tietoturvaan tai tietosuojaan liittyvä rajoitus tai työnjohdollinen linjaus.

Tietosuojavastaavan vinkit!

- Työnantaja ei voi kohdentaa teknistä valvontaa työntekijän tai tiettyjen työntekijöiden tarkkailuun työpaikalla tai heidän työoikeudellisten velvoitteiden valvontaan mm. työajan noudattamiseen.
- Työnantaja ei voi kohdentaa kameravalvontaa henkilöstö- ja sosiaalitiloihin, henkilökohtaiseen työhuoneeseen, pukeutumistilaan tai käymälään (WC).
- Kameravalvontaa voidaan kohdentaa tiettyyn työpisteeseen, mikäli se on välttämätöntä mm. työntekijään kohdistuvan väkivallan, turvallisuuden tai terveyden uhan vuoksi.
- Mikäli esihenkilöllä on tarve hakea esille tai avata työnantajalle kuuluvat sähköpostiviestit työntekijän henkilökohtaisesta työsähköpostista, tulee esihenkilön varmistua siitä, että lainmukaiset edellytykset täyttyvät. Tarvittaessa esihenkilö konsultoi asiassa turvallisuuspäällikköä tai tietosuojavastaavia.

[88] Siun sote – Tietosuojaseloste: Tallentava kameravalvontajärjestelmä (Siun sote intra)
[89] Siun sote – Tietosuojaseloste: Hyvinvointialueen lääkehuoneiden kameravalvonta (Siun sote intra)
[90] Siun sote – Tietosuojaseloste: Kulunvalvonta ja avaintenhallinta (Siun sote intra)

- Mikäli työntekijä saa sähköpostin, joka ei ole hänelle tarkoitettu, hän ei saa ilman lähettäjän suostumusta ilmaista tai käyttää hyväksi viestin sisältöä, välitystietoa tai tietoa viestin olemassaolosta, ellei laissa toisin säädetä.

9.6 Paikantaminen

Työntekijän paikantamista voidaan pitää teknisin menetelmin tapahtuvana valvontana, jonka käyttöönotto kuuluu yhteistoimintamenettelyn piiriin. Työntekijän paikantaminen voi olla välitöntä tai välillistä. Välittömällä paikantamisella tarkoitetaan tietyn työntekijän paikantamista ja seuraamista (mm. työntekijälle annettu erillinen paikannuslaite tai paikannus toteutetaan työntekijän käytössä olevan älypuhelimen avulla). Välillisellä paikantamisella tarkoitetaan paikantamista ja seuraamista muun kuin suoraan tietyn työntekijän kohdistetun paikannuslaitteen käyttämällä (mm. työntekijän käyttämä työnantajan ajoneuvo, johon on asennettu paikannuslaite). Tällöin kuitenkin työntekijä voi olla välillisesti tunnistettavissa mm. työvuorolistan perusteella.

Välittömässä työntekijän paikantamisessa pelkästään yhteistyötoimintamenettelyn myötä tapahtuva yleinen informointi ei ole riittävä. Jokaisen työntekijän, joita paikantaminen koskee, tulee olla tietoinen paikannuksen tarkoituksesta ja heidän henkilötietojensa käsittelystä paikantamisen yhteydessä. Tarve paikantaa työntekijä on arvioitava aina työntekijäkohtaisesti. Välittömässä paikannuksessa tulee työntekijän suostumuksen lisäksi huolehtia siitä, että paikannuksen voi kytkeä pois päältä luvallisesti esimerkiksi lakisääteisten taukojen ajaksi tai tilanteissa, jossa työntekijä käyttää työnantajan laitetta (mm. älypuhelin) luvallisesti myös työajan ulkopuolella.

Mikäli paikannustietoa ja työntekijöitä koskevia muita henkilötietoja kerätään ja tallennetaan automaattisen tietojenkäsittelyn avulla ja/tai niistä muodostuu henkilörekisteri, tulevat kaikki tietosuoja-asetuksen velvoitteet huomioitavaksi. Lisäksi työnantajan on nimettävä ne henkilöt, joilla on työntehtävän mukainen oikeus käsitellä työntekijöistä kerättävää paikannustietoa.

Tietosuojavastaavan vinkit!

- Siun sotessa työntekijän paikantamista sisältävästä henkilötietojen käsittelytoimesta tulee aina laatia tietosuojaa koskeva vaikutustenarviointi (DPIA)[91].

9.7 Esityslistat, pöytäkirjat, viranhaltijapäätökset

Siun soten aluevaltuuston, aluehallituksen, aluehallituksen alaisena toimivien jaostojen (henkilöstöjaosto, yksilöasioiden jaosto, ympäristöterveydenhuollon jaosto), lautakuntien ja muiden toimielinten esityslistoilla sekä muistioissa ja viranhaltijapäätöksissä on usein henkilötietoja. Ne liittyvät esimerkiksi asianosaisiin, työntekijöihin,

[91] Siun sote – Tietosuojaa koskeva vaikutustenarviointi (DPIA) (Siun sote intra)

viranhaltijoihin ja muutoksenhakua koskeviin asioihin. Päätöstentekijät, esittelijät ja valmistelijat ovat usein välttämättömiä tietoja. Heidän osaltaan henkilötietojen (mm. nimi ja yhteystiedot) julkaiseminen yleisessä tietoverkossa on pääsääntöisesti aina välttämätöntä. Muiden asianosaisten henkilötietojen julkaisua tulee aina harkita erikseen.

Esityslistat voivat sisältää henkilötietoja ja ne voidaan julkaista yleisessä tietoverkossa silloin kun on kysymys tiedonsaannin kannalta välttämättömistä tiedoista, jotka eivät ole salassa pidettäviä. Pöytäkirjat julkaistaan tarkastuksen jälkeen myös yleisessä tietoverkossa. Pöytäkirjoissa saa julkaista ainoastaan julkiset ja tiedonsaannin kannalta välttämättömät henkilötiedot. Pöytäkirjojen salassa pidettävä tietoaineisto merkitään siten, että pöytäkirjassa julkaistaan ainoastaan maininta salassa pidettävän asian käsittelystä. Mikäli vain osa asian tiedoista on salassa pidettävää, vain tämä asian kohta merkitään kyseisellä maininnalla.

Viranhaltijapäätöksissä voi olla tarpeen mainita mm. viranhaltijan nimi, ammatti sekä koulutusta koskeva tieto. Nämä tiedot voidaan julkaista, mikäli se on välttämätöntä muutoksenhaun kannalta.

Tietosuojavastaavan vinkit!

- Esityslistojen, pöytäkirjojen ja päätösten valmistelijoiden tulee tarkkaan harkita, minkä luonteisia valmisteltavassa asiassa esiintyvät henkilötiedot ovat ja voidaanko ne julkaista.

10 Henkilötietojen käsittelystä sopiminen palveluntuottajan kanssa

Siun soten on rekisterinpitäjänä noudatettava kaikessa henkilötietojen käsittelyssä EU:n yleistä tietosuoja-asetusta, myös hankittaessa palvelua ulkopuoliselta palveluntuottajalta. Palveluntuottajan tulee täyttää tietosuoja-asetuksen asettamat vaatimukset ja henkilötietojen käsittelystä on sovittava sopimuksella tai muulla sitovalla asiakirjalla tietosuoja-asetuksen 28 artiklan mukaisesti, jossa vahvistetaan tietojen käsittelyn tarkoitus, luonne, kohde, kesto, henkilötietojen tyypit ja rekisteröityjen ryhmät sekä rekisterinpitäjän velvollisuudet ja oikeudet.

Henkilötietojen käsittelystä sopimiseen on Siun sotelle laadittu aluehallituksen hyväksymät henkilötietojen käsittelyn ehdot. Ehtoja sovelletaan myös palvelusetelipalvelujen tuottajaksi hakeutuvien palveluntuottajien osalta. Ehtojen liitteenä olevan henkilötietojen käsittelytoimien kuvauksen tarkoituksena on määritellä käsittelytoimet, joita palveluntuottaja henkilötietojen käsittelijänä tekee Siun soten puolesta, hyväksi ja eduksi.

Tietosuojavastaavan vinkit!

- Tutustu Siun soten henkilötietojen käsittelyn ehtoihin[92] sekä niiden liitteenä olevaan käsittelytoimen kuvauslomakkeeseen! Henkilötietojen käsittelyn ehdot ovat aina ensisijainen sopimukseen liitettävä asiakirja, kun Siun sote sopii käsittelystä palveluntuottajan kanssa!
- Lue lisää henkilötietojen käsittelyn ehtojen käytöstä sekä käsittelytoimen kuvaamisesta erillisestä toimintaohjeesta[93] sekä Siun soten intrasta[94]!
- Siun soten sopimuksesta tai palvelun hankkimisesta vastaava henkilö vastaa siitä, että henkilötietojen käsittelystä sovitaan tietosuoja-asetuksen mukaisesti palveluntuottajan kanssa! Huolehdi, että vastuullasi olevissa sopimuksissa ja hankinnoissa tämä on huomioitu hyvissä ajoin ennen sopimuksen allekirjoittamista ja käsittelytoimen alkamista!
- Henkilötietojen käsittelyn ehdot on mainittava sopimuksessa ja/tai sopimuksen liitelistassa!
- Muista, että rekisterinpitäjällä on päätösvalta henkilötietojen käyttämisen ja säilyttämisen suhteen. Palveluntuottajalla (henkilötietojen käsittelijällä) ei itsenäistä päätösvaltaa näihin asioihin ole!
- Huomioithan, että henkilötietojen käsittelijällä ei tarkoiteta rekisterinpitäjän alaisuudessa työskenteleviä työntekijöitä. Esimerkiksi Siun soten työntekijä ei ole tietosuoja-asetuksessa määritelty henkilötietojen käsittelijä!

11 Henkilötietojen käsittely tutkimuksissa

Tietosuojasta huolehtiminen on tieteellisen tutkimuksen menestymisen edellytys. Keskeisintä on suunnitella tutkimukseen kuuluva henkilötietojen käsittely koko tiedon elinkaaren ajalta ennen tutkimuksen aloittamista. Tavoitteena on turvata tutkittavien henkilöiden tietosuoja. Tutkimussuunnitelmassa tulee olla määriteltynä henkilötietojen käsittelyn tarkoitukset ja keinot sekä käsiteltävät henkilötiedot. Henkilötietojen käsittelyperuste määräytyy myös jokaisessa tutkimuksessa ja tutkimushankkeessa erikseen. Henkilötietojen säilytys tulee suunnitella osana tutkimusta ja lähtökohtaisesti henkilötietoja säilytetään vain tutkimuksen ajan, jonka jälkeen aineisto joko hävitetään tietoturvallisesti tai arkistoidaan tunnisteellisena tai anonyyminä.

Tieteellisessä tutkimuksessa rekisterinpitäjänä voi toimia esimerkiksi tutkija, tutkimusryhmä tai esimerkiksi yliopisto. Rekisterinpitäjyys tutkimuksessa määräytyy sen perusteella, mikä taho määrittää henkilötietojen käsittelyn tarkoituksen ja keinot. Rekisterinpitäjyys määrittää myös velvollisuuksia ja vastuita liittyen henkilötietojen käsittelyyn.

[92] Siun sote – Henkilötietojen käsittelyn ehdot (Siun sote intra)
[93] Siun sote – Toimintaohje: Henkilötietojen käsittelyn ehdot ja henkilötietojen käsittelytoimien kuvaus (Siun sote intra)
[94] Siun sote – Henkilötietojen käsittelystä sopiminen (Siun sote intra)

Tutkimuksissa henkilötiedot voidaan saada joko tutkittavilta itseltään tai muista lähteistä esimerkiksi viranomaisen aineistoista ja rekistereistä. Lähtökohtaisesti henkilötietojen käsittelystä informoidaan tutkittavia henkilöitä aina kun se on mahdollista. Esimerkiksi joissakin rekisteritutkimuksissa informointi ei ole aina mahdollista, jolloin informointivelvoitteesta voi poiketa. Informointi tulee kuitenkin aina harkita tutkimus- ja tapauskohtaisesti.

Tutkimuksissa kuten muussakin henkilötietojen käsittelyssä tulee lisäksi kiinnittää huomiota turvalliseen tietojen käsittelytapaan sekä ympäristöön (mm. tietojärjestelmät) joissa tietoja käsitellään. Pelkästään tietosuojan huomioiminen ei siis riitä, vaan tulee arvioida myös riittävää tietoturvaa, jotta saavutetaan tutkimusaineiston näkökulmasta riittävä ja asianmukainen tietoturvallisuuden tila. Ajoittain tutkimuksista tulee tehdä myös tietosuojaa koskeva vaikutustenarviointi (DPIA), jonka tavoitteena on tunnistaa tutkimuksen henkilötietojen käsittelyyn liittyviä riskejä. DPIA on laadittava, jos tutkimukseen suunniteltuun henkilötietojen käsittelyyn liittyy merkittäviä tietosuojariskejä tutkittavien eli rekisteröityjen kannalta. Riskejä voivat olla mm. suuret tietomäärät tai mikäli käsittely kohdistuu lapsiin tai arkaluonteisiin tietoihin. Arkaluonteisten henkilötietojen käsittely edellyttää myös tutkimuseettisen toimikunnan ennakkoarviointia. Ennakkoarviointi voidaan vaatia myös muissa tilanteissa mm. tutkimuskumppanin tai rahoittajan vaatimuksesta.

Siun sotessa tehdään toimialaan kuuluvaa tieteellistä tutkimusta sekä eri alojen perustutkintoihin kuuluvia opinnäytetöitä. Mikäli tutkimus kohdistuu sosiaali- ja terveydenhuollon asiakas- ja/tai potilastietoihin, kyseessä on sosiaali- ja terveystietojen toissijainen käyttö, jota ohjaa laki sosiaali- ja terveystietojen toissijaisesta käytöstä (552/2019).

Tietosuojavastaavan vinkit!

- Muista, että Siun sotessa tehtäviin tieteellisiin tutkimuksiin tarvitaan Siun soten myöntämä tutkimuslupa. Tutustu tutkimusluvan hakemiseen liittyvään ohjeistukseen[95]!
- Tutustu Siun soten rekisteritutkimuksiin liittyvään ohjeistukseen[96]!
- Tutustu tieteellisen tutkimuksen tietosuojaan sekä tieteellisen tutkimuksen tietosuojapolkuun[97]!
- Lue lisää sosiaali- ja terveystietojen toissijaista käyttöä koskevista pyynnöistä ja tutustu Siun soten aineistoneuvontaan[98]!
- Muista, että henkilötietojen käsittely pitää pystyä perustelemaan tutkimuksen jokaisessa vaiheessa!

[95] Siun sote – Tutkimusluvan hakeminen
[96] Siun sote - Rekisteritutkimus
[97] Tietosuojavaltuutetun toimisto – Tieteellinen tutkimus ja tietosuoja
[98] Siun sote - Toisiolaki

- Minimoi käsiteltävien henkilötietojen määrä tieteellistä tutkimusta tehtäessä! Pyri anonymisoimaan tiedot aina, kun se on mahdollista. Kun henkilötietojen tunnistettavuus on poistettu anonymisoimalla oikein, henkilön tunnistaminen edes yhdistämällä tiedot muualta saataviin tietoihin ei ole enää mahdollista.

12 Henkilötietojen käsittelyn valvonta

Tietosuojan valvonnan tarkoituksena on varmistaa, että henkilötietoja käsitellään laillisesti ja tietosuojan periaatteiden mukaisesti. Valvonnalla varmistetaan myös tietojen käsittelijöiden oikeusturvan toteutuminen. Siun sotessa tietosuojan valvontaa toteutetaan tietosuojan valvontasuunnitelman[99] mukaisesti. Myös henkilötietojen käsittelyn selvityspyyntöjen prosesseja on kuvattu tarkemmin tietosuojan valvontasuunnitelmassa.

Asiakastietolain mukaisesti sosiaali- ja terveydenhuollon palvelunantajan on kerättävä lokitietoja seurantaa ja valvontaa varten kaikesta asiakastietojen käytöstä, luovutuksesta sekä tietojärjestelmien käytöstä, ja asiakkailla on oikeus saada lokitiedot tietojensa käsittelystä. Siun sotessa valvontaa toteutetaan asiakkailta tulevien lokitietopyyntöjen perusteella sekä osana tietosuojan omavalvontaa, jossa tietosuojavastaavat valvovat tietojen asianmukaista käsittelyä tekemällä satunnaistarkastuksia asiakas- ja potilastietojärjestelmien tuottamiin asiakas- ja käyttäjälokeihin. Valvonta sisältää myös Kanta-palvelujen käytön valvonnan asiakas- ja potilastietojärjestelmä Mediatrin Medikanta -katselimen osalta. Tarvittaessa tietosuojavastaavat tekevät Kelalle pyynnön luovuttaa reseptikeskuksen ja Kanta-palvelujen lokitietoja seurannan ja valvonnan toteuttamiseksi.

Tietosuojan omavalvontaa kohdennetaan myös muihin henkilötietoja sisältäviin tietojärjestelmiin, mikäli on tarpeen tarkastella henkilötietojen käsittelyä myös muissa kuin asiakas- ja potilastietojärjestelmissä. Valvonnan tarve määräytyy tällöin toimialueelta, ja valvonta toteutetaan yhteistyössä järjestelmien ylläpitäjien ja pääkäyttäjien kanssa, joiden avulla tietosuojavastaavat saavat tarpeelliset lokiraportit käyttöönsä.

Tietosuojavastaavan vinkit!

