KESKI-
SUOMEN
HYVINVOINTI-
ALUE

Tietoturva- ja tietosuojaohjeet

Rekisterinpitäjän lukuun asiakas- ja potilastietoja käsitteleville palveluntuottajille

Sisällys

1. Johdanto

Nämä tietoturva- ja tietosuojaohjeet on tarkoitettu niille Keski-Suomen hyvinvointialueen yhteistyökumppaneille, jotka sopimuksen mukaisia tai palvelusetelillä palveluja tuottaessaan käsittelevät henkilötietoja tai sosiaali- ja terveyspalveluiden asiakas- ja potilastietoja Keski-Suomen hyvinvointialueen lukuun. Palveluntuottaja sitoutuu noudattamaan henkilötietojen käsittelyyn liittyvää kulloinkin voimassa olevaa lainsäädäntöä, henkilötietojen käsittelyn ehtoja sekä niitä täydentäviä Rekisterinpitäjän tietoturva- ja tietosuojaohjeita (tämä ohje).

Mikäli näihin ohjeisiin liittyy huomautettavaa, ota yhteyttä Keski-Suomen hyvinvointialueen sopimusyhteyshenkilöösi.

EU:n yleisen tietosuoja-asetuksen (28A) mukaan rekisterinpitäjän on ohjeistettava henkilötietojen käsittelyssä niitä tahoja, jotka käsittelevät henkilötietoja rekisterinpitäjän lukuun.

Ostopalvelusopimuksella/toimeksiantosopimuksella tai palvelusetelillä hankittujen terveydenhuollon palveluiden osalta potilasasiakirjat kuuluvat Keski-Suomen hyvinvointialueen potilasrekisteriin ja sosiaalihuollon asiakasasiakirjat sosiaalihuollon asiakasrekisteriin. Sopimuksissa/sääntökirjoissa on sovittava kirjallisesti rekisterinpitoon ja tietojenkäsittelyyn liittyvistä tehtävistä ja vastuista sekä varmistua, että tietosuoja ja salassapito säilyvät.

Keski-Suomen hyvinvointialueen sopimusten tai palvelusetelipalveluiden mukaisten asiakkaiden/potilaiden tiedot on pidettävä erillään Palveluntuottajan muiden asiakkaiden/potilaiden tiedoista. Mikäli Keski-Suomen hyvinvointialueen sopimuksen piiriin kuuluva asiakas/potilas ostaa itse sopimuksen ulkopuolisia palveluita, ei näitä tietoja kirjata Keski-Suomen hyvinvointialueen henkilörekistereihin.

2. Tietoturvan ja tietosuojan organisointi ja vastuut

Nämä ohjeet pohjautuvat Keski-Suomen hyvinvointialueella hyväksyttyyn Tietoturva- ja tietosuojapolitiikkaan ja sitä täydentäviin ohjeisiin. Palveluntuottaja vastaa oman henkilöstönsä osaamisesta ja toiminnasta. Palveluntuottajan työntekijät vastaavat omalta osaltaan tietoturvan ja tietosuojan toteuttamisesta ja ohjeiden noudattamisesta

3. Salassapito ja vaitiolovelvollisuus

Sopimuksen aikana tai sen päätyttyä, sivullisille ei saa ilmaista työssä tietoon saatua organisaatiota, sen toimintayksikköä, asiakkaita/potilaita, sopimuskumppaneita tai muita yhteistyötahoja koskevia salassa pidettäviä tietoja. Vaitiolovelvollisuus koskee myös harjoittelijoita, opiskelijoita, tutkijoita jne. Salassa pidettävät tiedot voivat olla nähtyjä, kuultuja tai asiakirjoista ilmeneviä. Jo tieto asiakkuudesta on salassa pidettävä. Salassapitoa ohjaavat useat lait esim. EU:n yleinen tietosuoja-asetus, Tietosuojalaki,

Laki viranomaisen toiminnan julkisuudesta, Laki potilaan asemasta ja oikeuksista, Laki sosiaalihuollon asiakkaan asemasta ja oikeuksista, Laki terveydenhuollon ammattihenkilöstä, Laki sosiaalihuollon ammattihenkilöstä.

Salassapito ja vaitiolo ovat osa ammattitaitoa. Henkilötietoja saa käsitellä hoitosuhteen tai työtehtävän vuoksi ja vain siinä laajuudessa kuin työtehtävät edellyttävät. Keski-Suomen hyvinvointialueen henkilötietoja, asiakirjoja, ohjelmia ja laitteita käyttäessä sitoudutaan noudattamaan Keski-Suomen hyvinvointialueen tietoturva- ja tietosuojaohjeita.

4. Keski-Suomen hyvinvointialueen laitteet ja niiden käyttö

Päätelaitteen tietoturvasta vastaa jokainen käyttäjä noudattamalla näitä tietoturva- ja tietosuojaohjeita. Päätelaitteita ovat pöytätyöasemien ja kannettavien tietokoneiden lisäksi mm. puhelimet, älypuhelimet, päätteet ja taulutietokoneet (tabletit), jotka Keski-Suomen hyvinvointialue on mahdollisesti luovuttanut työvälineiksi. Päätelaitteella käytetään organisaation tietoja, jotka ovat itse laitteella, sähköisissä tietojärjestelmissä tai muissa työntekijälle käyttöön annetuissa palveluissa.