- Asiakas- ja potilastietojärjestelmiin tallentuu automaattisesti lokitieto eli tieto siitä, kuka on käsitellyt asiakas- tai potilastietoja. Asiakkaalla on oikeus saada tietää, kuka on käsitellyt häntä koskevia tietoja.

[99] Siun sote – Tietosuojan valvontasuunnitelma (Siun sote intra)

12.1 Henkilötietojen tietoturvaloukkaukset

Tietoturvaloukkauksella tarkoitetaan tapahtumaa, jonka seurauksena henkilötietoja tuhoutuu, häviää, muuttuu tai niitä luovutetaan luvattomasti sivulliselle tai niihin pääsee käsiksi ulkopuolinen taho, jolla ei ole tietojen käsittelyoikeutta. Tietoturvaloukkaus voi tapahtua vahingossa tai tahallisesti.

Henkilötietojen tietoturvaloukkauksia ovat mm. seuraavat tilanteet:

- henkilötietoja on postitettu väärälle asiakkaalle tai lähetetty muutoin väärälle vastaanottajalle
- asiakas- tai potilastietoihin on tehty virheellinen merkintä tai kirjaus (mm. virhe kirjauksessa, tiedot kirjattu väärälle asiakkaalle, ajanvaraus tehty väärälle asiakkaalle)
- asiakas- tai potilastietoja on käsitelty ilman asiallista syytä mm. ilman asiakas- tai hoitosuhdetta
- henkilötietoja on luovutettu luvattomasti tai tietoja on lainvastaisesti tuhottu tai muutettu
- henkilötietoihin on ollut luvaton pääsy tai käyttöoikeus
- henkilötietoja sisältävää aineistoa löytyy paikasta, jossa sitä ei kuuluisi säilyttää (mm. toimitilojen käytävälle pudonnut henkilötietoja sisältävä asiakirja tai väärälle tulostimelle tulostunut henkilötietoja sisältävä asiakirja)
- henkilötietoja sisältävä laite katoaa tai varastetaan (mm. työasema, tiedonsiirtoväline)
- henkilötietojen saatavuus tai käytettävyys estyy (mm. järjestelmähäiriö)
- henkilö-, asiakas- tai potilastietojen joutuminen sivullisten saataville ja nähtäville (esim. asiakastietoja on postitettu väärälle asiakkaalle)
- henkilötietojen käsittely ilman asiallista syytä (mm. ei työtehtävään liittyvä käsittely).

Siun soten on rekisterinpitäjänä dokumentoitava kaikki toiminnassa esille tulleet ja havaitut tietoturvaloukkaukset. Lisäksi rekisterinpitäjän tulee ilmoittaa riskinarvion perusteella tapahtuneista tietoturvaloukkauksista tietosuojavaltuutetun toimistoon sekä loukkauksen kohteeksi joutuneelle henkilölle. Tarvittaessa ilmoitukset tehdään myös viranomaisille mm. poliisille tai Kyberturvallisuuskeskukselle. Tietoturvaloukkausilmoitukset sekä niiden käsittely kirjataan asianhallintajärjestelmään Siun soten tietosuojavastaavien toimesta.

Jokainen Siun soten työntekijä on velvollinen ilmoittamaan omalle esihenkilölleen tai Siun soten tietosuojavastaavalle havaitessaan tietoturvaloukkauksen tai epäillessään sellaisen tapahtuneen. Kaikista tietoturvaloukkauksista tulee tehdä ilmoitus sähköisesti Miunpalveluissa[100].

Tietosuojavastaavan vinkit!

[100] Miunpalvelut – Ilmoitus henkilötietojen tietoturvaloukkauksesta Siun sotelle

- Huomioitavaa on, että vaaratapahtumailmoituksen (Laatuportti) tekeminen ei korvaa virallista ilmoitusta henkilötietojen tietoturvaloukkausilmoituksesta! Ilmoitus laaditaan aina Miunpalveluissa.
- Tietoturvaloukkausilmoituksen voi Siun sotelle tehdä myös asiakas. Asiakkaille tietoturvaloukkausilmoituksen tekeminen on ohjeistettu Siun soten verkkosivuilla[101].
- Riskinarvio tehdään tietosuojavastaavan ja toiminnasta vastaavan esihenkilön kanssa. Tietosuojavastaavat neuvovat rekisteröidylle ilmoittamisessa sekä tekevät tarvittaessa ilmoituksen valvontaviranomaiselle!
- Mikäli riskinarviossa päädytään rekisteröidylle ilmoittamiseen, kirjallisesta ilmoituksesta on saatavilla mallipohja[102]. Ilmoittamisen voi hoitaa myös puhelimitse. Voit tarvittaessa pyytää ohjausta rekisteröidylle ilmoittamiseen tietosuojavastaavilta.
- Älä ilmoita tapahtumasta itse tietosuojavaltuutetun toimistoon, ilmoitukset valvontaviranomaiselle tehdään tietosuojavastaavien toimesta!
- Mikäli tietoturvaloukkaukseen liittyy asiakas- ja potilastietojen korjaamisen tarvetta, toiminnasta vastaavat esihenkilöt vastaavat korjaustoimenpiteiden toteutuksesta!
- Havaitut tietoturvaloukkaukset tulee käydä toimintayksiköissä läpi. Esihenkilöt arvioivat toimintakäytäntöjen kehittämistarpeet ja ovat vastuussa niiden toteuttamisesta!
- Turvallisuuspäällikkö tekee tarvittaessa tapahtumasta ilmoituksen poliisille, mikäli kyseessä on tutkintaa edellyttävä rikos. Laajemmissa häiriötilanteissa Siun soten häiriötilannejohtoryhmä tekee arvion tarvittavista viranomaisilmoituksista.

13 Tiedon käsittely

Tiedon elinkaari kattaa kaikki tiedon käsittelyn vaiheet, jotka ovat tiedon tuottaminen tai vastaanotto, säilytys, käyttö, jakaminen, siirto ja arkistointi tai tuhoaminen. Tietoaineistojen ja niiden käsittelyn turvallisuus tulee varmistaa koko tiedon elinkaaren ajan. Pääsääntöisesti tiedot tallennetaan niihin tietojärjestelmiin, jotka ovat kyseisten tietojen tallennuspaikoiksi määriteltyjä.

Tiedon luokittelun tarkoituksena on jaotella tiedot niiden luonteen mukaan, jotta tietojen käsittely tapahtuisi asianmukaisella tavalla. Luokittelun mukaisen suunnitelmallisen ja riskilähtöisen käsittelyn tarkoituksena on varmistaa tiedon tietoturvallisuus kaikissa tiedon elinkaaren vaiheissa. Siun sotessa tietoaineistot luokitellaan ja käsitellään tietojärjestelmien ulkopuolella erillisen toimintaohjeen[103] mukaisesti. Lisäksi tiedon luokittelusta

[101] Siun sote – Henkilötietojen käsittely
[102] Siun sote – Ilmoitus henkilötietojen tietoturvaloukkauksesta, kirjepohja (Siun sote intra)
[103] Siun sote – Toimintaohje: Tietoaineiston luokittelu ja käsittely tietojärjestelmien ulkopuolella (Siun sote intra)

riippumatta kaikessa henkilötietojen käsittelyssä tulee noudattaa tietosuojan periaatteita ja voimassa olevaa lainsäädäntöä.

Tietosuojavastaavan vinkit!

- Perehdy Siun soten tiedonhallintamalliin[104] sekä tiedonhallinnan vastuisiin[105].
- Tutustu Siun soten tiedonohjaussuunnitelmaan[106], jossa on kuvattu mm. tietojärjestelmissä käsiteltävien tietojen säilytysajat (pois lukien asiakas- ja potilastiedot, joiden pysyvästä sähköisestä säilyttämisestä vastaa valtakunnallinen Kanta-arkisto).
- Tutustu Siun soten tietojärjestelmäluetteloon[107], jossa on listattu kaikki Siun soten tietojärjestelmät sekä järjestelmiin liittyvät lisätiedot. Huomioi lisäksi, että luettelo on päivittyvä kuvaus, jonka tulee vastata toiminnan nykytilaa. Tietojen ajantasaisuudesta vastaavat tietojärjestelmien yhteyshenkilöt!

13.1 Tiedon hakeminen ja internet-palvelut

13.1.1 Internetin käyttö

Internet-turvallisuus on käsite, jolla tarkoitetaan internetissä tehtyjen toimintojen ja tapahtumien turvallisuutta. Se kuuluu osana laajempiin kyberturvallisuuden ja tietokoneturvallisuuden käsitteisiin ja siihen sisältyy myös verkkoselaimen turvallisuus, käyttäytyminen verkossa ja verkon turvallisuus.

Internetissä esiintyy uhkia, joista on hyvä olla tietoinen. Verkkourkinta, hakkerointi ja etäkäyttöohjelmistot, haittaohjelmat ja -mainonta ovat valitettavasti arkipäivää. Internetissä myös luotettavaksi luultu sivusto voi joutua palvelunestohyökkäyksen kohteeksi tai sivusto voidaan naamioida näyttämään aidolta, mutta taustalle onkin luotu rikollistarkoitukseen tietojenkalastelusivusto.

Työajalla internetin käyttö on sallittua luotettavan tiedon hakemiseen ja työtehtäviin liittyvien palvelujen käyttämiseen sekä muihin työtehtävien hoitamiseen liittyviin tehtäviin. Turha ja tarpeeton surffailu internetissä tulee jättää vapaa-ajalle. Kaikki tarkoitukseltaan haitallinen tai hyvän tavan vastainen internetin käyttö on työnantajan laitteilla kielletty.

[104] Siun sote – Tiedonhallintamalli (Siun sote intra)
[105] Siun sote – Tiedonhallinnan vastuut (Siun sote intra)
[106] Siun sote – Tiedonohjaussuunnitelma (Siun sote intra)
[107] Siun sote – Tietojärjestelmäluettelo (Siun soten intra)

Tietosuojavastaavan vinkit!

- Tunnista informaatiovaikuttaminen, tutustu Kyberturvallisuuskeskuksen ohjeeseen[108]!
- Käytä luotettavia tietolähteitä ja huomioi aina tekijänoikeudet ja asianmukaiset lähdeviitaukset.
- Älä tallenna salasanoja tai käyttäjätunnuksia internet-selaimen muistiin.
- Muista tyhjentää internet-selaimen välimuisti (ml. sivuhistoria, evästeet).
- Siun soten tietoliikenneyhteyksien ja muiden työvälineiden (mm. puhelin ja työasema) käyttö henkilökohtaiseen opiskeluun, muiden työnantajien töihin tai muihin sivuansioihin on kielletty, ellei siitä ole erikseen sovittu työnantajan kanssa.
- Älä käytä työhön liittyviä käyttäjätunnuksia ja salasanoja muissa palveluissa. Jokaiseen palveluun on hyvä luoda erilliset käyttäjätunnukset ja salasanat. Näin mahdollisen tietomurron yhteydessä muut palvelut ja työnantajan käyttäjätilit eivät vaarannu!
- Älä rekisteröidy Siun soten sähköpostiosoitteella tai muulla työnantajan käyttäjätunnuksilla tai salasanoilla työhön liittymättömiin palveluihin (mm. verkkokauppaostokset, kuntosalijäsenyydet, harrastetoiminta).
- Poistu jokaisesta asiointipalvelusta aina sen omalla uloskirjautumistoiminnolla. Älä jätä kirjautumisistuntoja koskaan avoimeksi poistuessasi työaseman ääreltä! Lukitse poistuessasi myös koko työasema!
- Tutustu Kyberturvallisuuskeskuksen Netiketti – Verkossa liikkujan työkalupakkiin[109]. Tiedoista on hyötyä niin työelämässä kuin vapaa-ajalla!

13.1.2 Salasanat

Siun soten työntekijät käyttävät salasanoja kirjautuessaan erilaisiin palveluihin ja työasemalle työtehtävissään. Hyvän ja laadukkaan salasanan luomiseen kannattaa uhrata aikaa, sillä salasanojen murtaminen on nykypäivänä erittäin helppoa. Hyvän salasanan keksiminen on tärkeää niin työssä kuin vapaa-ajalla. Salasanojen sijaan suositellaan käytettävän salalauseita, joka voi olla esimerkiksi helposti muistettava lause sisältäen isoja kirjaimia ja erikoismerkkejä.

Salasanojen luomisessa kannattaa muistaa seuraavat asiat:

- Mitä pidempi salasana on, sitä turvallisempi se on!
- Hyvä salasana on helppo muistaa, mutta vaikea arvata! Liian tunnistettavat asiat, kuten läheisten tai lemmikkien nimet on helpompi murtaa.

[108] Kyberturvallisuuskeskus – Ohje: Vinkkejä informaatiovaikuttamisen tunnistamiseksi, Ole tarkkana ja toimi vastuullisesti
[109] Kyberturvallisuuskeskus – Netiketti, Verkossa liikkujan työkalupakki

- Käytä salasanassa isoja ja pieniä kirjaimia sekä erikoismerkkejä!
- Erilaiset murresanat ja tahalliset kirjoitusvirheet ja puhekielen ilmaisut ovat salasanalle vahventava tekijä!
- Älä koskaan kerro kenellekään salasanaasi! Epäile heti sellaista tahoa, joka salasanaasi kysyy!

Kaikissa palveluissa tulee käyttää aina yksilöllisiä salasanoja. Salasanan vaihtaminen on tehtävä aina, mikäli on pienikin epäily salasanan joutumisesta vääriin käsiin.

Tietosuojavastaavan vinkit!

- Tutustu Meitan ohjeeseen salasanan vaihtamisesta[110] ja hyvän salasanan periaatteista[111]!
- Tutustu Kyberturvallisuuskeskuksen salasanoihin liittyviin ohjeisiin[112][113].

13.1.3 MFA – Monivaiheinen tunnistautuminen

Monivaiheinen tunnistautuminen (Multifactor Authentication, MFA) mahdollistaa turvallisemman kirjautumisen ja suojaa käyttäjätunnuksia paremmin väärinkäytöksiltä. Käytännössä monivaiheinen tunnistautuminen tarkoittaa sitä, että verkkopalveluun kirjautuminen todennetaan palveluun liitetyllä laitteella, tavallisimmin älypuhelimella. MFA:n avulla pystytään luotettavasti tunnistamaan käyttäjät verkkopalveluissa.

Verkkopalveluihin on käytetty aiemmin vain käyttäjätunnusta ja salasanaa, joka on yhdistelmänä haavoittuvainen tietomurron osuessa kohdalle. Laitteiden ja palvelujen tietoturva paranee monivaiheisen tunnistautumisen käyttöönotolla. Vaikka käyttäjätunnus ja salasana joutuisi vääriin käsiin, kirjautuminen ei onnistuisi ilman käyttäjän kolmatta todennustapaa.

Vahva ja monivaiheinen tunnistautuminen tekee käyttäjätilistä turvallisemman ja vähemmän alttiin hyökkäyksille. Monivaiheisen tunnistautumisen tarkoituksena onkin hankaloittaa väärinkäytöksiä ja havaita ne ennen tunnusten murtamista. Tämä ei kuitenkaan tarkoita sitä, että käyttäjätunnuksista ja salasanoista ei tarvitsisi enää pitää huolta tai mm. salasanojen vaihtoväliä voisi huoletta pidentää.

Monivaiheiden tunnistautumisen avulla Siun sotessa on mahdollista reagoida tietomurtoyrityksiin ennen kuin ne pääsevät toteutumaan. Vaikka yksittäisestä Siun soten työntekijästä esimerkiksi oman M365-tilin tietosisältö voi

[110] Miten voin vaihtaa vanhentuneen tai unohtuneen salasanan? - Asiakaspiste (meita.fi)
[111] Meita – Muutos salasanan pituuteen, vaihtoväliin sekä rakenteeseen (Siun sote intra)
[112] Kyberturvallisuuskeskus – Pidempi parempi, näin teet hyvän salasanan
[113] Kyberturvallisuuskeskus – Salasanat haltuun, kuka käyttää tiliäsi?

tuntua ns. arvottomalta, niin todellisuudessa jokaiseen M365-tiliin pääsy mahdollistaa pääsyn organisaatiolle tärkeisiin tietoihin sekä mahdollistaa tilin väärinkäytön uusien huijausten toteuttamiseksi.

Siun sotessa monivaiheinen tunnistaminen M365-palveluissa tapahtuu käyttäjätunnuksen ja salasanan lisäksi hyväksymällä mobiililaitteeseen (tavallisimmin älypuhelin) tuleva ilmoitus. Ilmoitus voi olla tekstiviesti, puhelinsoitto tai todentajasovellukseen tuleva ilmoitus. Ilmoituksen muoto riippuu siitä, millainen todennusmenetelmä tiliin on asetettu.

Tietosuojavastaavan vinkit!

- Siun sotessa MFA:n toteuttaminen tulisi lähtökohtaisesti aina tapahtua Authenticator-sovelluksen kautta. Todentajasovellukseen on tullut v. 2023 uutena ominaisuutena numerokysely eli ns. number matching -toiminto. Kirjautuminen todennetaan antamalla sovellukseen kaksinumeroinen koodi, joka näkyy palvelun kirjautumisikkunassa.

13.1.4 AI - Tekoäly

Tekoäly eli keinoäly (Artifical Intelligence, AI) kykenee tekemään erilaisia älykkäitä toimintoja, päättelyä, oppimista ja luomista. Tunnetuimpia tekoälyn muotoja ovat mm. puheentunnistus, erilaiset puhetoiminnot (mm. Siri), luovat työkalut (mm. ChatGPT) sekä ns. ruumiillistetut tekoälyt (mm. robotit). Tekoälyn perusajatuksena on jonkin järjestelmän tai ohjelmiston kyvykkyys tulkita ulkoisia tietoja, oppia niistä tiedoista ja käyttää opittuja asioita tavoitteiden ja tehtävien saavuttamiseen.