Keski-Suomen hyvinvointialueen laitteita saa käyttää vain henkilöt, joiden käyttöön ne on annettu. Edes perheenjäsenet eivät saa käyttää laitteita, joilla käsitellään Keski-Suomen hyvinvointialueen aineistoja.

Mikäli työskentelet Keski-Suomen hyvinvointialueen tilojen ulkopuolella hyvinvointialueen päätelaiteella, noudata erityistä huolellisuutta. Huomio, ettei päätelaitteen jää lukitsemattomaan tilaan taikka autoon ilman valvontaa. Selvitä myös, mitä tietoja ja aineistoja voi käsitellä Keski-Suomen hyvinvointialueen tilojen ulkopuolella.

Päätelaitteiden salasanat ja PIN-koodit on vaihdettava heti, kun laite otetaan käyttöön. Suositeltava salasanan pituus on vähintään 12 merkkiä, eikä koostu yksittäisistä sanoista. Salasanan tulee sisältää isoja ja pieniä kirjaimia, numeroita ja erikoismerkkejä.

Työntekijän varmennekortit, käyttäjätunnukset ja salasanat ohjelmiin on tarkoitettu vain henkilökohtaiseen käyttöön, eikä niitä saa jättää toisten henkilöiden saataville. Kun poistut päätelaitteen ääreltä väliaikaisestikin, huolehdi ettei laite ja siinä olevat ohjelmat jää henkilökohtaisilla käyttäjätunnuksillasi toisen käytettäväksi.

Asiakas- ja potilastietojen käsittelystä tallentuu lokitietoa käyttäjätunnuksen haltijan tekemäksi. Tietoliikenneverkon sekä asiakas- ja potilasasiakirjojen käsittelyä valvotaan automaattisten seuranta- ja valvontajärjestelmien ja lokitietojen avulla.

Tallenna valmiit työt niille sovittuihin paikkoihin. Asiakas- ja potilastiedot kuuluvat vain asiakas- ja potilastietojärjestelmiin. Käytä vain tunnistettuja ja turvallisia tietovälineitä, koska vieraat tietovälineet saattavat sisältää haitta- tai vakoiluohjelmia.

Palveluntuottaja vastaa käyttämiensä ohjelmistojen lainmukaisuudesta, käyttöoikeuksista ja sopivuudesta tarjoamiensa palvelujen toteuttamisessa.

4.1. Vikatilanteet ja laitteiden palautus

Jos Keski-Suomen hyvinvointialueen omistama älypuhelin, tietokone tai muu laite häviää tai varastetaan, ota viipymättä yhteyttä:
Asiakaspalvelupiste (puh, 014 269 5995, asiakaspalvelut@istekki.fi).

Käytössäsi olleet Keski-Suomen hyvinvointialueen omistamat puhelimet ja tietokoneet palautettaan henkilökohtaisesti asiakaspalvelupisteeseen (puh. 014 269 5995). Puhelimelle ja muille laitteille tehdään tietoturvatyhjennys, jossa laitteissa olevat tiedot (kuvat, viestit, sähköpostit) tyhjennetään, ennen kuin laitteet luovutetaan seuraavalle käyttäjälle.

5. Internet, sähköposti ja sosiaalinen media

5.1. Internet ja haittaohjelmat

Keski-Suomen hyvinvointialueen laitteita tai tietoverkkoja käytettäessä Internet on tarkoitettu työtehtävien hoitamiseen. Käytä työsi kannalta hyödyllisiä sivustoja ja vältä muita. Harkitse tarkkaan, mitä linkkejä käytät ja mitä valintoja teet. Tuntematon sivusto saattaa sisältää haittaohjelmia. Harkitse, jos tietokone ehdottaa asennettavaksi tai suoritettavaksi jotakin ohjelmaa tai ohjelman osaa. Ota tarvittaessa yhteys asiakaspalvelupisteeseen.

Älä liitä Keski-Suomen hyvinvointialueen verkkoon sellaisia laitteita, jotka eivät sinne kuulu.

5.2. Sähköposti

Sopimukseen liittyen palveluntuottajan työntekijöille on voitu mahdollistaa Keski-Suomen hyvinvointialueen sähköpostin käyttö. Tätä sähköpostia käytetään vain työtehtäviin ja sopimuksen mukaisiin palveluihin liittyen. Sähköpostin edelleen ohjaus Keski-Suomen hyvinvointialueen ulkopuolelle on kielletty. Työ- tai sopimussuhteen päättyessä sähköpostiosoitteesi poistetaan käytöstä.

Varmista mitä tietoa voi lähettää milläkin kommunikointikanavalla viranomaisille tai asiakkaille/potilaille. Viranomaisyhteistyössä käytetään turvapostia salassa pidettävien tietojen lähettämisessä. Sähköinen asiointi asiakkaiden ja potilaiden kanssa edellyttää asiakkaan ja potilaan luotettavaa tunnistamista, joka toteutuu esim. vahvaa tunnistautumista hyödyntäen.

5.3. Sosiaalinen media

Vaitiolovelvollisuus pätee myös sosiaalisessa mediassa. Älä esiinny Keski-Suomen hyvinvointialueen edustajana missään sosiaalisen median palvelussa, ellei se kuulu työtehtäviisi tai sopimuksen mukaisiin palveluihin. Huomioi, että yhteisön on joskus

vaikea erottaa, toimitko yksityishenkilönä, ammattiryhmäsi tai organisaatiosi edustajana.