Tekoäly on kehittynyt viime aikoina voimakkaasti ja sen odotetaan ottavan uusia edistysaskelia lähitulevaisuudessa. Tekoälyn on osa yhteiskunnan digitaalista muutosta. Vaikka monet tekoälyn edistysaskeleet ovat toivottuja, tekoäly tuo väistämättä mukanaan myös riskejä, ja tekoälyä voidaan hyödyntää myös rikolliseen toimintaan entistä tehokkaammin ja nopeammin.

Tekoälyn turvallinen hyödyntäminen ja käyttö edellyttää vastuiden määrittelyä ja valvontaa. Tekoälyn hyödyntämistä ja soveltuvuutta tulee tarkastella käyttötapausten kautta; mihin tekoäly soveltuu hyödynnettäväksi ja mitä tietoja sen kanssa voidaan käsitellä. Esimerkiksi Excelin laskentataulukoiden ja -kaavioiden tekemiseen liittyy todennäköisesti vähemmän riskejä, kuin salassa pidettävien asiakas- ja potilastietojen tai muiden henkilötietojen käsittelyyn.

Tekoäly tulee todennäköisesti muuttamaan myös kyberhyökkäysten luonnetta tulevaisuudessa. Tekoälyä haluavat siis hyödyntää myös rikolliset, sillä se avaa heille uusia mahdollisuuksia toteuttaa erilaisia hyökkäyksiä. Tekoälyä hyödyntävät mallit kykenevät aikaisempaa paremmin automatisoimaan sekä kohdennettuja tietojenkalasteluhyökkäyksiä että haavoittuvuuksien etsimistä. Myös tekoälyn tukemat sosiaalisen manipuloinnin ja imitaatioon perustuvat hyökkäykset voivat lisääntyä.

Lähtökohtaisesti Siun sotessa käytetään vain käyttöön hyväksyttyjä järjestelmiä ja ohjelmistoja. Niiden tulee olla Siun soten tiedonhallintamallissa ja arkkitehtuurissa ja niistä tulee tarvittaessa olla laadittuna tietosuojaa koskeva

vaikutustenarviointi (DPIA). Joidenkin palvelujen käyttö tulee arvioida erikseen esimerkiksi asiakasrajapintatyössä (esim. kotihoidon käytössä olevat kauppojen ostostilaukset asiakkaille). Luottamuksellista ja salassa pidettävää tietoa ei tule kuitenkaan missään tilanteessa tallentaa Siun soten ulkopuoliseen järjestelmään tai palveluun.

Tietosuojavastaavan vinkit!

- Tutustu valtiovarainministeriön tekoälyn eettiseen ohjeistukseen[114].
- Osana digitaalista strategiaa, EU haluaa jatkossa säädellä tekoälyä. Sääntelyllä pyritään varmistamaan, että innovatiivista teknologiaa käytetään sekä kehitettään parhaalla mahdollisella tavalla. Huhtikuusta 2021 lähtien on valmisteltu EU:n ensimmäistä tekoälysääntelyä. EU:n parlamentti hyväksyi kesäkuussa 2023 kantansa sääntöihin tekoälyn riksien hallitsemiseksi sekä eettisen käytön edistämiseksi. Neuvottelut lain lopullisesta muodosta eivät ole vielä valmistuneet.
- Mikäli haluat hyödyntää tekoälysovellusta tai -ohjelmistoa työssäsi, keskustele asiasta esihenkilösi kanssa ennen käytön aloittamista. Tarvittaessa käyttöä on arvioitava ICT-palvelujen, tietoturvan, tietosuojan ja käsiteltävien tietojen näkökulmasta laajemmin. Tulee myös harkita, tuleeko käsittelytoimesta laatia tietosuojaa koskeva vaikutustenarviointi (DPIA).

13.1.5 IoT- Esineiden internet ja IoE -Kaiken internet

”Esineiden internet” (Internet of Things, IoT) tarkoittaa järjestelmiä, joiden taustalla on teknisten laitteiden suorittama automaattinen tiedonsiirto tai laitteiden etäseuranta ja -ohjaus. Teknisesti IoT-järjestelmä koostuu joko langattomasta tai kiinteästä verkosta, johon on kytketty jokin laite. Tunnetuimpia internettiin yhdistettyjä esineitä ovat mm. älykello, aktiivisuusranneke ja älykodit (sis. älykäs valaistus, langattomat kodinkoneet).

IoT-järjestelmiin ja laitteisiin liittyy tietosuoja ja tietoturvariskejä, jotka on tiedostettava ennen käyttöä ja käyttöönottoja. IoT-laitteiden tuottaman tiedon määrä on valtava, joka voi jo luoda hakkeroinnin mahdollistavia haavoittuvuuksia. IoT-laitteiden käyttöön liittyy myös usein pitkät käyttöehdot, joiden hyväksyminen on pakollista, että laitteen käyttö mahdollistuu.

”Kaiken internet” (Internet of Everything, IoE) tarkoittaa kattavaa ja älykästä yhteyksien verkostoa. IoT:n tavoin IoE-ratkaisujen tavoitteena on koota tietoa ja muuttaa se uudenlaisiksi mahdollisuuksiksi. IoE yhdistää niin ihmiset, esineet, tiedon ja prosessit. Prosesseista tyypillisimpiä ovat pilvipalvelut, tekoäly (AI), ns. Big Data sekä koneoppiminen.

[114] Valtiovarainministeriö – Tekoälyn eettinen ohjeistus

Tietosuojavastaavan vinkit!

- Mikäli IoT- tai IoE-järjestelmä tai laite otetaan käyttöön Siun sotessa, tulee jo käyttöönoton suunnitteluvaiheessa arvioida tietojen käsittelyyn mahdollisesti kohdistuvia riskejä. Mikäli tietojen käsittely kohdistuu mm. asiakas- ja potilastietoihin, tulee käsittelystä laatia aina tietosuojaa koskeva vaikutustenarviointi (DPIA).
- Huolehdi, että tunnistat omien tietojesi käsittelyyn liittyvät riskit, kun esimerkiksi käytät erilaisia IoT-laitteita vapaa-ajalla. Tutustu huolellisesti käyttöehtoihin, jotta tiedät missä tietojasi käsitellään ja mihin tarkoitukseen niitä voidaan mahdollisesti hyödyntää ja siirtää kolmansille osapuolille!
- Älä yhdistä omaa henkilökohtaista IoT-laitettasi työhön liittyviin laitteisiin, mm. työpuhelimiin tai työasemiin! Pidä omat ja työhön liittyvät tiedot erillään, äläkä vaaranna laitteiden yhdistämisellä työvälineiden tietoturvaa!

13.2 Tiedon tallentaminen

13.2.1 M365-pilviympäristö

Siun sotessa on otettu käyttöön vuodesta 2019 lähtien Microsoft 365-pilviympäristöä vaiheittain. M365-palvelut ovat tärkeä osa Siun soten sähköistä työympäristöä ja ne ovat monelle työntekijälle päivittäisessä käytössä olevia palvelua. M365-palveluihin kirjaudutaan omilla tunnuksilla ja jokaisella työntekijällä on käytössään oma profiili ja siihen määritelty lisenssitaso. M365-palvejen käyttö Siun sotessa edellyttää monivaiheista todennusta (MFA).

Tietosuojan näkökulmasta M365-palveluissa toteutettavissa tietojen käsittelytoimissa olennaisista on se, kuinka palvelua käytetään ja mitä tietoa palveluihin viedään käsiteltäväksi. Tietoaineiston käsittelyä M365-palveluissa ohjaa erillinen toimintaohje[115]. Toimintaohjeen mukaisesti salassa pidettäväksi luokitellun tietoaineiston tallennus, käsittely ja säilytys on M365-palveluissa kielletty.

Tietosuojavastaavan vinkit!

- Uusia M365-palveluja käyttöönotettaessa tulee huomioida kaikkien käyttäjien ohjeistus ja koulutus palvelujen ominaisuuksista, käytöstä, käyttöoikeuksien hallinnasta. Käsittelytoimen turvallisuuden takaamiseksi on syytä huomioida ohjeistukset myös tietojen tallentamisesta, jakamisesta ja säilyttämisestä palvelussa.

[115] Siun sote – Toimintaohje: Tietoaineiston luokittelu ja käsittely tietojärjestelmien ulkopuolella (Siun sote intra)

- Varaudu tietoliikenneyhteyksistä johtuviin katkoksiin. Esihenkilöiden johdolla yksiköissä tulee pohtia, kuinka esimerkiksi Teams-palvelun kaatuminen voisi vaikuttaa työhön ja miten poikkeustilanteisiin tulisi ennakolta varautua.
- Tutustu M365-pilviympäristön pelikirjaan ja ohjeisiin intrassa116.
- Huomioi, että OneDrive-tallennustila ei sovellu mm. asiakas- ja potilastietojen tai muiden salassa pidettävien tietojen tallennuspaikaksi!
- Huomioi, että poistaessasi mm. tiedostoja M365-palveluista, ne säilyvät kuitenkin kolmessa eri vaiheessa: 1. vaiheen roskakorissa (30vrk), 2. vaiheen roskakorissa (93vrk) sekä mahdollisuuksien mukaan vielä pitopolitiikan mukaisesti tämän jälkeen 1 vuoden ajan. Pitopolitiikka ei koske Teams-viestejä.
- Tiesithän, että voit myös salata Office-tiedostoja salasanalla. Valitse Tiedot-välilehdeltä asiakirjan suojaus ja aseta salasana. Muista asetettu salasana! Mikäli salasana unohtuu, tietojen salausta ei voi purkaa.

13.2.2 Työaseman paikallinen levytila ja henkilökohtainen verkkolevy

Työaseman paikallisia levytiloja ovat mm. työpöytä ja C-asema. Lisäksi työntekijällä voi olla käytössään henkilökohtainen verkkolevy mm. X-asema. Oikeudet voivat vaihdella Microsoft-lisenssitason mukaisesti.

Asiakas- ja potilastietoja ei tule käsitellä kyseisillä levytiloilla tai verkkolevyillä. Myös henkilötietoja sisältävien tietojen käsittely on lähtökohtaisesti kiellettyä. Väliaikaistallennuksia voi tehdä, mikäli on tarve laatia esimerkiksi lausunto tai vastine. Tällöin tulee huolehtia siitä, että tiedosto poistetaan asianmukaisesti käsittelytoimen päätyttyä.

Siun sotessa on lisäksi käytössä joitain yhteisiä verkkolevyjä Z-asemalla, joihin myös oikeudet vaihtelevat Microsoft lisenssitason mukaisesti. Yhteisellä verkkolevyllä voi olla myös työyksikön sisäisiä kansioita, joihin käyttöoikeudet on määritelty esihenkilön toimesta. Myös yhteisillä verkkolevyillä asiakas- ja potilastietojen sekä muiden henkilötietoja sisältävien tietojen käsittely on lähtökohtaisesti kiellettyä. Mikäli Z-asemalla on tarpeen käsitellä kyseisiä tietoja, tulee käsittelytoimesta laatia tietosuojaa koskeva vaikutustenarviointi (DPIA).

Tietosuojavastaavan vinkit!

- Ennen levytilojen ja verkkolevyjen käyttöä on varmistuttava siitä, kenellä on kyseisiin tallennustiloihin pääsy!

[116] Siun sote – Pelikirja – 365-pilviympäristö (Siun sote intra)

- Yksiköiden omiin ja tiettyihin käsittelytoimiin rajoitettuja verkkolevyjä on syytä tarkastella sisällöllisesti, esimerkiksi kerran vuodessa verkkolevyille on suositeltavaa suorittaa siivous, jossa tarpeettomat ja vanhentuneet tiedot poistetaan.
- Huomioi, että työaseman työpöydälle tallennettuja tiedostoja ei varmisteta, eli työaseman hajotessa, kaikki työpöydälle tallennetut tiedostot poistuvat eikä niitä voi palauttaa!
- Palvelussuhteen päättymisen lähestyessä (mm. eläkkeelle siirtyminen) työhön liittyvät tiedostot on hyvä käydä läpi. Tarpeettomat tiedostot tulee poistaa. Esihenkilön kanssa tulee sopia sellaisten tiedostojen siirtämisestä, jotka ovat työhön liittyviä ja jotka tulee siirtää työnantajalle ennen palvelussuhteen päättymistä.

13.2.3 Ulkoinen tallennusväline

Ulkoisia tallennusvälineitä ovat mm. muistitikut, CD- ja DVD-levykkeet sekä ulkoiset kovalevyt. Mikäli työntekijä käyttää työssään ulkoisia tallennusvälineitä, hän vastaa itse niiden turvallisesta käytöstä ja tarvittavista suojauksista. Ulkoisten tallennusvälineiden käytöstä on keskusteltava ja sovittava esihenkilön kanssa, jotta voidaan arvioida niiden tarve työtehtävän hoitamisessa ja suunnitella tietojen käsittely mahdollisimman tietoturvallisella tavalla.

Ulkoinen tallennusväline tulee salata aina, mikäli sillä säilytetään Siun soten sisäistä ja luottamuksellista tietoa. Asiakas- ja potilastiedon tallentaminen ja käsittely ilmoisilla tallennusvälineillä on kielletty.

Tietosuojavastaavan vinkit!

- Älä yhdistä henkilökohtaista ulkoista tallennusvälinettä Siun soten työasemiin. Älä siis käytä Siun soten työasemalla esimerkiksi samaa muistitikkua, jota käytät kotikoneella, oppilaitoksessa tai julkisissa käytössä olevissa työasemissa (esim. kirjasto).
- Älä yhdistä tuntematonta tallennusvälinettä Siun soten työasemaan, mikäli esimerkiksi löydät toimitiloista tai kokoushuoneista muistitikun.
- Käytä esimerkiksi muistitikkujen salaukseen Bitlocker-suojausta! Lisää suojaus ja muistitikun avaamiseen tarvittava salasana muistitikkuun ennen sen käytön aloittamista. Muista asetettu salasana tai palautusavain, ja pidä ne erillään muistitikusta aina! Mikäli salasana ja palautusavain unohtuu, muistitikun sisältöä ei voi mitenkään palauttaa.
- Muista, että voit myös salata Office-tiedostoja salasanalla. Valitse Tiedot-välilehdeltä asiakirjan suojaus ja aseta salasana. Muista asetettu salasana! Mikäli salasana unohtuu, tietojen salausta ei voi purkaa.

13.2.4 Paperiset tietoaineistot

Siun soten toimipaikoissa käsitellään paperisia tietoaineistoja. Toimintayksiköiden esihenkilöt vastaavat siitä, että paperisten tietoaineistojen käsittely ja säilytys on suunniteltu asianmukaisesti. Mikäli tietoaineistot sisältävät

luottamuksellista tai salassa pidettävää tietoa, säilytys tulee tapahtua lukitussa kaapissa tai lukitun huoneen kaapissa, johon on pääsy rajatuilla henkilöillä, joilla on työtehtävän mukainen oikeus kyseisiin aineistoihin.

Paperisten tietoaineistojen tarpeetonta säilytystä (arkistointia) työpisteillä ja toimipaikoissa tulee välttää. Tarpeettomat tiedot on tuhottava tietoturvallisesti.

Tietosuojavastaavan vinkit!

- Pohdi kriittisesti, mitä tietoja on tarpeellista säilyttää paperisena. Arvioi kriittisesti myös tietojen tulostamisen tarvetta!
- Asiakas- ja kotikäynneillä paperisten tietoaineistojen osalta on kiinnitettävä huomiota niiden turvalliseen käsittelyyn.
- Varmistu, missä ja miten kuljetat tietoaineistoa! Taiteltu paperi taskussa voi tippua helposti toimitilojen käytäville, niiden ulkopuolelle tai päätyä työasusteen mukana pesulaan!
- Jätä aina paperiset tiedot työyksikköön poistuessasi. Älä vie esimerkiksi potilaslistoja mukanasi pukuhuoneeseen!

13.3 Tiedon välittäminen

13.3.1 Sähköposti ja kalenteri

Sähköposti on työväline, joka on ensisijaisesti tarkoitettu työasioiden hoitamista varten. Yksityisasioiden hoitamiseen ei suositella käytettäväksi työsähköpostia. Työsähköpostin käyttäminen on kielletty mm. henkilökohtaisten tarjouspyyntöjen tai tarjousten tekemiseen, kaupankäyntiin tai muuhun henkilökohtaiseen toimintaan, jossa viestin vastaanottajan on vaikea tulkita viestin lähettäjän roolia.

Siun soten työntekijä vastaa työsähköpostinsa käyttämisestä, sähköpostien sisällöstä sekä kalenterin ja tehtäväluetteloiden sisällöstä ja ylläpidosta. Sähköpostien edelleen lähettäminen ulkoiseen sähköpostiosoitteeseen (esim. oma henkilökohtainen sähköpostiosoite tai muu luottamustoimen tai toisen palvelussuhteen sähköpostiosoite) on kielletty. Sähköpostin käyttöoikeus päättyy palvelussuhteen päättyessä.

Sähköpostin kalenteri on hyvä tapa pitää yllä aikatauluja ja hallinnoida omaa työtä. Kalenterin käytössä on huomioitava, että siihen ei tule merkitä kenenkään henkilötietoja tai asiakkaiden asiakas- tai potilastietoja tai muuta salassa pidettävää tietoa. Oman kalenterin voi jakaa halutessaan toiselle käyttäjälle, omalle työyhteisölle tai tiimille. Mikäli kalenterin jakamisesta on sovittu omassa työyhteisössä, on hyvä käydä läpi kalenterin jakamisen pelisäännöt. Muutoin kalenterin jakamisesta ja käyttöoikeuksien määrittelemisestä päättää työntekijä itse.

Tietosuojavastaavan vinkit!

- Tarkasta viestin vastaanottajan sähköpostiosoite erittäin huolellisesti! Älä luota sähköpostin automaattisesti ehdottamiin sähköpostiosoitteisiin ja huomioi, että mahdollisten nimikaimojen

vuoksi vastaanottajan sähköpostiosoite ei välttämättä ole aina muotoa etunimi.sukunimi@domain.fi

- Sähköpostien liitetiedostoihin tai ulkoisiin linkkeihin tulee suhtautua varauksella, mikäli et ole varma niiden sisällöstä. Liitetiedostot ovat yleinen virusten tai haittaohjelmien levittämismuoto ja ulkoiset linkit voivat johtaa huijaussivustoille!
- Arkaluontoisten ja salassa pidettävien tietojen lähettämiseen tulee käyttää suojattua sähköpostia! Tämä pätee myös silloin, kun viesti lähetetään Siun soten työntekijöiden välillä!
- Mikäli saat tietojen kalastelulta tai huijaukselta vaikuttavan sähköpostin, älä avaa viestiä tai sen sisältämiä liitetiedostoja tai linkkejä. Ole yhteydessä asiasta Meitaan!
- Käytä sähköpostin automaattisia vastauksia ilmoittaaksesi poissaolostasi (esim. loma-ajat) sekä siitä, kuka hoitaa työtehtäviäsi poissaolosi aikana!
- Mikäli saat jollekin toiselle kuuluvan sähköpostiviestin, ilmoita asiasta viipymättä viestin lähettäjälle. Tuhoa saamasi sähköpostiviesti ja sen liitetiedostot. Mikäli viesti on sisältänyt asiakas- tai potilastietoa tai henkilötietoja, kyseessä on tietoturvaloukkaus, josta tulee tehdä ilmoitus!
- Viranomaiselle toimitettu tai viranomaisen laatima sähköpostiviesti voidaan katsoa julkisuuslain mukaiseksi viranomaisen asiakirjaksi.
- Asiakasnumeron (mm. Mediatrinumero) käyttö sähköposteissa on mahdollista tilanteissa, joissa asiakasnumero ei ole yhdistettynä muuhun asiakas- ja potilastietoon.
- Tiesithän, että yleinen sähköpostiosoite (mm. kirjaamo@siunsote.fi) ei ole henkilötiedoksi luokiteltava tieto.

13.3.2 Yhteiskäyttöinen sähköposti

Sähköpostiosoite voi olla yhteiskäyttöinen, jolloin sähköpostiosoitetta hallinnoi ja käyttää useampi eri käyttäjä. Yhteiskäyttöisen sähköpostin Meitalta tilaa esihenkilö, ja hän vastaa myös sähköpostin käyttötarkoituksista, ajantasaisista käyttöoikeuksista sekä sähköpostiosoitteen lakkauttamisesta, kun käyttötarve päättyy.

Tietosuojavastaavan vinkit!

- Laadi yhteiskäyttöiselle sähköpostille pelisäännöt, joita sitoutuvat noudattamaan kaikki käyttäjät. Pelisäännöissä on suositeltavaa huomioida mm. viestien käsittely sekä vanhojen viestien poistaminen ja kalenterimerkinnät.
- Saapuneet-kansioon voi luoda alikansioita, jolloin viestien käsittelyä voi jaotella.
- Yhteiskäyttöisestä sähköpostista lähetetyissä viesteissä on hyvä esiintyä työntekijän omalla nimellä. Älä siis tarpeettomasti ”piiloudu” esimerkiksi tiimin nimen taakse, vaan allekirjoita lähettämäsi sähköpostit omalla nimelläsi!
- Esihenkilön tulee tarkastaa käyttöoikeudet säännöllisesti, ettei kenelläkään ole tarpeettomia käyttöoikeuksia sähköpostiin.

13.3.3 Suojattu sähköposti

Sähköpostiviestin suojaaminen mahdollistaa viestin turvallisen lähettämisen, viestin sisällön pysymisen salassa sekä vastausviestin vastaanottamisen luottamuksellisesti. Suojattua sähköpostia tulee käyttää, mikäli sähköpostitse lähetetään arkaluontoisia ja salassa pidettäviä tietoja. Samoin kuin tavallisen sähköpostiviestin lähetyksessä, tulee suojatun sähköpostiviestin vastaanottajan osoitetieto kirjoittaa ja tarkastaa huolellisesti.

Esihenkilö tilaa suojatun sähköpostin käyttöoikeudet Meitalta niille työntekijöille, joilla on tarve lähettää omaan työtehtävään liittyen salassa pidettävää tietoa sähköpostitse.

Tietosuojavastaavan vinkit!

- Tarkasta viestinvastaanottajan sähköpostiosoite erittäin huolellisesti! Älä luota sähköpostin automaattisesti ehdottamiin sähköpostiosoitteisiin!
- Mikäli asiakasviestinnässä on tarpeen varmistua asiakkaan sähköpostiosoitteesta, varmin tapa on pyytää asiakasta lähettämään ensin sähköpostia työntekijälle!
- Muista, että sähköpostiosoitteen kirjoittamisessa pienikin virhe voi johtaa siihen, että viesti lähtee väärälle vastaanottajalle!
- Poista lähettämäsi sähköpostiviesti Lähetetyt-kansiosta ja sen jälkeen Poistetut-kansiosta.
- Huomioithan, että mikäli vastataan suojattuun sähköpostiviestiin ja kahden sähköpostiosoitteen välille muodostuu suojattu TSL-yhteys, ei viestejä vaihtaessa muodostu enää linkkiä, jonka kautta viesti avautuu, vaan sähköpostiviesti todellakin avautuu ”sellaisenaan” vastaanottajalle. TSL-yhteydessä kertova tieto viestin alussa informoi ja varmistaa viestin suojauksen tasosta.

13.3.3.1 Suojatun sähköpostin tasot

Suojatussa sähköpostissa on kolme tasoa. Suojauksen taso tulee valita sen mukaisesti, kenen kanssa suojatulla sähköpostilla viestitään.

- ”Kirje” -taso
  - Tätä tasoa käytetään vain viranomaisyhteistyössä tai organisaation sisällä, mikäli sähköpostiviestin vastaanottajaa ei ole tarpeen tunnistaa vahvasti
  - Tätä tasoa ei tule käyttää asiakas- ja potilasviestinnässä!
  - Vastaanottajan sähköpostiosoitteen perään lisätään ***.s*** (esim. etunimi.sukunimi@domain.fi.s)
- ”Kirjattu kirje” -taso
  - Tätä tasoa käytetään asiakkaille ja potilaille lähetettävissä sähköpostiviesteissä, mikäli asiakkaalla ei ole käytössään vahvaan tunnistautumiseen tarvittavia välineitä (mm. pankkitunnukset tai mobiilivarmenne)
  - Vastaanottaja saa hänelle lähetetyn viestin auki tekstiviestitse saapuvalla koodilla
  - Vastaanottajan sähköpostiosoitteen perään lisätään ***.GSM-numero.s*** (esim. etunimi.sukunimi@domain.fi.0501234567.s)

- ”Suomi.fi tunnistautuminen” -taso
    - Tätä tasoa käytetään asiakkaille ja potilaille lähetettävissä sähköpostiviesteissä, kun on tarve tunnistaa asiakas vahvasti
    - Vastaanottajan saa hänelle lähetetyn viestin auki vahvalla tunnistautumisella (mm. pankkitunnukset tai mobiilivarmenne)
    - Vastaanottajan sähköpostiosoitteen perään lisätään ***.vastaanottajan henkilötunnus.s*** (esim. etunimi.sukunimi@domain.fi.010101-010A.s tai etunimi.sukunimi@domain.fi.010101A0101.s)

Tietosuojavastaavan vinkit!

- Suojatun sähköpostiviestin seuraamiseksi on suositeltavaa pyytää sähköpostiviestiin vastaanotto- ja lukukuittaus viestin vastaanottajalta. Nämä määritykset on tehtävä sähköpostiviestiin ennen viestin lähettämistä!

13.3.4 Faksi

Faksi on lyhennetty sanasta Telefax, joka tarkoittaa asiakirjan jäljitelmän tai kopion lähettämistä puhelinverkon kautta. Faksi laaditaan liittämällä tai skannaamalla asiakirja ja se lähetetään toiseen faksilaitteeseen tai -palveluun. Faksin käyttö on vähentynyt merkittävästi, kun käytössä on edistyneempiä, helpompia ja tietoturvallisempia tapoja välittää asiakirjoja.

Faksia tulee käyttää erittäin harkiten luottamuksellisen ja salassa pidettävän tietoaineiston välittämisessä. Faksin käyttö kyseisissä tietoaineistoissa edellyttää, että kaikki seuraavat ehdot täyttyvät:

- lähetettävät asiakirjat tulee salata siirron aikana
- tietoaineiston lähetys ja vastaanotto tapahtuu siten, että asiakirjat lähettävät ja vastaanottavat sellaiset tahot, jotka ovat oikeutettuja asiakirjojen sisältöön
- tietoaineiston lähetyksestä ja vastaanottamisesta jää merkintä (huomioiden asianmukaiset merkinnät asiakas- ja potilasasiakirjoihin)
- tietoaineiston lähetys tapahtuu suunnitelmallisesti ja hallitusti osana muiden tietojärjestelmien käyttöä
- asiaan liittyvät menettelyt on ohjeistettu
- tietoaineiston käsittelyssä huolehditaan suojaamis- ja huolellisuusvelvoitteista
- menettely on sovittu vastaanottavan osapuolen kanssa.

Kiireellisissä tapauksissa faksin käyttö voi olla edelleen välttämätöntä. Tällöinkin on syytä varmistua siitä, että lähetyksestä sovitaan vastaanottavan tahon kanssa, jotta vastaanottava taho voi osaltaan huolehtia tietoaineistosta asianmukaisesti. Viime kädessä faksin osalta ratkaisevaa on, että vastaanottajan numero laitetaan oikein ennen lähetystä.

Tietosuojavastaavan vinkit!

- Soita henkilölle, jolle faksi on tarkoitettu ja pyydä hänet faksin ääreen! Pyydä häneltä myös kuittaus, että hän on saanut kyseisen faksin.
- Laita aina faksin ensimmäiseksi sivuksi kansilehti, jossa ilmenee, kenelle viesti on tarkoitettu ja mitä se sisältää.
- Sijoita faksilaite sellaiseen tilaan, joihin ei ulkopuolisilla ole pääsyä.
- Suosi mahdollisuuksien mukaan suojatun sähköpostin käyttöä, mikäli sellainen on mahdollista faksin sijaan!

13.3.4.1 eFax-palvelu

eFax-palvelun kautta on mahdollista lähettää sähköposti ja mahdolliset tarvittavat liitetiedostot niin, että vastaanottaja saa ne perinteisessä faksimuodossa. Perusperiaate eFax-palvelun kautta lähetettävissä viesteissä on siis sama kuin suojatun sähköpostin lähettämisessä. eFax-palvelun käytössä tulee huomioida samat asiat kuin sähköpostien ja perinteisten faksien käsittelyssä. Vastaanottajatiedon kirjaaminen oikein on erittäin tärkeää, jotta välitettävä tieto päätyy halutulle vastaanottajalle.

Tietosuojavastaavan vinkit!

- Tutustu eFax-palvelun käyttöohjeeseen[117] ja kysy tarvittaessa lisätietoja Siun soten ICT-yksiköstä.
- Suosi mahdollisuuksien mukaan suojatun sähköpostin käyttöä, mikäli sellainen on mahdollista faksin sijaan!

13.3.5 Kirjeposti

Kirjeposti on osoitteellinen lähetys, josta ilmenee vastaanottajan nimi, osoite sekä mahdollisesti vastaanottajatahon organisaatio. Suomessa postin kulkua säätelee Postilaki (415/2011). Perustuslaissa (731/1999) säädetään yksityiselämän suojasta, joka koskettaa myös kirjeitä sekä muita luottamuksellisia viestejä. On hyvä tiedostaa, että pelkästään kirjekuoreen merkitty henkilö on oikeutettu avaamaan hänelle osoitetun kirjeen.

Siun sotessa käsitellään paljon salassa pidettäväksi luokiteltavaa kirjepostia, joten on kiinnitettävä huomiota myös niin lähtevän kuin saapuvankin kirjepostiin säilyttämiseen. Siun soten toimintayksiköissä on huolehdittava, että sekä lähtevän että saapuvan kirjepostin säilyttäminen tapahtuu tilassa, jossa kirjeposti ei voi joutua sivullisten

[117] Siun sote – Ohje Elisa eFax palvelun käytöstä (Siun sote intra)

käsiin. On suositeltavaa, että kirjeposti säilytetään tilassa, jonne esimerkiksi asiakkailla ei ole pääsyä. Kirjepostia voi säilyttää esimerkiksi myös lukittavassa laatikossa tai kaapissa.

Asiakirjojen käsittely paperiaineistona on herkästi haavoittuvaa työtä ja siinä voi tapahtua yllättäviäkin poikkeamia. Lähetettävän kirjeen sisällön osalta on varmistuttava siitä, että sisältö kuuluu vastaanottavalle taholle. Osoitetiedot tulee kirjata lähetykseen selkeästi, sille määrätylle paikalle. Jos postin kulku vastaanottajalle haluaa varmistaa, voi postin lähettää esimerkiksi kirjattuna kirjeenä.

Tietosuojavastaavan vinkit!

- Tutustu Siun soten saapuneiden kirjeiden käsittely ohjeeseen[118], kirjekuorien käyttöohjeeseen[119] sekä sisäisen postin lähettämisen ohjeeseen[120]
- Varmistu aina, kenen tietoja käsittelet ja käsittele vain yhden henkilön papereita kerrallaan. Useamman henkilön asiakirjat sekoittuvat helposti keskenään ja tulosteet saattavat myös ”liimautua” toisiinsa, eli käy jokainen kirjeitse lähetettävä asiakirja huolellisesti läpi.
- Varmista, että kaikki lähetettävät asiakirjat kuuluvat kyseiselle vastaanottajalle. Varsinkin tulosteiden kokoaminen pöydältä voi aiheuttaa riskin, että lähetykseen lipsahtaa sinne kuulumatonta aineistoa.
- Pyri lähettämään yhdessä kirjelähetyksessä vain yhtä henkilöä koskevat asiakirjat. Näin myös turvaat osaltasi lähetyksen vastaanottajan turvallista tietojen käsittelyä. Vaihtoehtoisesti voit postittaa yhdessä kirjelähetyksessä (isossa kirjekuoressa) samalle vastaanottajalle useampaa henkilöä koskevat asiakirjat siten, että asiakirjat ovat pakattuina henkilöittäin erillisiin pienempiin suljettuihin kirjekuoriin. Näin turvaat sekä lähetyksen vastaanottajan turvallista tietojen käsittelyä sekä säästät postituskustannuksissa. Huomioi kuitenkin, etteivät pienet kirjekuoret ole tällöin valmiiksi maksettuja kuoria, sillä niiden maksut menevät muutoin hukkaan!
- Huomioi, että kirjeiden vastaanottajan tiedot eli osoitetiedot luetaan Postissa koneellisesti. Kiinnitä huomiota, että käsin kirjoitetut osoitemerkinnät ovat oikealla paikalla kirjekuoressa ja selkeällä käsialalla kirjoitettuina.
- Sovi poissaolosi aikana sinua sijaistavan henkilön kanssa, miten sinulle osoitettua kirjepostia käsitellään poissaolosi aikana.
- Huomioithan, että ruskeat sisäisen postin kuoret ovat vain ns. lähetyskansia, joita ei ole tarkoitettu yksistään suojaamaan lähetettävää materiaalia. Asiakas- tai potilastietoja tai muita

[118] Siun sote – Saapuneiden kirjeiden käsittely (Siun sote intra)
[119] Siun sote - Kirjekuorien käyttöohje (Siun sote intra)
[120] Siun sote - Sisäisen postin lähettäminen (Siun sote intra)

henkilötietoja sisältävä asiakirja on suljettava valkoiseen kirjekuoreen ennen sen lähettämistä sisäisellä postilla. Älä kuitenkaan käytä tällöin maksettuja kirjekuoria!

13.3.6 Puhelut

Puhelimitse tapahtuva tiedonvälitys on tietoturvallista, kun huolehditaan siitä, että puhelu ohjautuu oikealle henkilölle eli varmistetaan puhelun vastaanottajan henkilöllisyys. Asiakas- ja potilaspuheluissa on siis syytä varmistua siitä, että olet tunnistanut henkilön, ennen kuin keskustelet mm. hoitoon tai palveluun liittyvistä asioista tai luovutat keskustelussa salassa pidettävää tietoa. Puheluiden turvallisuutta parantaa se, että varmistutaan, ettei puhelun aikana käytyjä keskusteluja kuule sivulliset henkilöt.