Sosiaalista mediaa käyttäessä tulee huomioida, että kaikki julkaistu materiaali saattaa päätyä julkiseksi, vaikka se olisi tarkoitettu vain yksityiseksi tai vaikka olisit jo poistanut sen.

6. Muu käyttäytyminen

Järjestä työpisteesi siten, että luottamuksellisia tietoja ei ole ulkopuolisten nähtävillä työhuoneessasi tai työpöydälläsi. Tarkista näytön sijainti, jotta ulkopuoliset eivät näe salassapidettäviä tietoja. Huomio näyttösi ja asiakirjojen sijainti asiakkaisiin ja potilaisiin sekä ikkunoihin ja oviin nähden. Mikäli työasemaa, mobiililaitetta, manuaalisia asiakirjoja tms. on kuljetettava mukana, huolehdi, että ulkopuoliset (esim. perheenjäsenet) eivät pääse näkemään luottamuksellisia tietoja.

Kun keskustelet luottamuksellisista asioista henkilöiden kanssa tai puhelimella, huomioi, että keskusteluympäristössä ei ole kuuloetäisyydellä muita ihmisiä. Varmista puhelinkeskusteluissa henkilön oikeellisuus ennen salassapidettävien tietojen luovuttamista.

Käytä aina turvatulostusta, mikäli se on mahdollista. Sijoita tulostimet ja kopiokoneet ulkopuolisilta lukittuihin tiloihin siten, että ulkopuolisilla ei ole pääsyä laitteille ja niissä oleviin aineistoihin. Tarkista aina, että olet valinnut oikean tulostimen ennen kuin tulostat mitään. Muista noutaa tulosteet heti tulostamisen jälkeen. Huolehdi, ettei tulostaminen vaaranna asiakirjojen luottamuksellisuutta.

Hävitä suojaamista vaativat tulosteet, esimerkiksi henkilötietoja sisältävät tulosteet asianmukaisesti. Paperiset asiakirjat on laitettava lukittuun tietosuoja-astiaan, jonka sisältö menee asianmukaisesti tuhottavaksi. Mikäli sinulla ei ole käytettävissä tietosuoja-astiaa, käytä tietoaineiston sisällön näkökulmasta asianmukaista silppuria.

7. Loukkauksista ilmoittaminen

Palveluntuottaja ja palveluntuottajan työntekijät ovat velvollisia ilmoittamaan kaikista havaitsemistaan tietosuojauhkista, - riskeistä ja – loukkauksista Keski-Suomen hyvinvointialueen tietosuojavastaavalle, mikäli loukkaus uhkaa hyvinvointialueen tietoja.

EU:n yleisen tietosuoja-asetuksen mukaisesti tietoturvaloukkauksista ilmoitetaan valvontaviranomaiselle, mikäli niihin liittyy riskiä rekisteröidyille. Ilmoituksen tekee Rekisterinpitäjä tarvittaessa Palveluntuottajan avustuksella. Mikäli loukkaus aiheuttaa rekisteröidylle korkean riskin, ilmoitetaan loukkauksesta rekisteröidylle. Rekisteröidylle ilmoittamisesta sovitaan Palveluntuottajan kanssa.

8. Asiakas- ja potilasasiakirjojen käsittely ja salassapito

Asiakas- ja potilastiedot ovat henkilötietoja, joiden käsittelyä ohjaa lait, asetukset ja muu kansallinen sääntely. EU:n yleisen tietosuoja-asetuksen mukaan henkilötietojen käsittelyllä tarkoitetaan toimintoa tai toimintoja, joita kohdistetaan henkilötietoihin tai henkilötietoja sisältäviin tietojoukkoihin joko automaattista tietojenkäsittelyä käyttäen tai manuaalisesti. Käsittely on tietojen keräämistä, tallentamista, järjestämistä, jäsentämistä, säilyttämistä, muokkaamista tai muuttamista, hakua, kyselyä, käyttöä, tietojen luovuttamista siirtämällä, levittämällä tai asettamalla ne muutoin saataville, tietojen yhteensovittamista tai yhdistämistä, rajoittamista, poistamista tai tuhoamista.

Asiakasasiakirjojen laatimisessa noudatetaan Lakia sosiaali- ja terveydenhuollon asiakirjojen käsittelystä 703/2023 (jäljempänä Asiakastietolaki 703/2023). Asiakas- ja potilasasiakirjojen käyttöoikeuksien määrittelyssä noudatetaan Sosiaali- ja terveysministeriön asetusta käyttöoikeudesta asiakastietoon (825/2022).

Asiakasasiakirjalla tarkoitetaan asiakirjaa, joka on laadittu tai vastaanotettu tai joka sisältää tietoja asiakkaan sosiaali- tai terveyspalvelujen tarpeen arviointia varten, tarvittavien palvelujen järjestämistä tai toteuttamista varten taikka lääkkeen toimittamista varten. Potilasasiakirjat koskevat potilasta ja sosiaalihuollon asiakasasiakirja sosiaalihuollon asiakasta.

Salassapidosta yleisesti kohdassa 4. Asiakas- ja potilasasiakirjat ovat arkaluonteisia ja salassa pidettäviä ja tietojen käyttäjiä sitoo vaitiolovelvollisuus. Asiakas- ja potilastietoja ei saa paljastaa sivullisille ilman asiakkaan/potilaan kirjallista suostumusta tai kuin laissa erikseen säädetään. Salassa pidettävää tietoa ei saa käyttää omaksi tai toisen hyödyksi tai vahingoksi. Salassa pidettävä tieto voi olla nähtyä, kuultua tai asiakirjoista ilmenevää. Salassapito säilyy myös palvelusopimuksen ja työsuhteen päättymisen jälkeen.

Asiakas- ja potilasasiakirjojen tietoja saa käyttää vain asiakas/potilassuhteen tai siihen liittyvän muun työtehtävän hoitamisessa. Mikäli Palveluntuottajan palvelussa oleva potilas siirtyy esim. erikoissairaanhoitoon, hoitosuhde katkeaa palveluntuottajan palveluun ja muodostuu erikoissairaanhoitoon. Potilastietojen katselu Palveluntuottajan palvelussa ei tällöin ole välttämättä perusteltua. Hoitosuhde muodostuu uudelleen Palveluntuottajan palveluun, kun erikoissairaanhoidosta tulee tieto potilaan siirtymisestä Palveluntuottajan palveluun.

Asiakirjoja saa käyttää vain siinä laajuudessa kuin työntekijän työtehtävät ja vastuut sekä asiakkaan asioiden/potilaan terveyden hoitaminen sillä hetkellä edellyttävät**.** Työntekijällä ei ole oikeutta esim. perheenjäsenensä tai omiin asiakas/potilasasiakirjoihinsa.

8.1. Asiakas- ja potilasrekisterit

Sosiaalihuollon asiakirjat ja terveydenhuollon potilasasiakirjat muodostavat henkilörekistereitä. Keski-Suomen hyvinvointialueen palveluissa tuotetut asiakasiedot kuuluvat Keski-Suomen hyvinvointialueen henkilörekistereihin myös siinä tapauksessa,

kun palvelut on toteutettu ostopalveluna, palvelusetelisopimuksen tai muun vastaavan sopimuksen mukaisesti. Kirjaamiseen liittyvät käytännöt sovitaan sopimuksissa.

8.2. Asiakas- ja potilasasiakirjojen laatiminen

Asiakas ja potilas tunnistetaan tietojärjestelmästä henkilötunnuksen – ei pelkän nimen perusteella. Sosiaali- ja terveydenhuollon ammattihenkilön ja palvelun antamiseen osallistuvan avustavan henkilön tulee kirjata asiakasasiakirjoihin asiakkaan palvelun ja potilaan hoidon järjestämisen, suunnittelun, toteuttamisen, seurannan ja valvonnan turvaamiseksi tarpeelliset ja riittävät tiedot. Asiakasasiakirjamerkintöjen on oltava virheettömiä, ymmärrettäviä ja niissä saa kyttää vain yleisesti tunnettuja ja hyväksyttyjä käsitteitä ja lyhenteitä. Asiakasasiakirjat on laadittava viipymättä.

8.3. Sosiaalihuollon asiakasasiakirjat

Velvollisuus kirjata sosiaalihuollon asiakastietoja alkaa, kun palvelunantaja on saanut tiedon henkilön palveluntarpeesta tai ryhtynyt toteuttamaan sosiaalipalvelua. Tieto asiakkuuden päättymisestä on kirjattava asiakasasiakirjaan.

Kaikista sosiaalihuollon asiakasrekisteriin tallennettavista sosiaalihuollon asiakasasiakirjoista on käytävä ilmi, mihin sosiaalihuollon palvelutehtävään tai palvelutehtäviin se liittyy.

Toisen lukuun tuotetussa sosiaalihuollossa tai sosiaalipalveluissa tallennetuista sosiaalihuollon asiakasasiakirjoista on ilmettävä niiden käsittelyperuste, palvelunjärjestäjä ja palveluntuottaja. Alihankintatilanteissa sosiaalihuollon asiakastiedoista on ilmettävä hankintaketju kokonaisuudessaan.

Jos sosiaalihuollon asiakasta koskevia tietoja saadaan muualta kuin asiakkaalta itseltään, tietojen vastaanottajan on voitava todentaa:

1. mitä tietoja on hankittu tai saatu
2. keneltä tiedot on saatu tai muu tiedonlähde, jos tiedot on saatu teknisen käyttöyhteyden kautta
3. milloin tiedot on saatu
4. henkilö, joka tiedot on pyytänyt, jos ne on hankittu oma-aloitteisesti
5. tiedon hankkimisen tai saamisen perusteena oleva säännös tai suostumusta koskevat tiedot
6. käyttötarkoitus, johon tiedot on hankittu tai saatu.

Jos alaikäinen sosiaalihuollon asiakas kieltää asiakastietojensa luovutuksen huoltajalle, muulle lailliselle edustajalle tai muulle tiedonsaantiin oikeutetulle henkilölle, on kielto ja sen perusteeksi esitetty painava syy kirjattava.

Lisää asiakirjojen laatimisesta Asiakastietolaissa (703/2023).