Puhelimitse tapahtuva tiedonvälitys ei sellaisenaan tallennu mihinkään, ellei sitä erikseen tarkoituksella nauhoiteta. Mikäli puhelut nauhoitetaan, sille tulee olla laissa määrätty peruste tai nauhoituksen tulee perustua asiakkaan antamaan suostumukseen. Suostumus on kysyttävä ennen nauhoituksen alkamista. Puhelun nauhoittaminen tulkitaan henkilötietojen käsittelyksi, sillä tallentuessaan ääni on henkilötieto. Tällöin puheluun osallistuneet henkilöt ovat rekisteröityjä ja heillä on tarkastusoikeus puhelunauhoitteeseen.

Asiakas voi kuitenkin nauhoittaa sellaiset puhelut, joihin itse osallistuu joko soittajana tai vastaajana. Oman viestinnän taltioiminen on Suomen perustuslain mukaan mahdollista eikä sitä ole kriminalisoitu myöskään viestinnän suojaa koskevissa rikoslain säännöksissä. Nauhoitteiden käytön lainmukaisuus arvioidaan sen perusteella, mihin tarkoitukseen sitä aiotaan käyttää ja kenen kuultavaksi se annetaan. Nauhoitteita annettaessa toisten kuultavaksi voi syyllistyä toisen kunnian loukkaamiseen, yksityiselämää koskevan tiedon levittämiseen tai salassa pidettävän tiedon paljastamiseen.

Tietosuojavastaavan vinkit!

- Tutustu asiakkaan tunnistaminen etäpalvelussa ohjeeseen[121]!
- Älä käy puhelinkeskusteluja julkisissa tiloissa, mikäli keskustelun myötä joku henkilö on tunnistettavissa tai aihe on muutoin luottamuksellinen tai salassa pidettävä.

13.3.7 Tekstiviesti

Tekstiviestejä käytetään osana Siun soten palveluja mm. asiakkaan etäasioinnissa. Tekstiviestitse on mahdollista viestiä ajanvarauksista sekä tiedottaa asiakkaita Siun soten palveluista. Tekstiviestitse voidaan kysyä myös asiakaspalautetta sekä mitata asiakaskokemusta.

[121] Siun sote - Asiakkaan tunnistaminen etäpalvelussa (Siun sote intra)

Siun sotessa asiakkaille tarkoitetut tekstiviestit perustuvat asiakkaan antamaan tekstiviestilupaan. Tekstiviestin käyttämisestä tulee siis informoida asiakasta ja merkitä asiakkaan antama lupa tai kielto asiakas- ja potilastietojärjestelmään. Siun sotessa tekstiviestejä voidaan lähettää asiakkaille asiakas- ja potilastietojärjestelmistä tai työntekijän työpuhelimesta. Tekstiviestejä lähtee lisäksi automaattisesti mm. sähköisen verkkoajanvarauksen yhteydessä, kun asiakas varaa asiointiaikaa Siun soten verkkosivuilta.

Tekstiviestissä ei saa olla asiakkaan henkilötietoja (mm. etu- ja sukunimi, henkilötunnus, puhelinnumero tai osoite). Asiakkaan etunimi voidaan tekstiviestissä mainita, jos on esimerkiksi tarve erotella huoltajalle lähtevään tekstiviestiin, kenen lapsen asiaa viesti koskee.

Siun soten työntekijöiden väliset tekstiviestit ja niiden käyttö on Siun sotessa sallittua. Tekstiviesteissä ei kuitenkaan tule käsitellä asiakas- ja potilastietoja eikä kenenkään henkilön henkilötietoja. Turhat tekstiviestit on poistettava viipymättä.

Tietosuojavastaavan vinkit!

- Tarkasta aina asiakkaan asioinnin yhteydessä asiakkaan perustiedot! Tarkasta lisäksi aina 18-vuotta täyttäneen asiakkaan perustiedot ja että tekstiviestilupaan on kirjattu henkilön itsensä puhelinnumero eikä esimerkiksi huoltajan!
- Varmistu ennen tekstiviestin lähettämistä, että asiakas on antanut luvan ja viesti on lähdössä siihen puhelinnumeroon, johon asiakas on toivonut viestin lähetettävän.
- Mediatri-tietojärjestelmässä asiakkaan antaman tekstiviestilupa näkyy Henkilön perustiedoista. ProConsona/OMNI360-tietojärjestelmässä asiakkaan antama tekstiviestilupa näkyy Hälytykset-osiossa.
- Tutustu Mediatrin tekstiviestiohjeeseen[122]!
- Asiakas voi itse hallinnoida antamaansa tekstiviestilupaa Medinet-palvelussa, joka päivittää tiedot Mediatri-tietojärjestelmään. Huomioitavaa on, että Medinet-palvelussa asiakas ei voi hallinnoida sosiaalihuollon asiakastietojärjestelmässä olevaa tekstiviestilupaa!
- Poista työpuhelimeen saapuneet tekstiviestit säännöllisesti, ettei puhelimeen kerry viestejä tarpeettomasti.
- Mediatrin PTH-käyttäjän oppaassa[123] on kuvattu, kuinka tulee toimia tilanteessa, jossa tekstiviestin on havaittu menneen väärälle henkilölle.

[122] Meita – Mediatri, Tekstiviesti (Siun sote intra)
[123] Siun sote – Tietojärjestelmäohje (Mediatri), PTH käyttäjän opas (Siun sote intra)

13.3.8 Microsoft Teams

Microsoftin Teams viestintä- ja yhteistyöalusta on käytössä Siun soten työntekijöillä. Käyttöympäristö riippuu siitä, millainen lisenssitaso työntekijällä on Microsoftin palveluihin. Teams mahdollistaa keskustelut, kokoukset, tiedostojen jakamisen, tallennuksen ja käsittelyn. Teamsia käytetään ensisijaisesti työasemasovelluksessa, mutta tilanteen vaatiessa työntekijä voi myös käyttää Teamsin mobiilisovellusta.

Tietosuojavastaavan vinkit!

- Perehdy Siun soten intrassa Teams-ohjeisiin[124]!

13.3.8.1 Teams ammattilaisten välisenä sovelluksena

Teamsia voi hyödyntää monipuolisesti työssä mm. tiedon jakamisessa sekä kokouksissa. Huomioitavaa kuitenkin on, että konsultaatioita ei saa tehdä Teamsin viestitoiminnon välityksellä, vaan ne tulisi hoitaa ensisijaisesti asiakas- ja potilastietojärjestelmien omilla toiminnallisuuksilla (mm. työviestit). Teams-viestissä voi välittää ainoastaan esimerkiksi asiakkaan Mediatrinumeron tai muun tietojärjestelmäkohtaisen asiakasnumeron ilman potilas- tai asiakastietoja mm. seuraavilla tavoilla:

- ”Med.nro 12345 aika vastaanotolle annettu”
- ”Mdnumero 12345 resepti valmis”
- ”Nro 12345 asia hoidettu”
- ”Mdnro 12345 lausunto valmis”

Teams-viestissä ei tule käsitellä esimerkiksi asiakkaan Mediatrinumeroa yhdistettyjä asiakas- ja potilastietoon mm. seuraavilla tavoilla:

- ”Med.nro 12345 kuumeilee 39 astetta, valittaa mahakipua. Hoito-ohjeet?”
- ”Med.nro 12345 keuhkokuvassa keuhkokuumeeseen sopiva löydös.”
- ”Md.nro 12345 Somac resepti kirjoitettu närästysvaivaan”
- ”Md.nro 12345 varattava aika ravitsemusterapiaan ylipainon vuoksi”

Teams-kokoustoimintoa voidaan käyttää työpaikan palavereissa ja esimerkiksi tiimipalavereissa, joissa käsitellään asiakas- ja potilastietoja. Tiedostojen jakaminen on kiellettyä, mutta asiakkaan ja potilaan asioista voi keskustella osallistujien kesken.

[124] Siun sote - Microsoft 365 ohjeet (Siun sote intra)

Tietosuojavastaavan vinkit!

- Asiakas- tai potilastietoja tai muita salassa pidettäviä tietoja ei saa tallentaa pilvipalveluun eikä jakaa Teams-viesteissä!
- Muista, että ammattilaisten välisessä viestinnässä on aina ensisijaisesti hyödynnettävä asiakas- ja potilastietojärjestelmien omia toiminnollisuuksia (mm. työviestit)!
- Huomioi, että kaikki Siun soten työntekijät eivät välttämättä käytä Teamsia päivittäin. Mikäli siis viestiisi ei vastata, ole henkilöön yhteydessä muutoin, ettei asian hoitaminen viivästy! Huomioitavaa on myös henkilöiden lomat sekä äkilliset poissaolot!
- Se mitä lyhennettä esimerkiksi Mediatrinumerosta käytetään, on sovittava yhteisesti, ettei vääriä tulkintoja viesteissä tule ammattilaisten välillä. ”Mediatrinumero” on ammattilaisille arkikielessä tunnetuin, mutta Mediatrin mainitsematta jättäminen pienentäisi numeron hyödynnettävyyden mahdollisuuksia entisestään.

13.3.8.2 Teams asiakas- ja potilastyössä

Siun soten työntekijät voivat hyödyntää Teamsia asiakas- ja potilastyössä esimerkiksi videovälitteisen etäkäynnin toteuttamiseen, huomioiden tietosuojaan ja yksityisyyteen liittyvät asiat. Keskustelun lisäksi käyttäjät pystyvät jakamaan Teamsissa näytön kuvia/tiedostoja ja lähettämään toisilleen pikaviestejä sekä tiedostoja, jotka eivät kuitenkaan saa sisältää mitään salassa pidettäviä tietoja. Riskienhallinnan näkökulmasta on hyvä tiedostaa, että asiakas saattaa tallentaa käydyn Teams-keskustelun.

Tietosuojavastaavan vinkit!

- Huomioithan, että videovälitteinen etäkäynti edellyttää aina asiakkaan suostumusta.
- Teams-kutsu videovälitteiseen etäkäyntiin tulee lähettää aina suojattuna sähköpostina.
- Tutustu etäkäynti Teamsin välityksellä ohjeeseen[125]!

13.3.9 WhatsApp

WhatsApp-pikaviestintäpalvelun voi ladata Siun soten työpuhelimelle. Palvelua voi hyödyntää, mikäli se on tarpeen työyhteisön, työkavereiden tai muun tiimin yhteisellä sopimuksella. Palvelun käytöstä ja yhteisistä pelisäännöistä on keskusteltava esihenkilön kanssa ennen käyttöönottoa. Lisäksi on sovittava siitä, mitä tietosisältöä on palvelussa turvallista jakaa ja kuinka palvelua käytetään (oma henkilökohtainen älypuhelin vs. työpuhelin). Viranomaisviestintään ja kriisiviestintään WhatsApp-palvelu ei kuitenkaan sovellu.

[125] Siunsote_TIE_OHJE_etakaynti_Teamsin_valityksella.docx (sharepoint.com)

WhatsApp-palvelu ei sovellu käytettäväksi asiakas- ja potilasviestinnässä. Asiakasta ei kuitenkaan voi estää tekemästä yhteydenottopyyntöä WhatsApp-palvelun kautta, mikäli asiakas on saanut tietoonsa työntekijän GSM-työpuhelinnumeron. Yhteydenottopyyntöön ei tule kuitenkaan vastata WhatsApp-palvelun kautta, vaan asiakkaaseen on otettava yhteyttä muutoin. Asiakkaan lähettämät viestit, mahdolliset puhelutiedot ym. on poistettava viipymättä.

Siun soten työntekijä ei voi perustaa WhatsApp-palveluun asiakasryhmää tai liittyä osalliseksi asiakkaan/asiakkaiden perustamaa ryhmää. Ryhmiin liittämisen asetuksista voi estää työpuhelimen ryhmään liittämisen, jolloin ryhmätoiminnot palvelussa estyvät.

Siun soten asiakkaat voivat perustaa oman WhatsApp-ryhmän niin halutessaan. Siun soten työntekijä ei voi olla ryhmän perustamisessa mukana, eikä tätä kannata myöskään suositella asiakkaille.

WhatsApp-palvelu ei ole Siun soten ICT-tuen hallinnassa edes työpuhelimien osalta. Mahdolliset palvelun haavoittuvuuksiin kohdistetut tietoturvapäivitykset ja versiokorjaukset on päivitettävä työpuhelimiin itse ja niiden ajantasaisuudesta tulee huolehtia. Tämä kannattaa huomioida myös silloin, mikäli palvelua käyttää omalla henkilökohtaisella älypuhelimellaan. Lisäksi WhatsApp-palvelu kerää käyttäjästä vähintään puhelinnumero- ja profiilinimitiedot, jotta palvelua voi ylipäänsä käyttää. Tämän lisäksi palvelu kerää puhelimeen tallennetut yhteystiedot, tilatiedot, hakutiedot, sijaintitiedot sekä tietoja käyttötottumuksesta (mm. milloin palvelua käytetään, miten olet vuorovaikutuksessa muiden käyttäjien kanssa ja mitä ominaisuuksia palvelussa käytät). Palvelu kerää myös laitteesta tietoja, jolla käytät palvelua (mm. laitteiston malli, käyttöjärjestelmä, akun varaustaso, IP-osoite).

Tietosuojavastaavan vinkit!

- WhatsApp-palvelun käyttö tulee olla jokaiselle vapaaehtoista, mikäli sitä halutaan hyödyntää mm. työyhteisön sisäisessä viestinnässä. Ketään ei voi pakottaa palvelun käyttöön!
- Mikäli työntekijä käyttää WhatsApp-palvelua omalla henkilökohtaisella älypuhelimellaan, hän on itse vastuussa siitä, missä työyhteisön keskusteluryhmissä hän on mukana ja kenelle hän luovuttaa henkilökohtaisia tietojaan (mm. puhelinnumero).
- Työyhteisön WhatsApp-ryhmissä tai keskusteluissa ei tule käsitellä Siun sotea koskevia luottamuksellisia tai salassa pidettäviä tietoja. Palvelun välityksellä ei ole suositeltavaa jakaa myöskään työvuorolistoja tai muuta, josta käyvät ilmi työntekijöiden henkilötiedot.
- Työyhteisön WhatsApp-ryhmissä tai keskusteluissa ei tule käsitellä asiakas- ja potilastietoja (mm. varattuja aikoja, asiakaslistoja tai muuta, joista ilmenee asiakkaiden henkilöllisyys tai heidän terveydentilaansa tai palvelun toteuttamiseen liittyviä tietoja).
- Eettisestä näkökulmasta on suositeltavaa myös pohtia, onko asiakas- ja potilastyöstä järkevää ottaa kuvaa tai videota, vaikka niissä ei esiintyisi tunnistettavia henkilöitä. Älä siis kuvaa ja jaa eteenpäin mm. mielenkiintoisia haavoja tai leikkausalueita omaksi tai työyhteisön iloksi!
- WhatsApp-palvelua (mm. viestit, puhelut, videopuhelut) ei saa käyttää asiakas- ja potilasviestinnässä!

- Huomioithan, että vaikka WhatsApp-palvelun viestintä on salattua, palvelussa tietojen varmuuskopiointi, päätelaitteen vaihtuminen ja tietojen siirto toiselle laitteelle ovat tilanteita, jossa palvelun sisältämä tieto on tallennettuna jossain päin maailmaa salaamattomassa muodossa ja palvelun toimittajalla on niihin vapaa pääsy.
- Kaikki lähetetyt viestit poistuvat WhatsApp-palvelimilta, mutta toimittamattomat viestit säilyvät 30vrk!

13.3.10 Signal-viestisovellus

Signal-viestisovelluksen voi ladata Siun soten työpuhelimille. Signal ei kerää käyttäjätietoa sovelluksen käyttäjästä, eikä se hyödynnä käyttäjän tietoja kaupalliseen tarkoitukseen. Signalissa ei ole myöskään mainoksia, eikä se käytä markkinointikumppaneita tai seurantaevästeitä. Signal-viestit eivät myöskään tallennu palvelimelle. Signal-sovellusta käytettäessä tulee huomioida sovelluksen lukitus. Sovellukseen tulee asettaa sormenjälki- tai PIN-koodilukitus.

Tietosuojavastaavan vinkit!

- Signal on Siun sotessa viranomaiskäyttöön soveltuva viestisovellus, jota mm. johtoryhmä hyödyntää. Kriisiviestintään käytössä on Secapp-sovellus.
- Signal-sovelluksen voi asentaa myös laitteille, jotka käyttävät julkisen hallinnon turvallisuusverkkoa (TUVE).
- Huomioithan, että voit tarvittaessa estää kuvakaappausten ottamisen sovelluksessa!

13.3.11 Sähköinen asiointi

Sähköinen asiointi on vaihtoehto kasvokkain tai puhelimitse tapahtuvalle asioiden hoitamiselle. Asiakkaan näkökulmasta sähköinen asiointi on asioiden hoitamista mm. viranomaisen kanssa sähköisiä kanavia, palveluja ja tietojärjestelmiä käyttäen. Sosiaali- ja terveydenhuollossa sähköiset asiointikanavat kehittyvät jatkuvasti ja niistä on tulossa osa palvelujärjestelmän arkea yhä tiiviimmin.

Sähköinen asiointi edellyttää sähköistä tunnistautumista palveluun, jossa henkilö todentaa henkilöllisyytensä vahvalla tunnistamisella. Joihinkin verkkopalveluihin voi myös riittää ns. kevyt tunnistautuminen käyttäjätunnus-salasanaparilla.