8.4. Potilasasiakirjat

Potilasasiakirjoihin saavat tehdä merkintöjä potilaan terveyspalvelujen järjestämiseen ja toteuttamiseen osallistuvat terveydenhuollon ammattihenkilöt ja vastaavan johtajan ohjeiden mukaisesti myös muut henkilöt siltä osin kuin he osallistuvat terveyspalvelun järjestämiseen ja toteuttamiseen. Terveydenhuollon opiskelijan tekemät merkinnät hyväksyy hänen esimiehensä tai ohjaajansa taikka muu hyväksymiseen valtuutettu henkilö.

Potilasasiakirjoihin on kirjattava potilasasiakirjamerkinnät jokaisesta palvelutapahtumasta. Merkinnöistä tulee tarpeellisessa laajuudessa käydä ilmi potilaan terveydentilaa, annettua palvelua ja sairauden ja hoidon kulkua koskevat tiedot sekä taudinmäärityksen, valitun hoidon ja tehtyjen hoitoratkaisujen perusteet. Lääkemääräyksistä on kirjattava lääkemääräyslain 6 §:n mukaiset tiedot sekä valitun lääkehoidon perustelut siltä osin kuin tieto ei sisälly lääkemääräykseen.

Mikäli potilaan hoidon kannalta on välttämätöntä kirjata toisen henkilön itsestään kertomia tai muita muun henkilön yksityiskohtaisia arkaluonteisia tietoja, nämä tiedot kirjataan potilaan palvelutapahtuman asiakirjoihin kuuluvaan erilliseen asiakirjaan. Erillisasiakirja ei näy potilaalle OmaKannasta.

Hoitovastuussa olevan terveydenhuollon ammattihenkilön tulee tehdä potilasasiakirjoihin merkinnät potilaan taudinmäärityksen tai hoidon kannalta merkittävästä puhelinneuvottelusta sekä muusta vastaavasta konsultaatiosta ja hoitoneuvottelusta. Merkinnöistä tulee käydä ilmi konsultaation tai neuvottelun ajankohta, asian käsittelyyn osallistuneet sekä tehdyt hoitoratkaisut ja niiden toteuttaminen.

Osastohoidossa ja pitkäaikaisen hoidon piirissä olevasta potilaasta tulee tehdä potilaan hoidon kannalta riittävän usein merkinnät hänen tilansa muutoksista, hänelle tehdyistä tutkimuksista ja hänelle annetusta hoidosta. Päivittäin on tehtävä merkinnät potilaan tilaan liittyvistä huomioista, hoitotoimista ja vastaavista seikoista. Lääkärin tulee tehdä sairaalahoidossa olevan pitkäaikaispotilaan potilasasiakirjoihin vähintään kolmen kuukauden välein seurantayhteenveto.

Kun alaikäinen henkilö on terveydenhuollon asiakkaana, on palvelutapahtumakohtaisesti kirjattava tieto siitä, onko alaikäinen ollut kykenevä itse päättämään hoidostaan. Merkinnöistä tulee käydä ilmi myös, salliiko hoidostaan päättämään kykenevä alaikäinen potilas terveydentilaansa tai kyseistä hoitoa koskevien tietojen antamisen hänen huoltajalleen, muulle lailliselle edustajalleen tai muulle tiedonsaantiin oikeutetulle vai onko hän kieltänyt tietojen antamisen.

Potilaan tai hänen omaisensa tekemään muistutukseen, kanteluun ja potilasvahinkoasiaan sekä tarkastus- ja korjaamispyyntöihin liittyviä tietoja ei kirjata potilasasiakirjoihin. Merkintä on sallittua vain silloin, jos tieto on hoidon kannalta välttämätöntä. Muistutukseen, kanteluun ja potilasvahinkoon liittyvät asiakirjat arkistoidaan potilastiedoista erilliseen arkistoon.

Lisää Potilasasiakirjojen laatimisesta Asiakastietolaissa (703/2023).

8.5. Asiakas- ja potilasasiakirjojen luovuttaminen

Asiakas- ja potilasasiakirjojen luovutuksesta ulkopuolisille vastaa Rekisterinpitäjä, ellei toisin ole sovittu.

9. Asiakkaan ja potilaan oikeudet

Sosiaalihuollon asiakkaan asioita on hoidettava yhteisymmärryksessä hänen kanssaan. Hänelle on selvitettävä oikeutensa ja velvollisuutensa sekä erilaiset vaihtoehdot ja niiden vaikutukset sekä muut mahdolliset seikat, jotka vaikuttavat hänen asiansa hoitamisessa. Asiakkaan toivomukset ja mielipide on otettava huomioon sosiaalihuoltoa toteutettaessa ja muutoinkin kunnioitettava asiakkaan itsemääräämisoikeutta. Ensisijaisesti on huomioitava asiakkaan etu. Mikäli asiakas ei itse pysty osallistumaan ja vaikuttamaan asioittensa hoitamiseen, on asiakkaan tahtoa selvitettävä hänen laillisen edustajansa, omaisen tai muun läheisen kanssa. (Laki sosiaalihuollon asiakkaan asemasta ja oikeuksista 812/2000).

Potilasta on hoidettava yhteisymmärryksessä hänen kanssaan ja hänellä on oikeus saada selvitys hänen terveydentilastaan sekä seikoista, jotka vaikuttavat hänen hoitamiseensa (hoidon merkityksestä, eri hoitovaihtoehdoista ja niiden vaikutuksista). Selvitys on annettava siten, että potilas sen ymmärtää (Laki potilaan asemasta ja oikeuksista 785/1992).