Sähköisen asioinnin avulla asiakas voi saada ohjausta ja neuvontaa, hän voi hakeutua palveluihin ja niiden suunnitteluun, sähköinen asiointi voi myös olla osa palvelun toteutusta, tukipalvelua tai se voi tukea omahoitoa. Sähköisessä asioinnissa myös palautteen antaminen on mahdollista. Siun sotella on käytössä mm. seuraavat sähköiset asiointipalvelut:

- Miunpalvelut, sähköinen asiointipalvelu mm. hakemuksille.
- Kanta-palvelut (asiakkaille Oma-Kanta), valtakunnallinen palvelu
- Omaolo-palvelut

- Medinet-terveyspalvelu
- Verkkoajanvaraus
- Suomi.fi.

Tietosuojavastaavan vinkit!

- Muista arvioida aina sähköisen asioinnin soveltuvuus asiakkaalle! Tarjoa asiakkaalle ohjausta ja neuvontaa, älä oleta kaikkien asiakkaiden osaavan itsenäisesti hyödyntää tai käyttää erilaisia asiointikanavia.
- Ammattilaisen kannattaa myös itse tutustua tarjolla oleviin sähköisiin asiointipalveluihin, jotta asiakasohjaus ja -neuvonta tarvittaessa onnistuu! Palveluja on myös hyvä ajoittain arvioida asiakkaan näkökulmasta, jotta ne palvelisivat mahdollisimman monipuolisesti erilaisia asiakkaita!
- Asiakkaille ohjeita puolesta-asiointiin löytyy mm. Kanta-palvelusta[126] sekä Suomi.fi-palvelusta[127].
- Tutustu alaikäisen tietojen käsittely sähköisessä asioinnissa -toimintaohjeeseen[128]!

13.3.12 Etäkäynnit ja etäkonsultaatiot

Etäkäynnillä tarkoitetaan vastaanottoa tai muuta palvelua, joka tapahtuu asiakkaan ja ammattilaisen välillä reaaliaikaisesti videon välityksellä tai puhelimitse. Etäkäynti perustuu aina asiakkaan antamaan etäkäyntilupaan. Etäkäynti soveltuu kiireetöntä asiointia vaativiin tilanteisiin. Tärkeintä on arvioida aina yksilöllisesti ja huolellisesti, soveltuuko asiakkaan asia hoidettavaksi alusta alkaen etänä vai tuleeko esimerkiksi ensikäynti toteuttaa lähivastaanottona. Mikäli etäkäynnin aikana ilmenisi tarve asiakkaan lähivastaanotolle, se on asiakkaalle järjestettävä.

Annettaessa etäpalveluja, tulee varmistua siitä, että niin ammattilaisella kuin asiakkaalla on käytettävissään tarvittavat laitteet ja yhteydet. Ammattilaisen näkökulmasta tulee huomioida lisäksi tilat sekä riittävä perehdytys ja ohjeistus. Vastuu etäpalvelujen tietosuojasta ja tietoturvasta on Siun sotella. Etäkäynneistä kirjataan asiaankuuluvat asiakas- ja potilastietomerkinnät. Merkinnöissä tulee käydä ilmi, että asiakkaan hoito tai palvelu on toteutettu etänä ja että kuinka asiakkaan henkilöllisyys on tunnistettu asioinnissa.

Etäkonsultaatiot mahdollistavat mm. ammattilaisten väliset konsultaatiot asiakkaiden asioissa. Etäkonsultaation muotoja ovat mm. puhelinkeskustelut, videovälitteiset tapaamiset tai etäkonsultaatioihin käytössä olevat tietojärjestelmät tai sovellukset. Etäkonsultaatioissa on tietosuojan näkökulmasta huomioitava aina asiakkaan yksityisyyden suoja sekä se, että asiakkaan tietoja käsitellään aina luottamuksellisesti ja konsultaation on

[126] Kanta-palvelut – Asiointi toisen puolesta
[127] Suomi.fi – Henkilön puolesta asiointi
[128] Siun sote – Alaikäisen tietojen käsittely sähköisessä asioinnissa (Siun sote intra)

perustuttava olemassa olevaan hoitosuhteeseen. Läpinäkyvyyden ja avoimuuden näkökulmasta on lisäksi huomioitava, että konsultaatiosta voi olla hyvä myös kertoa asiakkaalle itselleen.

Etäkonsultaatiomuodot mahdollistavat joustavaa asiakkaan asian hoitamista, riippumatta henkilöiden fyysisestä sijainnista. Ammattilainen voi siis tehdä työtä myös etänä, jolloin on hyvä huomioida etätyöhön liittyvät tietosuoja ja tietoturva-asiat sekä varmistua siitä, että etätyöhön käytetty fyysinen tila vastaa työlle asetettuja vaatimuksia.

Tietosuojavastaavan vinkit!

- Mikäli olet suunnittelemassa etäkäyntien tai etäkonsultaation käyttöönottoa yksikössä, tutustu Siun soten intrasta käyttöönoton prosessiin[129] sekä etäkäynteihin liittyviin ohjeistuksiin[130][131][132][133].
- Tutustu asiakkaan tunnistaminen etäpalveluissa ohjeeseen[134].
- Etäkäynneistä on suositeltavaa tehdä yksiköihin toimintamallit, joka kuvaa kaikki etäkäyntien toteutuksen vaiheet ja toteuttamiseen liittyvät ohjeet. Toimintamalleissa on syytä kiinnittää huomiota myös mahdollisiin riskeihin ja varautuminen poikkeamatilanteisiin.
- Tutustu Valviran ohjeistuksiin terveydenhuollon etäpalvelujen osalta[135].

13.3.13 Sosiaalinen media

Sosiaalinen media eli some on osa Siun soten julkista verkkoviestintää. Siun soten käytössä olevia sosiaalisen median pääkanavia hallinnoi Siun soten Viestintä. Viestintä tuottaa myös ohjeet ja toimintaperiaatteet sosiaalisen median palvelujen käyttöön ja käytössä huomioitaviin asioihin, mikäli sosiaalisen median kanavia käytetään työyksiköissä. Ohjeet ja periaatteet tulee huomioida myös toimialuekohtaisissa viestintäsuunnitelmissa.

Sosiaalisessa mediassa toimiminen edellyttää työtehtäviin liittyvien salassapitovelvoitteiden, asiallisen käyttäytymis- ja vuorovaikutustavan sekä Siun soten eettisten periaatteiden ja eri ammattialojen eettisten ohjeiden noudattamista. Jokainen sosiaalisen median käyttäjä vastaa omasta toiminnastaan. Mikäli sosiaalisen median kanavia käytetään työyksiköissä, käytänteitä on hyvä tarkastaa ajoittain ja sopia yhteisistä pelisäännöistä, jotta sosiaalisen median käyttö työssä on laadukasta ja hallittua, eikä siitä aiheudu ongelmia tai väärinkäytöksiä.

---

[129] Siun sote – Etäkäynti ja etäkonsultaatio (Siun sote intra)
[130] Siun sote – Ohje työntekijälle: Etäkäynti Teamsin välityksellä (Siun sote intra)
[131] Siun sote – Ohje asiakkaalle: Etäkäynti Teamsin välityksellä (Siun sote intra)
[132] Siun sote – Ohje työntekijälle: Etäryhmäkäynti Teamsin välityksellä (Siun sote intra)
[133] Siun sote – Ohje asiakkaalle: Etäryhmäkäynti Teamsin välityksellä (Siun sote intra)
[134] Siun sote – Asiakkaan tunnistaminen etäpalvelussa (Siun sote intra)
[135] Valvira - Etäpalvelut

Toimintayksiköiden esihenkilöt ovat vastuussa sosiaalisen median käytöstä toimintayksiköissä, sekä riittävästä perehdytyksestä ja valvonnasta. Jokaisen työntekijän ja esihenkilön velvollisuus on puuttua ja tuoda esille havaittu epäkohta.

Siun soten omien viestintäkanavien lisäksi sosiaalinen media voi olla läsnä myös työntekijöiden omassa henkilökohtaisessa arjessa. Mikäli työntekijä ilmaisee omassa henkilöprofiilissaan työnantajansa tiedot, esiintyy hän tällöin myös työnantajan epävirallisena edustajana.

Tietosuojavastaavan vinkit!

- Sosiaalisessa mediassa jaettuun sisältöön tulee aina suhtautua siten kuin se olisi täysin julkista. Vaikka sisältöä julkaistaisiin vain rajatulle ryhmälle, se voidaan aina kopioida, tallentaa, tulostaa ja jakaa näin edelleen ulkopuolisille. On myös huomioitava, että some-palveluntarjoaja voi muuttaa halutessaan palvelun käyttöehtoja, jolloin rajatulle ryhmälle suunnattu sisältö voikin myöhemmin muuttua julkiseksi!
- Tutustu Siun soten sosiaalisen median kanaviin, niiden käyttötarkoituksiin sekä ohjeisiin Siun soten intrassa[136]!
- Muista, että työaika ja työvälineet ovat tarkoitettu työtehtävien hoitamiseen. Työaikana somettaa voi pelkästään silloin, kun se kuuluu työtehtäviin!
- Työntekijän yleinen lojaliteettivelvoite työnantajaa kohtaan ulottuu myös vapaa-ajalle! Suositeltavaa on siis käydä työpaikkaa koskevat keskustelut mieluummin työpaikalla kuin somessa ja puhua työnantajasta sekä työyhteisöstä asiallisesti, salassapitovelvollisuutta noudattaen!
- Älä vaaranna omalla some-käytökselläsi Siun soten asiakkaiden ja potilaiden yksityisyydensuojaa!
- Muista, että Siun soten eri toimipisteissä kuvaaminen on pääsääntöisesti rajoitettua. Et siis voi täysin vapaasti ottaa työpaikaltasi kuvia ja jakaa niitä somessa!
- Sosiaalinen media on hyvä kanava verkostoitua mm. ammattilaisten kesken ja siellä voi tuoda esille asiantuntemustaan. Työntekijän tulee kuitenkin aina erottaa sosiaalisen median eri näkökulmat: toimiiko somessa yksityishenkilönä, työnantajan, työyhteisön tai ammattikunnan edustajana.
- Mikäli asiakas pyytää sinua liittymään some-verkostoonsa, ole tarkkana, ettei verkostoituminen vaaranna asiakkaan ja ammattilaisen välisen hoito- ja palvelusuhteen puolueettomuutta, asianmukaisuutta tai aiheuta väärinkäsityksiä toiminnastasi sosiaali- tai terveydenhuollon ammattihenkilönä.

[136] Siun sote – Sosiaalinen media (Siun sote intra)

- Huolehdi sosiaalisessa mediassa myös omasta, perheesi sekä läheistesi yksityisyydestä: pohdi tarkkaan mitä tietoja ja kuvia haluat jakaa omasta henkilökohtaisesta elämästäsi ja kenelle. Pohdi myös, mihin kaikkeen annat palvelulle luvan, kun rekisteröidyt palvelun käyttäjäksi. Mitä tiukemmiksi säädät asetukset, sitä paremmin hallitset omia tietojasi!

13.3.14 Asiakirjojen salassapitomerkinnät ja turvallisuusluokitukset

Asiakirjojen salassa pitämisen perusteena voi olla esimerkiksi se, että asiakirja sisältää tietoja, joilla on laissa säädetty vaitiolovelvollisuus. Salassa pitämisen perusteita kuvataan tarkemmin julkisuuslaissa. Viranomaisen asiakirjaan on tehtävä merkintä asiakirjan salassa pitämisestä. Merkinnästä on käytävä ilmi, miltä osin asiakirja on salassa pidettävä sekä se, mihin salassa pitäminen perustuu.

Myös muuhun kuin lain mukaan salassa pidettävään asiakirjaan voidaan tehdä merkintä, esimerkiksi tilanteissa, joissa viranomainen käyttää asiakirjan luovuttamisessa omaa harkintaa. Tällöin merkintä on *”harkinnanvaraisesti annettava”*. Tällöinkin merkinnästä on käytävä ilmi, mihin määrittely perustuu.

Turvallisuusluokiteltavat asiakirjat jaetaan tiedonhallintalain mukaisesti seuraaviin turvallisuusluokkiin, josta on myös säädetty valtioneuvoston asetuksessa asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019):

- **Turvallisuusluokka I eli TL I** asiakirjat sisältävät salassa pidettävää tietoa, jonka oikeudeton paljastuminen tai käyttö voi aiheuttaa erityisen suurta vahinkoa. Tämän luokan asiakirjaan tehdään turvallisuusluokituksen merkinnän lisäksi merkintä *”erittäin salainen”*.
- **Turvallisuusluokka II eli TL II** asiakirjat sisältävät salassa pidettävää tietoa, jonka oikeudeton paljastuminen tai käyttö voi aiheuttaa merkittävää vahinkoa. Tämän luokan asiakirjaan tehdään turvallisuusluokituksen merkinnän lisäksi merkintä *”salainen”*.
- **Turvallisuusluokka III eli TL III** asiakirjat sisältävät salassa pidettävää tietoa, jonka oikeudeton paljastuminen tai käyttö voi aiheuttaa vahinkoa. Tämän luokan asiakirjaan tehdään turvallisuusluokituksen merkinnän lisäksi merkintä *”luottamuksellinen”*.
- **Turvallisuusluokka IV eli TL IV** asiakirjat sisältävät salassa pidettävää tietoa, jonka oikeudeton paljastuminen tai käyttö voi aiheuttaa lievää vahinkoa. Tämän luokan asiakirjaan tehdään turvallisuusluokituksen merkinnän lisäksi merkintä *”käyttö rajoitettu”*.

Turvallisuusluokitelluille asiakirjoille on myös omat tietojärjestelmiä ja tietoliikennejärjestelyjä koskevat vaatimukset, jotka tulee huomioida käsiteltäessä turvallisuusluokiteltuja tietoja. Tiedoille on myös asetettu rajoitteita liittyen asiakirjojen kopiointiin, lähettämiseen kirjeenä, siirtämiseen tietoverkossa sekä hävittämistä koskien. Asiakirjoissa voi olla lisäksi *”LIMITE”*-merkintä. Se ei osoita asiakirjan turvallisuusluokitusta, vaan se on EU:n sisäinen asiakirjan jakelurajoitetta osoittava merkintä.

Tietosuojavastaavan vinkit!

- Tunnista asiakirjojen salassapitoa ja turvallisuusluokittelua sekä jakelurajoitteita ilmaisevat merkinnät ja huolehdi, että käsittelet merkittyjä tietoja huolellisesti sekä ohjeistuksien mukaisesti!

13.3.15 Skannaaminen ja asiakirjojen kopiointi

Skannaamisella tarkoitetaan paperisen asiakirjan muuntamista digitaaliseen muotoon. Osa skannattavista asiakirjoista voi sisältää salassa pidettäviä tietoja, kuten asiakas- ja potilastietoja, muita henkilötietoja tai liikesalaisuuksia. Salassa pidettävät tietoaineistot tulee skannata tietoturvallisesti, valiten tietoaineiston mukaisen tallennuspaikan.

Asiakirjoja kopioitaessa asiakirjoja tulee käsitellä samoin kuin alkuperäisä asiakirjoja. Mikäli asiakirja sisältää salassa pidettävää tietoa, siitä voidaan ottaa sekä sähköisiä että paperimuotoisia kopioita. Salassa pidettäviä tietoja kopioitaessa tulee huolehtia kopiointiin käytettyjen laitteiden turvallisuudesta sekä kopioiden tietoturvallisesta säilyttämisestä ja jatkokäytöstä.

Tietosuojavastaavan vinkit!

- Tutustu Meitan ohjeeseen Mediatri-skannauksesta[137] ja pyydä apua tarvittaessa tietojärjestelmän pääkäyttäjiltä. Muiden asiakas- ja potilastietojärjestelmien osalta saat myös lisätietoja pääkäyttäjiltä!
- Työntekijä voi skannata asiakirjan myös suoraan omaan sähköpostiinsa. Tällöin on huolehdittava siitä, että sähköpostissa tietoaineistoa käsitellään turvallisesti!
- Muista, että tekijänoikeuslailla suojattuja materiaaleja ovat mm. kirjat, lehdet, valokuvat, tutkimusraportit ja muut julkaisut! Näiden kopiointiin ja sähköiseen jakamiseen tai tallentamiseen tarvitaan tekijänoikeudenhaltijan lupa.
- Asiakirjoja tulee kopioida ja skannata vain tarpeeseen Vältä turhia kopioita tai skannailuja ja arvioi myös aina riskit, huomioiden tietoaineiston sisältö!

13.3.16 Tulostaminen ja turvatulostus

Siun sotessa tulostimet hankitaan OfficePro:lta ja tulostamisesta muodostuvat kustannukset perustuvat käyttömääriin. Tulostimet voivat olla myös ns. yhteiskäyttöisiä, jolloin samaa tulostinta käyttävät useat työntekijät tai jopa useat eri toimintayksiköt. Ennen tulostamista on ehdottoman tärkeää tarkastaa, mille tulostimelle työasemalta tulostetut asiakirjat ohjautuvat. Jokainen käyttäjä on velvollinen tarkastamaan työasemalle

[137] Meita - Mediatri skannaus (Siun sote intra)

määritellyn tulostimen tiedot ja niiden oikeellisuuden ennen asiakirjojen tulostamista. Mikäli tulostusasetukset ovat väärin (mm. oletustulostimena on muu kuin yksikön käyttöön määritelty tulostin) on asetuksia muutettava.

Siun sotessa on mahdollista käyttää myös turvatulostusta. Turvatulostus mahdollistaa asiakirjojen tulostamisen miltä tahansa työasemalta turvatulostusjonoon ja tulostustyön voi vapauttaa miltä tahansa tulostimelta, joka on määritelty turvatulostuksen monitoimilaitteeksi. Turvatulostus vaatii käyttäjältä henkilökohtaisen turvatulostuslätkän, joka toimii tulostustyön vapauttajana tulostuslaitteilla. Mikäli on tarve tulostaa esimerkiksi asiakas- ja potilastietoja tai henkilötietoja sisältäviä tietoaineistoja yhteiskäyttöiselle tulostimelle, tulee käyttää turvatulostusta. Tällöin tulosteet tulostuvat vasta, kun käyttäjä antaa tulostimelle turvatulostuslätkällä tulostusluvan.

Tietosuojavastaavan vinkit!

- Nouda tulostamasi asiakirjat viipymättä tulostamisen jälkeen!
- Saat lisätietoja tulostamisesta, turvatulostamisesta, tulostuslaitteista sekä tulostusympäristön muuttumiseen liittyvissä asioissa (mm. yksikkö vaihtaa sijaintia tai toimipisteen toiminta päättyy) Siun soten ICT-yksiköstä[138] tai OfficeProlta (tuki.officepfo.fi).
- Yhteiskäyttöisissä tulostimissa on tärkeää, että käyttäjät täydentävät asiakirjoja tulostaessa ja kopioitaessa ns. tilikirjauksen yhteyteen yksikkönsä kustannuspaikkatiedon! Tällöin myös laitteiden käytöstä muodostuvat kustannukset ohjautuvat oikein.
- Vältä ylimääräistä tulostamista, sillä ylimääräiset tulosteet kustannus- ja ympäristövaikutusten ohella lisäävät riskiä siihen, että tiedot joutuvat vääriin käsiin. Ylimääräisiä paperisia asiakirjoja ei saa myöskään tarpeettomasti säilyttää työpisteellä tai työhuoneessa!
- Kun on tarve tulostaa asiakas- ja potilastietoja tai henkilötietoja sisältävää tietoaineistoa yhteiskäyttöiselle tulostimelle, tulee käyttää turvatulostusta! Silloin asiakirjat tulostuvat vasta, kun tulostimelle antaa laitteen äärellä tulostusluvan. Tulostusluvan antamisen jälkeen, odota, että kaikki tulosteesi ovat tulostuneet ja huolehdi, että otat mukaasi kaikki sinulle kuuluvat tulosteet. Älä poistu tulostimen ääreltä kesken tulostamisen!
- Muista, että turvatulostuslätkä on henkilökohtainen ja se on liitetty käyttäjän omaan verkkotunnukseen! Huolehdi turvatulostuslätkästäsi yhtä huolellisesti kuin esimerkiksi käyttäjätunnuksistasi, salasanoistasi ja toimikortistasi! Mikäli turvatulostuslätkäsi häviää, ilmoita asiasta viipymättä esihenkilöllesi!

[138] Siun sote - ICT-laitteet ja -hankinnat (Siun sote intra)

13.3.17 Kuvaaminen Siun sotessa

Siun soten aulat, odotustilat, kahviot ja toimitilojen ulkoalueet ovat julkisia tiloja, joissa kuvaamiselle ei tarvitse erillistä lupaa. Julkisilla paikoilla tulee kuitenkin huomioida muiden henkilöiden oikeus yksityisyyteen, eli toisten henkilöiden kuvaaminen julkisilla paikoillakin tarvitsee luvan.

Siun soten muut tilat eivät ole julkisia ja tiloilla on oma käyttötarkoituksensa sekä käyttäjänsä. Kuvaaminen muissa kuin julkisissa tiloissa vaatii aina erillisen kuvausluvan. On lisäksi suotavaa, että kuvattavilta henkilöiltä pyydetään myös erilliset suostumukset, mikäli kuvissa esiintyy muita henkilöitä (mm. työntekijät, asiakkaat, vierailijat). Suostumus voi olla tilanteen mukaan suullinen tai kirjallinen. Kirjallinen suostumus tarvitaan tilanteissa, joissa kuvat tai videot on tarkoitus julkaista.

Omaa tai läheisen hoito- tai palvelutilannetta, hoitokeskustelua, vastaanottoa tai vastaavaa käyntiä saa pääsääntöisesti kuvata tai videoida. Asiakas- ja potilastyö tulee tehdä aina niin hyvin ja laadukkaasti, että se kestää tarvittaessa myös julkisen tarkastelun. Asiakasta tai läheistä voidaan kuitenkin pyytää lopettamaan kuvaus tai videointi hoitotoimenpiteiden ajaksi.

On olemassa joitakin poikkeuksia oman tai läheisen hoidon kuvaamiselle. Esimerkiksi mielenterveyslaissa (1116/1990) voi olla säädöksiä, joilla rajoitetaan asiakkaan oikeuksia. Tällöin oman tai läheisen hoidon kuvaaminen ei ole mahdollista. Myös asiakas- ja potilasturvallisuus voi asettaa rajoituksia erilaisten laitteiden käytölle (mm. älypuhelin tai tabletti).

Tietosuojavastaavan vinkit!

- Muista, että jokaisella asiakkaalla, vierailijalla sekä työntekijällä on oikeus yksityisyyteen!
- Huomioi, että asiakkaita, vierailijoita ja työntekijöitä koskevat samat kuvaamiseen liittyvät säännöt ja ohjeet! Työntekijöillä tai esimerkiksi opiskelijoilla ei ole siis erityisoikeuksia!
- Tutustu Siun soten kuvaamiseen liittyviin ohjeisiin sekä tarvittaviin kuvauslupakäytänteisiin[139]!
- Muista kuvaukseen liittyvän suostumuksen osalta arvioida, onko henkilö itse kykenevä antamaan lupaa ja ymmärtämään mihin tarkoitukseen lupaa pyydetään, ja mitkä ovat kuvien käyttötarkoitukset sekä julkaisupaikat! Esimerkiksi alaikäinen henkilö, muistisairashenkilö tai kehitysvammainen henkilö ei useinkaan voi olla itse suostumuksen antaja!
- Mikäli kuvia käytetään Siun sotessa viestinnän- tai markkinoinnintarkoituksiin, kuvissa esiintyviltä henkilöiltä pyydetään aina kirjallinen suostumus.
- Asiakkaille ja vierailijoille kuvaamiseen liittyvät ohjeet ovat saatavilla Siun soten verkkosivuilta[140].

[139] Siun sote – Kuvaaminen (Siun sote intra)
[140] Siun sote – Potilaille ja läheisille

- Medialle kuvaamiseen liittyvät ohjeet ovat saatavilla Siun soten verkkosivuilla[141].
- Dronen lennättämiseen Pohjois-Karjalan keskussairaalan alueella tarvitsee aina luvan! Lue lisää Siun soten verkkosivuilta[142] sekä Traficomin Droneinfosta[143].

13.4 Tiedon asianmukainen hävittäminen

Kun tietojen käyttötarkoitus tai arkistointivelvoite päättyy, tarpeeton tieto tulee hävittää asianmukaisesti. Henkilötietoja sisältävien tietojen säilytyksen tulee aina perustua ennalta määritettyyn käyttötarkoitukseen ja niiden tarpeeton säilyttäminen on kielletty. Ennen tietojen hävittämistä tulee aina varmistua siitä, ettei tiedolle ole arkistointivelvoitetta ja varmistuttava siitä, kuinka pitkä tietojen arkistointivelvoite kulloinkin on. Tietojen asianmukaisessa hävittämisessä tulee huomioida lisäksi tietoaineiston muoto sekä sisältö.

Tietosuojavastaavan vinkit!

- Muista, että tiedon asianmukaisen hävittämistavan arviointiin vaikuttaa tiedonmuoto ja tietosisältö. Mitä luottamuksellisempaa tieto on tai jos se sisältää henkilötietoja, sen enemmän hävittämistapaan tulee kiinnittää huomiota!
- Jokainen työntekijä on itse velvollinen laittamaan esimerkiksi potilas- ja asiakastietoja sisältävät paperiset asiakirjat tietosuojajäteastiaan! Älä oleta, että ”joku” hoitaa asian puolestasi!
- Toimintayksikön esihenkilön vastuulla on arvioida, onko yksikössä käytössä sen toiminnan ja käsiteltävien tietojen kannalta riittävät tietosuojajäteasiat ja että jäteastioiden säännöllinen tyhjennys on sovittu asianmukaisesti. Tutustu Siun soten jäteohjeeseen[144] ja muihin jätehuoltoon liittyviin materiaaleihin[145].
- Huomioi, että esimerkiksi lääkkeiden annosjakelupussit sisältävät henkilötietoja sekä asiakkaan lääkitystietoa! Älä hävitä annosjakelupusseja sekajätteen mukana ennen niiden silppuamista. Ohjaa oikea toimintamalli tarvittaessa myös asiakkaille ja heidän läheisilleen!
- Älä hävitä rikkimennyttä ja toimimatonta työnantajan laitetta (mm. työpuhelin) omatoimisesti. Laite tulee toimittaa Meitalle ja laitteen tiedot on poistettava laiterekisteristä esihenkilön toimesta.
- Tutustu Siun soten tietoaineiston luokittelu- ja käsittelyohjeeseen[146]!

[141] Siun sote - Medialle
[142] Siun sote - Medialle
[143] Traficom – Droneinfo, Missä ei saa lennättää?
[144] Siun sote – Jäteohje (Siun sote intra)
[145] Siun sote – Jätehuolto (Siun sote intra)
[146] Siun sote – Tietoaineiston luokittelu- ja käsittelyohje (Siun sote intra)

- Tutustu Siun soten tiedonohjaussuunnitelmaan sekä säilytysaikojen ja arkistoinnin ohjeisiin[147]! Muista tehdä myös hävitysesitys paperiasiakirjoista[148] tiedonhallintapäällikölle tarvittaessa!

14 Tietoturvan osa-alueet

Tietoturva mielletään usein teknisinä toimina, esimerkiksi palomuureina sekä virustentorjuntaohjelmina. Tietoturva on kuitenkin kokonaisuus, joka muodostuu erilaisista osa-alueista.

Tietoturvalla tarkoitetaan sekä hallinnollisia että teknisiä toimia, joilla varmistetaan tiedon

- **luottamuksellisuus** eli se, että tiedot ovat vain niiden käyttöön oikeutettujen saatavilla,
- **eheys** eli se, että tietoja eivät voi muuttaa muut kuin siihen oikeutetut sekä
- **käytettävyys** eli se, että tiedot ja tietojärjestelmät ovat niiden käyttöön oikeutettujen hyödynnettävissä.

14.1 Hallinnollinen tietoturva

Tietoturvallisuutta tukevat toimintatavat tarvitsevat johtamista ja kehittämistä samoin kuten muutkin Siun soten toimintaprosessit sekä palvelut. Hallinnollinen tietoturva sisältää menettelytavat muiden tietoturvan osa-alueiden ohjaamiseen ja sen tavoitteena on varmistaa, että kaikki osa-alueet ovat riittävän hyvällä tasolla. Hallinnolliseen tietoturvaan liittyy olennaisena osana myös riskien arviointi, jonka avulla pyritään löytämään hallintakeinoja, joiden avulla vältetään tietoturvaan liittyvät vahingot.

Hallinnollisen tietoturvan näkyvimpiä tuotoksia ovat henkilöstön organisointi, yleiset linjaukset sekä erilaiset dokumentaatiot mm. Siun soten tietoturvapolitiikka ja tietoturvasuunnitelma. Hallinnollisen tietoturvan vastuu on Siun sotessa turvallisuuspäälliköllä.

14.2 Henkilöstön tietoturvaosaaminen

Henkilöstön tietoturvaosaamista tuetaan ja kehitetään Siun sotessa tietoturvaohjein ja koulutuksin. Henkilöstön osaaminen on yksi merkittävimmistä tietoturvan tekijöistä. Jokaisen työntekijän on tärkeää kehittää omaa osaamistaan tietosuojaan ja tietoturvaan liittyvissä asioissa ja osaamisen kehittämistä on työnantajan myös tuettava.

[147] Siun sote – Säilytysajat ja arkistointi (Siun sote intra)
[148] Siun sote – Hävitysesitys (Siun sote intra)

14.3 Toimitilojen tietoturva

Siun soten tilat on luokiteltu eri turvallisuustasojen mukaisesti ja tiloihin on asetettu kulunvalvontaa, kameravalvontaa sekä asianmukaiset lukitusjärjestelmät. Toimitilojen turvallisuutta varmistetaan myös vartioinnilla ja palo-, vesi-, sähkö-, ilmastointi- ja murtovahinkojen torjunnalla.

Tietosuojavastaavan vinkit!

- Lukitse työhuoneesi ovi aina poistuessasi työpisteestäsi.
- Ohjaa vierailijat oikeisiin paikkoihin ja ohjeista eksyneitä henkilöitä löytämään oikeaan paikkaan. Älä päästä koskaan päästä sivullisia tai tuntemattomia henkilöitä Siun soten toimitiloihin esimerkiksi ilta-aikaan töistä lähtiessäsi.
- Älä jätä kulunvalvonnassa olevia tai muuten suljettuina pidettäväksi tarkoitettuja ovia auki.

14.4 Laitteiden tietoturva

Työssä käytettävien laitteiden ja välineiden on oltava käyttötarkoitukseen sopivia ja niiden päivittämisestä on huolehdittava asianmukaisesti. Laitteistoturvallisuuden keinoin turvataan laitteiston elinkaarta ja pyritään varmistamaan erilaisin tukipalveluin ja sopimuksin, että tekniset laitteet on suojattu, asennettu, ylläpidetty ja ne poistetaan käytöstä asianmukaisesti.

Liikkuvaa työtä tehtäessä on hyvä huomioida, että julkiset WiFi-yhteydet mm. kahviloissa, lentokentillä ja hotelleissa sisältävät aina riskejä. Niiden verkkojen turvallisuus on usein heikko, ellei jopa olematon. Kyberrikolliset tiedostavat nämä heikkoudet ja siitä syystä julkisten WiFi-yhteyksien käyttöä ei suositella missään tilanteissa Siun soten työasemissa tai muissa laitteissa (mm. työpuhelimet).

Tietosuojavastaavan vinkit!

- Älä jätä kannettavaa työasemaa tai työpuhelinta ilman valvontaa. Mikäli laite häviää tai varastetaan, ilmoita asiasta viipymättä esihenkilöllesi sekä Siun soten turvallisuuspäällikölle!

14.5 Ohjelmistojen tietoturva

Siun soten laitteissa tulee olla asennettuna vain Siun soten toiminnan kannalta tarpeelliset ja Siun soten hyväksymät ohjelmistot ja palvelut. Ohjelmistoturvallisuuden tavoitteena on tietosuojan ja tietoturvan toteutuminen tietojärjestelmissä koko niiden elinkaaren ajan. Sekä ammattilaisten työskentely että asiakkaiden asiointi siirtyvät yhä enemmän digitaaliseen ympäristöön, jolloin ohjelmistoturvallisuudesta huolehtiminen on keskeinen edellytys tietojen turvalliselle käsittelylle ja henkilöiden yksityisyyden suojaamiselle.

Ohjelmistoturvallisuuteen liittyy myös olennaisena osana käyttäjähallinta ja käyttöoikeuksien määrittely. Ohjelmistojen osalta on lisäksi huolehdittava siitä, että käyttäjien vahvaan tunnistautuminen on varmistettu. Tämä on tärkeää etenkin, jos ohjelmistossa tai tietojärjestelmässä käsitellään asiakas- ja potilastietoja, henkilötietoja tai muita arkaluonteisia tai salassa pidettäviä tietoja.

14.6 Tietoliikenteen turvallisuus

Tietoliikenneturvallisuuden tavoitteena on tietoliikenneverkossa liikkuvan tiedon eheyden, luottamuksellisuuden ja saatavuuden turvaaminen erilaisin fyysisin ja teknisin keinoin, esimerkiksi tietoliikennelaitteiston tietoturvamekanismien (mm. segmentoinnit, palomuurit, salaukset) avulla, verkkojen valvonnalla sekä ongelma- ja häiriötilanteisiin varautumisella. Siun sotessa käytetään oman sisäverkon lisäksi myös palveluja, joissa tieto liikkuu internetissä. Tällöin verkko ja verkkolaitteet sekä muut määritykset ov valittava ja toteutettava asianmukaisesti.

Kyberturvallisuuden, jota voidaan myös kutsua digitaaliseksi turvallisuudeksi, pyrkimyksenä on turvata digitaalisesti verkostoitunutta yhteiskuntaa. Kyberturvallisuuden toimintaperiaatteena on tunnistaa, ehkäistä ja varautua digitaalisten järjestelmien häiriöiden vaikutuksiin. Kyberturvallisuus keskittyy tiedon, tietojärjestelmien ja laitteiden turvallisuuden takaamiseen verkkoympäristössä. Kyberturvallisuuden uhkia on mm. tietojen kalastelu, tietomurrot ja – vuodot, palvelunestohyökkäykset sekä erilaiset haittaohjelmat.

Kyberturvallisuutta lisätään virustorjuntaohjelmilla, ajantasaisilla ohjelmistopäivityksillä, vahvojen salasanojen käytössä sekä myös omalla toiminnalla. Omalla toiminnalla voi vaikuttaa paljon siihen, miten hyvin on turvassa verkossa liikkuvia vaaroja vastaan. Monien verkkorikollisten toiminta perustuu ihmisten varomattomuuteen. Tällöin verkkorikolliset voivat huijata uhrejaan esimerkiksi lataamaan haittaohjelmia sähköpostin liitetiedostoihin piilotettuna tai luovuttamaan henkilötietonsa tietojenkalastelun seurauksena.

Tietosuojavastaavan vinkit!