Lakisääteisiä palveluja annettaessa asiakkaalla/potilaalla on EU:n yleisen tietosuoja-asetuksen mukaan seuraavia oikeuksia henkilötietoihinsa:

- oikeus saada informaatiota henkilötietojen käsittelystä
- oikeus saada tutustua tietoihin
- oikeus oikaista tietoja
- oikeus rajoittaa tietojen käsittelyä
- henkilötietojen oikaisua tai käsittelyn rajoitusta koskeva ilmoitusvelvollisuus
- oikeus olla joutumatta automaattisen päätöksenteon kohteeksi ilman lainmukaista perustetta

Asiakkaalla/potilaalla on myös oikeus saada tietää, onko hänen tietojaan käsitelty asiallisesti. Näitä oikeuksia asiakkaan/potilaan on haettava kirjallisesti ja oikeuksien toteuttamisesta vastaa Rekisterinpitäjä. Tarvittavat lomakkeet palautusohjeineen ovat saatavissa Keski-Suomen hyvinvointialueen internet-sivustoilta. Lomakkeet | Keski-Suomen hyvinvointialue (hyvaks.fi)

10. Valvonta

Asiakas- ja potilastietojen käsittelyä valvotaan mm. automaattisesti tallentuvien lokitietojen avulla. Lokista käy ilmi mm. kuka tietoja on käsitellyt, missä roolissa ja toimintayksikössä tietoja on käsitelty sekä ajankohta, milloin tämä on tapahtunut.

Lokivalvontaa tehdään automaattisesti, säännöllisesti pistokokein sekä tarvittaessa esimiehen tai asiakkaan/potilaan pyynnöstä. Mikäli valvonnassa ilmenee lisäselvityksen tarvetta, pyytää esimies työntekijältä kirjallisen selvityksen tapahtuneesta. Jos asiassa todetaan väärinkäytös, ryhdytään organisatorisiin toimenpiteisiin ja tehdään tarvittavat ilmoituksen rekisteröidylle ja viranomaisille (kuten tietosuojavaltuutettu, poliisi). Asianomainen asiakas/potilas voi tehdä asiasta rikosilmoituksen.

Väärinkäytökset voivat johtaa sopimuksen purkamiseen.

Esimerkkejä mahdollisista rikosnimikkeistä ja sanktioista:

- **Salassapitovelvollisuuden rikkominen**: joka paljastaa asemassaan, toimessaan tai tehtävässään saadun salassa pidettävän tiedon tai käyttää sitä omaksi tai toisen hyödyksi voidaan tuomita salassapitorikkomuksesta, salassapitorikoksesta tai virkasalaisuuden rikkomisesta sakkoon tai enintään 1v vankeuteen. (RL 38 luku, 1§ ja 2§ ja RL 40 luku, 5§).

- **Tietosuojarikos**: joka tahallaan tai törkeästä huolimattomuudesta hankkii henkilötietoja niiden käyttötarkoituksen kannalta yhteensopimattomalla tavalla, luovuttaa tai siirtää henkilötietoja vastoin lakia ja näin loukkaa rekisteröidyn yksityisyyden suojaa tai aiheuttaa hänelle muuta vahinkoa voidaan tuomita tietosuojarikoksesta sakkoon tai enintään 1v vankeuteen. (RL 38 luku, 9§).

- **Tietomurto**: joka käyttää hänelle kuulumatonta käyttäjätunnusta tai muutoin oikeudettomasti tunkeutuu tietojärjestelmään, voidaan tuomita tietomurrosta sakkoon tai enintään 2v vankeuteen. (RL 38 luku, 8§).

11. Tärkeimpiä tietoturvallisuutta ja tietosuojaa ohjaavia säädöksiä

Perustuslaki (731/1999)
- 2:10 § (Yksityiselämän suoja ja luottamuksellisen viestin salaisuus)
- 2:12 § (Viranomaisten hallussa olevien asiakirjojen ja tallenteiden julkisuus)

Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus)

Tietosuojalaki (1050/2018)
- 4 § (yleisen edun ja julkisen vallan käytön perusteen täsmentäminen)
- 6 § (erityisiä henkilötietoryhmiä koskevan käsittely)
- 28–29 § (julkisuuslain soveltaminen, henkilötunnuksen käsittely)
- 31–34 § (tieteellinen tutkimus, rekisteröidyn oikeudet)
- 35 § (vaitiolovelvollisuus)

Terveydenhuoltolaki (1326/2010)
Laki terveydenhuollon ammattihenkilöistä (559/1994)
Laki sosiaalihuollon ammattihenkilöistä (817/2015)
Laki sähköisestä lääkemääräyksestä (61/2007)
Laki viranomaisten toiminnan julkisuudesta (621/1999)
Laki potilaan asemasta ja oikeuksista (785/1992)
Laki sosiaali- ja terveydenhuollon asiakastietojen käsittelystä (703/2023)
Laki sosiaalihuollon asiakkaan asemasta ja oikeuksista (812/2000)
Arkistolaki (831/1994) (Asiakirjojen laatiminen, säilyttäminen ja käyttö.)
Työsopimuslaki (55/2001)
Vahingonkorvauslaki (41/1974)
Laki yksityisyyden suojasta työelämässä (759/2004)
Laki sosiaali- ja terveystietojen toissijaisesta käytöstä (552/2019)
Laki eräistä EU-direktiiveissä säädetyistä lääkinnällisistä laitteista (629/2010)
Laki lääkinnällisistä laitteista (719/2021)
Laki julkisen hallinnon tiedonhallinnasta (906/2019)
Pelastuslaki (379/2011)
Rikoslaki 38 § (39/1889) Tieto- ja viestintärikoksista
Laki kunnan ja hyvinvointialueen viranhaltijasta (2003/304)
Laki sähköisen viestinnän palveluista (917/2014)
Laki hyvinvointialueesta (611/2021)
Laki sosiaali- ja terveydenhuollon järjestämisestä (612/2021)

Liitteet

Liite 1: Esimerkkejä tietoturva- ja tietosuojatoimenpiteistä, joita voi hyödyntää oman toiminnan tarkastelussa

Esimerkkejä tietoturva- ja tietosuojatoimenpiteistä, joita voi hyödyntää oman toiminnan tarkastelussa

MENETELMÄ	KUVAUS
Tietoturvatoimenpiteitä	
☐ Laitteiden käyttö	Päätelaitteet ovat pääosin tarkoitettu vain henkilökohtaiseen käyttöön ja sopimuksessa tarkoitettuun toimintaan. Yhteiskäyttölaitteet on mainittu erikseen ja näitä koskevat erilliset ohjeet.
☐ Laitteiden käyttö	Päätelaitteita ei tule jättää autoon säilytettäväksi tai muuhun valvomattomaan tai lukitsemattomaan tilaan.
☐ Laitteiden käyttö	Päätelaite on lukittava aina, kun et käytä laitetta.
☐ Laitteiden käyttö	Keski-Suomen hyvinvointialueen laitteet tulee palauttaa henkilökohtaisesti sopimuksen tai tehtävien päättyessä.
☐ Laitteiden käyttö	Keski-Suomen hyvinvointialueen päätelaitteelle ei ole lupaa asentaa mitään sovelluksia ilman hyvinvointialueen lupaa.
☐ Laitteiden käyttö	Älä tallenna mitään henkilö- tai muuta potilas-/asiakastietoa päätelaitteelle. Tietojen tallennukset tehdään niille tarkoitettuun tietojärjestelmään.
☐ Laitteiden käyttö	Älä liitä tuntemattomia tallennusvälineitä tietokoneeseesi, kuten tuntemattomia muistitikkuja.
☐ Laitteiden käyttö	Älä tallenna henkilötietoja tai muita potilas-/asiakastietoja muistitikuille tai muille ulkoisille tiedontallennuslaiteille.
☐ Käyttäjätunnus / salasana	Käyttäjätunnukset ovat henkilökohtaisia, joten ÄLÄ luovuta niitä kenellekään toiselle käytettäväksi.
☐ Käyttäjätunnus / salasana	Vaihda salasana järjestelmän sitä pyytäessä TAI mikäli uskot salasanasi vaarantuneen.
☐ Käyttäjätunnus / salasana	Muista, että asiakas- ja potilastietojen käsittelystä tallentuu lokitietoa käyttäjätunnuksen haltijan tekemäksi. Asiakas- ja potilasasiakirjojen käsittelyä valvotaan mm. lokitietojen avulla.
☐ Käyttäjätunnus / salasana	Suositeltava salasanan pituus on vähintään 12 merkkiä, eikä koostu yksittäisistä sanoista. Salasanan tulee sisältää isoja ja pieniä kirjaimia, numeroita ja erikoismerkkejä.
☐ Internet	Ole tarkkana käyttämiesi internet palveluiden suhteen. Haitallisia sivuja tai haittaohjelmia on joskus erittäin vaikea huomioida.
☐ Sähköposti	Älä avaa tuntemattomilta saamiesi postien linkkejä automaattisesti vaan tarkasta, onko siihen erityistä tarvetta. ÄLÄ hyväksy, jos avaamasi linkin jälkeen pyydetään tunnuksiasi tai ohjelmiston asennusta koneellesi.
☐ Sähköposti	Älä käytä sähköpostia potilaiden tai asiakkaiden kanssa viestimiseen ilman sovittua käytäntöä tilaajan kanssa.
☐ Sähköposti	Mikäli tunnistat postin roskapostiksi jo lähettäjän perusteella, poista se välittömästi. Älä avaa mitään roskapostissa olevia linkkejä tai liitetiedostoja.
☐ Sähköposti	Älä ohjaa Keski-Suomen hyvinvointialueen sähköposteja ulkopuolisiin postilaatikoihin.
☐ Fyysinen turvallisuus	Huolehdi aina, että työtilojesi ovet ja ikkunat ovat asianmukaisesti suljettuna ja lukittu, kun et ole paikalla.
☐ Fyysinen turvallisuus	Huolehdi työtilojesi avaimista ja tiedosta, kenellä on pääsy työtiloihin.
☐ Fyysinen turvallisuus	Huolehdi työtilojesi paloturvallisuudesta asianmukaisesti ja tarvittavista alkusammutusvälineistä.