- Mikäli sähköpostitse tiedustellaan esimerkiksi käyttäjätunnusta ja salasanaasi, kyseessä on hyvin mahdollisesti tietojen kalasteluyritys! Älä luovuta käyttäjätunnusta ja salasanaasi kenellekään!
- Mikäli epäilet kyberhyökkäystä, ilmoita asiasta heti Meitaan ja Siun soten turvallisuuspäällikölle!
- **Lukuvinkki:** Kyberhäiriöiden hallinta – Käsikirja terveydenhuollon toimijoille[149].

14.7 Tietoaineiston turvallisuus

Hallittu ja hyvä tiedonhallinta minimoi monia tietoturvariskejä. On tärkeää määritellä ja suunnitella tiedonhallinta, tietojen varmuuskopioinnit sekä palautukset sekä säilytys- ja arkistointiratkaisut.

15 Etätyön tietosuoja ja tietoturva

[149] JAMK - Kyberhäiriöiden hallinta, käsikirja terveydenhuollon toimijoille

Etätyöllä tarkoitetaan joustavaa, vapaaehtoisuuteen, sopimukseen ja sääntöihin perustuvaa työn tekemistä muualla kuin työnantajan tiloissa. Työskentely voi tapahtua yhdessä tai useammassa paikassa ja olla kestoltaan ja säännöllisyydeltään hyvin vaihtelevaa. Työ voidaan suorittaa sellaisessa ympäristössä, missä se on työntekijän, työnantajan ja tehtävän työn kannalta tehokkainta ja tarkoituksenmukaisinta.

Etätyötä tehdään tyypillisesti kotona, vapaa-ajan asunnolla, liikkuvana työnä matkoilla tai työnantajan kanssa sovitussa etätyöpisteessä. Kaikki työ ei kuitenkaan välttämättä sovi tehtäväksi etätyönä. Etätyön tekemisestä on aina sovittava etukäteen esihenkilön kanssa, joka ratkaisee, onko etätyön onnistumiselle olemassa olevia edellytyksiä. Etätyöstä sovitaan työntekijän ja esihenkilön välillä kirjallisesti. Siun soten Henkilöstöpalvelut vastaavat etätyön ohjeistuksesta, siitä sopimisesta sekä etätyön palvelussuhteen ehdoista.

Etätyötä suunniteltaessa esihenkilön on huomioitava seuraavat tietosuojaan ja tietoturvaan liittyvät asiat:

- Työntekijälle on tilattava ja asennettava etätyössä vaadittavat laitteet, ohjelmistot ja tietoliikenneyhteydet. Työnantaja vastaa myös työnteon kannalta tarpeellisten laitteiden huollosta sekä vakuuttamisesta ja niiden aiheuttamista vahingoista.
- Työntekijän kanssa tulee käydä läpi ennen etätyön aloittamista kaikki työhön sekä työvälineisiin liittyvät ohjeistukset, huomioiden tietosuojan ja tietoturvan
- Työnluonteen mukaisesti tulee tehdä riskinarviota siitä, mitä tietosuojaan ja tietoturvaan liittyvää on erityisesti huomioitava etätyön aikana
- Ulkomailla tehtävästä etätyöstä on sovittava tapauskohtaisesti, ja huomioitava mahdolliset rajoitteet ja lisäsuojaustoimet, mikäli henkilö työskentelee EU:n ja ETA-alueen ulkopuolella
- Työntekijän kanssa tulee käydä läpi toimintamallit, mikäli työhön liittyviä tietoaineistoja tai laitteita katoaa tai varastetaan etätyön aikana tai työssä tapahtuu henkilötietojen tietoturvaloukkaukseen viittaava tapahtuma
- Etätyön päätyttyä esihenkilön on huolehdittava, että työvälineet, tarvikkeet sekä mahdolliset tallenteet ja asiakirjat palautetaan työnantajalle.

Etätyössä työntekijän tulee huolehtia seuraavista tietosuojaan ja tietoturvaan liittyvistä asioista:

- Vain työnantajan osoittamia etätyöyhteyksiä ja -välineitä tulee käyttää etätyössä
- Etätyöhön luovutetuista työvälineistä on pidettävä hyvää huolta, eikä niitä saa hyödyntää muuhun tarkoitukseen kuin työn tekemiseen
- Kukaan ulkopuolinen (sivullinen) ei saa päästä käsiksi laitteisiin tai tietoihin, joita työssä käsitellään. Etätyöpisteeltä poistuttaessa työasemat on lukittava
- Työhön liittyvät keskustelut tulee käydä niin, ettei niitä kuule ulkopuoliset henkilöt
- Omia käyttäjätunnuksia tai tunnistautumisvälineitä ei tule säilyttää niin, että niihin pääsisi käsiksi ulkopuolinen (sivullinen)
- Julkisia suojaamattomia verkkoyhteyksiä ei saa hyödyntää työmatkoilla. Matkoilla verkkoyhteys on jaettava työpuhelimesta
- Hyvinvointialueen salassapito- ja käyttäjäsitoumus on voimassa myös etätyön aikana

- Hyvinvointialueen tietoaineistojen luokittelu- ja käsittelyohjetta on noudatettava myös etätyössä
- Mikäli työhön liittyviä tietoaineistoja tai laitteita katoaa tai varastetaan, työntekijän on ilmoitettava välittömästi asiasta esihenkilölle, turvallisuuspäällikölle, tietosuojavastaavalle tai Meitan ServiceDeskiin.
- Mikäli työssä havaitaan henkilötietojen tietoturvaloukkaus, työntekijän on ilmoitettava tapahtumasta välittömästi esihenkilölle tai tietosuojavastaavalle.
- Etätyön päätyttyä työntekijän tulee palauttaa kaikki etätyöhön luovutetut työvälineet sekä mahdolliset tallenteet ja asiakirjat esihenkilölle.

Tietosuojavastaavan vinkit!

- Tutustu etätyöhön liittyvään toimintaohjeeseen[150] sekä Siun soten etätyösopimukseen[151]!
- Työskennellessä kotoa, on hyvä pitää mielessä, että perheenjäsenet ovat ulkopuolisia eli sivullisia, jotka eivät saa päästä käsiksi mm. laitteisiin, tiedostoihin tai kuulla työhön liittyviä keskusteluja!
- Muista, että työhön liittyvät muistiinpanot (mm. omat muistikirjat ja post it -laput) ovat myös säilytettävä asianmukaisesti ja hävitettävä asianmukaisesti, jottei niihin pääse käsiksi ulkopuoliset tahot!
- Vältä työhön liittyviä keskusteluja esimerkiksi julkisissa kulkuvälineissä. Mikäli työhön liittyvä keskustelu on hoidettava, varmistu etteivät kanssamatkustajat kuule luottamuksellisia tai salassa pidettäviä tietoja. Lisäksi kannattaa välttää keskusteluja, jotka ovat yhdistettävissä työnantajaan, jotta mahdollisilta väärinymmärryksiltä vältytään tai anneta työnantajasta väärää kuvaa (lojaliteettivelvoite)!
- Tutustu Kyberturvallisuuskeskuksen ohjeisiin[152] etätyön tietoturvaan liittyen.

[150] Siun sote – Etätyö Siun sotessa (Siun sote intra)
[151] Siun sote – Etätyösopimus (Siun sote intra)
[152] Kyberturvallisuuskeskus – Etätyön tietoturva – ohjeita organisaatioille ja yrityksille

Liite 1 Tietosuojan pikaopas

Etkö jaksanut kahlata läpi koko tietosuoja- ja tietoturvakäsikirjaa, mutta haluaisit nopeasti tiedon siitä, mitä pitää tehdä ja mistä tulee varmistua, jotta voi sanoa noudattavansa EU:n yleistä tietosuoja-asetusta? Lue silloin tämä pikaopas, jotta tiedät mitä pitää tehdä. Varaudu kuitenkin siihen, että saatat tarvita lisätietoja, jolloin voit palata takaisin käsikirjan sisältöön.

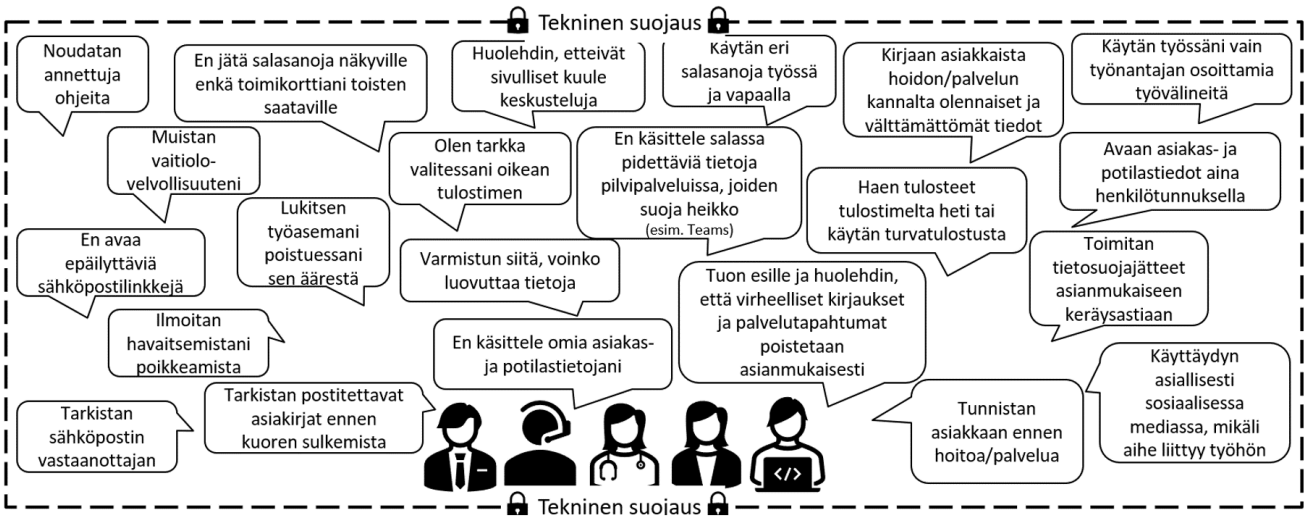
1. **Kartoita henkilötiedot**
    a. Mitä tietoja kerätään? Ryhmittele tiedot kokonaisuuksiksi niiden käyttötarkoituksen mukaan.
    b. Mitä tietoja meillä jo on? Huomioi tietojärjestelmät, edeten yksittäisiin tietoihin, joita voi olla yllättävän monissa paikoissa.
2. **Selvitä tietojen käyttötarkoitus ja tee siivous tietoihin**
    a. Kun kaikki henkilötiedot on listattu, jokaiselle tietokokonaisuudelle tulee määritellä syy, miksi näitä tietoja tarvitaan.
    b. Mikäli havaitset, että jotkut tiedot ovat tarpeettomia, ne kannattaa poistaa (huomioiden mahdolliset arkistointivelvoitteet!)
    c. Mikäli havaitset, että jotkut tiedot ovat virheellisiä tai vanhentuneet, ne kannattaa poistaa.
3. **Tee riskinarvio**
    a. Pohdi tietokokonaisuuksittain, mitä niille henkilöille voisi seurata, joiden tietoja on kerätty, jos tiedot päätyisivät esimerkiksi vääriin käsiin tai vaikkapa tuhoutuisivat vahingossa.
    b. Pohdi myös, mitä esimerkiksi tietomurrosta voisi aiheutua organisaatiolle, jos tietoihin ei enää päästäisi käsiksi.
    c. Luokittele tunnistamasi riskit niiden todennäköisyyden ja vakavuuden mukaan.
    d. Suunnittele toimenpiteet, joilla ainakin todennäköisimmät ja vaikutuksiltaan vakavimmat riskit saataisiin torjuttua ja vahinkoja pienennettyä.
4. **Suunnittele toimintatapa**
    a. Millä tavalla organisaatio huolehtii jatkossa kohtien 1.–3. toteuttamisesta?
5. **Dokumentoi**
    a. Kirjaa ylös kohtien 1.–4. tulokset ja voit olla jonain päivänä tyytyväinen, kun valvontaviranomainen ottaa yhteyttä.

Lähde: Korpisaari, P., Pitkänen, O. & Warma-Lehtinen, E. 2022. Tietosuoja. Alma Talent Oy, Helsinki.

Liite 2 Oman työn tietoturvallisuus

Tietosuoja ja tietoturva eivät rajaudu vain organisaation toimintaan. Jokainen työntekijä on päivittäin tekemisissä henkilötietojen, tietojärjestelmien, älypuhelinten, tietokoneiden ja muiden digitaalisten laitteiden ja alustojen kanssa. Jokainen työntekijä voi myös omalta osaltaan vaikuttaa työnsä tietoturvallisuuteen. Omat asenteet ja osaaminen on tärkeässä roolissa tietosuojan ja tietoturvan toteutumisen kannalta. Työn tietoturvallisuuteen liittyvät myös tärkeänä osana työohjeet, yksikössä sovitut toimintamallit ja yksikön toimintaan liittyvät tunnistetut työn riskit.

Valppaus ja varovaisuus sekä huolellisuus ovat hyödyllisiä ominaisuuksia, kun entistä enemmän työn arkeen kuuluu tietojen käsittelyä mm. sähköisessä muodossa. Ennen napin painallusta on aina lupa miettiä rauhassa ja mikäli jokin asia askarruttaa, kannattaa aina kysyä neuvoa ja apua. Kysyvä nimittäin harvoin eksyy tieltä!



Kuva 2 Oman työn tietoturvallisuus, esimerkkejä huomioitavista asioista

Liite 3 Henkilötietojen käsittelyn ulkoistamisen muistilista

Siun sote voi ulkoistaa henkilötietojen käsittelytoimia esimerkiksi sopiessaan palvelun hankkimisesta ulkopuoliselta palveluntuottajalta. On syytä huomioida, että käsittelytoimen ulkoistaminen ei poista Siun sotelle rekisterinpitäjänä kuuluvia vastuita ja velvoitteita. Tutustu muistilistaan ja sovella sekä jatkojalosta sitä tarvittaessa tarkemmalle tasolle!

1. **Varmistu siitä, että ymmärrät ja tiedostat, millaisia velvollisuuksia Siun sotelle kuuluu**
    a. Liittyykö toimintaan erityislainsäädäntöä, jossa säädetään erityisesti henkilötietojen käsittelystä?
    b. Millaisia käsiteltävät henkilötiedot ovat luonteeltaan? Onko käsittelyyn liittyvät riskit tunnistettu?
    c. Muodostuuko käsittelystä uusi henkilötietoja sisältävä rekisteri?
2. **Varmistu myös siitä, mitä velvoitteita kohdistuu palveluntuottajalle**
    a. Käytä vain palveluntuottajia, jotka noudattavat tietosuojaperiaatteita ja tietosuojalainsäädäntöä
    b. Palveluntuottaja ei saa missään tilanteessa käsitellä Siun soten rekisterinpidonalaisia tietoja muuhun käyttötarkoitukseen tai muulla tavalla kuin on sovittu!
    c. Tuleeko hankintaan liittää vaatimusmäärittelyjä, kuinka tietosuoja ja tietoturva on niissä huomioitu?
3. **Määrittele, mitä henkilötietoja ulkoistaminen koskee ja kuinka palveluntuottaja tulee henkilötietojen käsittelijänä niitä käsittelemään ja miten**
    a. Määrittele käsiteltävät tiedot (mm. rekisteröityjen ryhmät, henkilötietojen tyypit), niiden luonne, käsittelyn kesto ja käsittelyn tarkoitus
    b. Kartoita henkilötietojen käsittelyn kokonaisuus, huomioi koko tiedon elinkaari! Huomioi jo hankittaessa palvelua, että se voi myös joskus päättyä, mitä silloin tapahtuu?
    c. Millaisia teknisiä ja organisatorisia toimenpiteitä tulee toteuttaa ennen käsittelyn aloittamista? Muista, että mitä arkaluonteisemmista tiedoista tai mitä laajemmasta tietojen käsittelystä on kyse, sitä kattavampia toimenpiteitä edellytetään.
    d. Liittyykö käsittelytoimien toteuttamiseen alihankkijoita, millä tavalla? Missä maissa henkilötietoja käsitellään, käsitelläänkö niitä EU- tai ETA-maiden ulkopuolella?
4. **Pohdi, mitkä henkilötietojen käsittelytoimet kuuluvat edelleen Siun sotelle**
    a. Muista, että mm. tietopyyntöjen, rekisteröityjen tarkastuspyyntöjen sekä tietoturvaloukkausten käsittely kuuluu edelleen rekisterinpitäjälle eli Siun sotelle! Palveluntuottajan tulee tarvittaessa avustaa Siun sotea niiden käsittelyssä.
5. **Huolehdi, että käsittelytoimeen liittyvät ohjeet, käytänteet ja toimintamallit ovat ajan tasalla**
    a. Muista, että Siun sote on rekisterinpitäjänä velvollinen ohjaamaan ja ohjeistamaan tietojen käsittelyä. Pelkästään vaatimusmäärittely tai henkilötietojen käsittelystä sopiminen ei ole riittävä tapa ohjeistaa henkilötietojen käsittelijänä toimivaa palveluntuottajaa!
6. **Varmista sopimus ja henkilötietojen käsittelystä sopiminen**
    a. Sopimuksen liitteenä tulee olla henkilötietojen käsittelyn ehdot ja kuvaus palveluntuottajan suorittamasta henkilötietojen käsittelystä!
    b. Varmista, että sopimus ja ehdot pitävät myös poikkeamatilanteissa (mm. henkilötietojen tietoturvaloukkaus, tietomurto tai tietovuoto) ja huolehdi, että vahingonkorvausvelvoitteesta on sovittu!