☐ Fyysinen turvallisuus	Huolehdi, etteivät ulkopuoliset pääse näkemään laitteillasi olevia tietoja tai niiden käsittelyä esimerkiksi näyttösi kautta.
☐ Tietoaineistojen käsittely	Huolehdi, että luottamuksellisia materiaaleja ei jää työpöydällesi TAI tavalliseen jäteastiaan muiden nähtäville.
☐ Tietoaineistojen käsittely	Hävitä suojaamista vaativat paperimateriaalit asianmukaisesti esimerkiksi polttamalla tai käytä niille tarkoitettuja tietosuoja-astioita.
☐ Tietoaineistojen käsittely	Ole huolellinen puhuessasi luottamuksellisista asioista puhelimitse tai muuten julkisella paikalla, jossa muut voivat kuulla puheesi.
☐ Tietoliikenne	Suojaa tietoliikenneyhteydet aina tarvittavin keinoin, kuten palomuurein sekä salatuin yhteyksin (VPN, TLS).
☐ Tietoliikenne	Käytä tarvittaessa oman puhelimesi verkkoa tietoliikenneyhteytenä, mikäli et voi luottaa tarjottuun yhteyteen esimerkiksi hotelli / kahvilat tms.
☐ Tietoliikenne	Käytä aina päätelaitteillasi palomuuriohjelmistoja suojaamaan ulkopuolelta tulevia yhteyksiä
☐ Muu, mikä:	
Kommentit:	
Tietosuojatoimenpiteitä	
☐ Rajatut käyttöoikeudet	Huomioi roolipohjaiset ja rajattavat käyttöoikeudet sekä henkilötietojen näkyvyyden minimointi. Käyttöoikeudet ovat henkilökohtaisia ja perustuvat annettavaan palveluun ja työtehtäviin.
☐ Turvallinen tunnistautuminen	Käyttäjä tunnistetaan luotettavasti. Tekniset ratkaisut toteutetaan suhteessa järjestelmässä käsiteltävään henkilötietoon ja riskeihin.
☐ Lupa henkilötietojen käsittelyyn	Tunnista, mikä on henkilötietojen käsittelyn lainmukainen peruste (suostumus, sopimus, lakisääteiden velvoite, yleistä etua koskeva tehtävä tai julkisen vallan käyttäminen)
☐ Rekisteröityjen ryhmät	Tunnista keiden henkilötietoja käsittelet
☐ Henkilötietoryhmät	Tunnista mitä henkilötietoja käsittelet
☐ Rekisteröidyn pääsy tietoihin	Rekisteröity näkee kaikki omat tiedot järjestelmästä tai rekisteröidyn tiedot ovat luovutettavissa pyynnöstä.
☐ Rekisteröidyn oikeus oikaista tiedot	Rekisteröity voi muokata tietojaan järjestelmässä tai tehdä pyynnön tietojen korjaamiseksi.
☐ Rekisteröidyn oikeus poistaa tiedot	Rekisteröity voi poistaa tietonsa järjestelmästä tai tiedot voidaan poistaa pyynnöstä, mikäli henkilötietojen säilyttämiseen ei ole perustetta.
☐ Rekisteröidyn oikeus rajoittaa tietojen käyttöä	Rekisteröity voi vaatia tietojen käsittelyn rajoittamista liittyen juridiseen syyhyn.
☐ Rekisteröidyn oikeus siirtää tiedot toiseen järjestelmään.	Tiedostot ovat siirrettävissä sähköisessä muodossa toiseen vastaavaan rekisteriin.
☐ Rekisteröidyn oikeus vastustaa hlötietojen käsittelyä	Tietojen käsittelyä vastustavan rekisteröidyn henkilötiedot tulee voida poistaa rekisteristä. (esim. tutkimus- ja tilastointitiedot).
☐ Henkilötietojen pseudonymisointi ja salaus	Henkilötietojen aktiivisen käsittelyvaiheen aikana, henkilötiedot on pystyttävä piilottamaan sellaisista näkymistä ja käyttötavoista, joissa henkilön tunnistaminen ei ole tarpeen.

☐ Anonymisointi	Alkuperäisen henkilötiedon käsittelytarpeen päätyttyä, säilytettävät henkilötiedot on pystyttävä anonymisoimaan niin ettei henkilöä tunnista.
☐ Turvallinen tiedonsiirto	Henkilötietoa siirretään salattuna ja noudatetaan tiedon tietosuojaluokituksen mukaisia vaatimuksia. Tiedonsiirtoratkaisut on dokumentoitu.
☐Testausdata (henkilötiedon käyttö)	Oikean henkilötiedon käyttöä testaamisessa on vältettävä ilman perusteltua syytä. Erillisessä testiympäristössä tulee käyttää testiaineistoa tai pseudonymisoitua henkilötietoa.
☐ Lokitus (kirjautuminen)	Järjestelmän tulee tuottaa lokitietoa kirjautumistapahtumista.
☐ Lokitus (henkilötiedon muokkaaminen)	Järjestelmän tulee tuottaa lokitietoa henkilötiedon muokkaustapahtumista.
☐ Lokitus (admin)	Järjestelmän tulee tuottaa lokitietoa käyttöoikeuksien muutoksista.
☐ Lokitus (katselu)	Järjestelmän tulee tuottaa lokitietoja henkilötietojen katselusta.
☐ Henkilötietojen saatavuus, eheys, pääsy, vikasietoisuus	Järjestelmästä on dokumentoitu toipumissuunnitelma
☐ Muu, mikä:	
Kommentit:	