DiabetesSara

Päivitetty 16.3.2022

DiabetesSara Oy:n rekisteri- ja tietosuojaseloste

1. Rekisterinpitoa koskevat yleiset tiedot

Henkilörekisterin nimi: DiabetesSara Oy:n asiakasrekisteri

Rekisterinpitäjä: DiabetesSara Oy. Y-tunnus 2915899-5. Ajotie 7, 68380 Ullava.
asiakaspalvelu@diabetessara.fi

Rekisterinpitäjän tietosuojavastaava rekisteriä koskevissa asioissa:

Teija Vörlin, Ajotie 7, 68380 Ullava, 050 573 4222,
teija.vorlin@diabetessara.fi

2. Rekisterinpitäjän henkilötietojen käsittelyn yleinen ohjaus ja valvonta

Tietosuojariskit ja niiden vaikuttavuus on arvioitu. Yritykselle on perustettu tietosuojatoimikunta sekä nimetty tietosuojavastaava. Sekä palvelutoiminnan että tietojärjestelmien omavalvontaan on laadittu suunnitelmat. Päivitämme säännöllisesti työntekijöiden ohjeistusta ja omavalvontasuunnitelmia. Koulutamme henkilöstöä säännöllisesti asianmukaisesta tietojenkäsittelystä, tietoturvasta ja tietosuojasta.

Tietosuojatoimikunta huolehtii henkilöstön koulutuksesta sekä toteuttaa valvontaa ja puuttuu havaittuihin poikkeamiin. Tietosuojavastaavan tehtävänä on:

- auttaa rekisterinpitäjää lakisääteisten velvoitteiden toteuttamisessa
- antaa asiantuntija-apua henkilöstölle ja johdolle
- toimia henkilötietojen käsittelyn valvojana sekä yhdyssiteenä valvontaviranomaisiin

3. Yksityisyytesi suojaaminen

DiabetesSara Oy pitää asiakkaiden yksityisyyttä erittäin tärkeänä. Terveydenhuollossa tapahtuvaa asiakastietojen käsittelyä ohjaa kansallinen potilas- ja terveydenhuollon lainsäädäntö, kansallinen tietosuojalainsäädäntö ja EU:n yleinen tietosuoja-asetus. Olemme DiabetesSarassa sitoutuneet tietosuojaan ja suojaamaan asiakkaiden yksityisyyttä DiabetesSaran palveluiden käyttäjinä ja noudattamaan potilastietojen käsittelyä ja tietosuojaa koskevaa lainsäädäntöä. DiabetesSara toimii potilastietojen käsittelijänä siltä osin kuin tuottaa palveluaan tilaajaorganisaatioille ja

rekisterinpitäjänä palvelussaan tuottamalleen laajennetulle tiedolle sekä yksityisasiakkaille tuottamansa palvelun potilastiedoille. Rekisterinpitäjänä DiabetesSara on vastuussa tietosuojalainsäädännön ja tietosuojaperiaatteiden noudattamisesta kaikessa henkilötietojen käsittelyssä. Yksityiselämän suojaaminen on tärkeä osa DiabetesSaran vastuullisen liiketoiminnan periaatteita. Tämä tietosuojaseloste koskee DiabetesSaran asiakkaiden henkilötietojen käsittelyä, ja selosteen tarkoituksena on antaa tietoja rekisteröidyille tietosuojalainsäädännön edellyttämällä tavalla. Tämä tietosuojaseloste koskee DiabetesSaran potilasrekisteriä ja potilasrekisterin sisältämiä potilastietoja ja muita henkilötietoja, kuten verkkokaupan asiakasrekisteriä. DiabetesSara käsittelee kaikkia henkilötietoja pelkästään digitaalisesti.

Potilastietoihin on pääsy ainoastaan sillä henkilöstöllä, jolla on työtehtäviensä perusteella tarve käsitellä potilastietoja. DiabetesSara ei luovuta potilastietoja sivullisille. Sähköisesti käsiteltäviin tietoihin pääsee ainoastaan henkilökohtaisella käyttäjätunnuksella ja salasanalla. Potilasrekisterin tekninen ylläpito tapahtuu ohjelmistotuottajan toimesta varmuuskopioituna pilvipalveluna. Rekisteri sijaitsee DiabetesSaran potilastietojärjestelmä Diarium tuottajan salasanasuojatulla palvelimella. DiabetesSaran ylin johto päättää käyttöoikeuksien antamisesta DiabetesSaran työntekijöille potilasrekisteritietoihin siinä laajuudessa, kuin työtehtävät sitä edellyttävät. Potilastietojen käyttöä valvotaan seuraamalla muun muassa lokitietoja.

4. Henkilötietojen käsittelyn tarkoitus ja käsittelyn perusteet

DiabetesSara käsittelee asiakastietoja ainoastaan siihen tarkoitukseen, johon ne on kerätty. Noudatamme toiminnassamme yleisen tietosuoja-asetuksen (679/2016 EU), kansallisen tietosuojalain (1050/2018) sekä muun relevantin lainsäädännön mukaisia velvoitteita.

Potilastietojen käsittelyn tarkoitus on hoidon mahdollistaminen ja edistäminen. Rekistereihin tallennettuja tietoja käytetään potilaan hoitoon ja ohjaukseen tai hoidon suunnitteluun, toteuttamiseen ja seurantaan sekä muihin lain ja suostumusten mukaisiin käyttötarkoituksiin. Potilastietoja, kuten etävastaanottokäynnillä kirjattuja tietoja käsittelemme lakisääteisen velvoitteen perusteella. Erityisesti seuraavat lainsäädännöt säätelevät tietojenkäsittelyämme:

- Terveydenhuollon ammattihenkilöistä annetun lain (559/1994) mukaan terveydenhuollon ammattihenkilöllä on velvollisuus laatia ja säilyttää potilasasiakirjoja.
- Potilaan asemasta ja oikeuksista annetun lain (785/1992) mukaan terveydenhuollon ammattihenkilön on merkittävä potilasasiakirjoihin potilaan hoidon järjestämisen, suunnittelun, toteuttamisen ja seurannan turvaamiseksi tarpeelliset tiedot.
- Potilasasiakirjojen laatimisesta ja säilyttämisestä on säädetty tarkemmin sosiaali- ja terveysministeriön (STM) asetuksella (298/2009). Potilasasiakirjojen ensisijaisena tehtävänä on palvella potilaan hoidon suunnittelua ja toteutusta sekä edistää hoidon jatkuvuutta.

Koska potilastiedot sisältävät arkaluonteisia henkilötietoja, niin käsittelemme potilas- ja henkilötietoja vain silloin kun se on tarpeellista ja tarkoituksenmukaista, ja aina lainsäädännön mukaisesti. Potilastietojen käsittelyssä edellä mainittujen ja yleisen tietosuoja-asetuksen ja tietosuojalain lisäksi toimintaamme ohjaavan muun muassa seuraavat erityislait:

- Terveydenhuoltolaki (1326/2010)
- Kansanterveyslaki (66/1972)
- Erikoissairaanhoitolaki (1062/1989)
- Laki potilaan asemasta ja oikeuksista (785/1992)
- Sosiaali- ja terveysministeriön asetus potilasasiakirjojen laatimisesta ja säilyttämisestä (298/2009)
- Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007)
- Laki sähköisestä lääkemääräyksestä (61/2007)
- Työterveyshuoltolaki (1383/2001)
- Laki terveydenhuollon ammattihenkilöistä (559/1994)
- Mielenterveyslaki (1116/1990)
- Potilasasiakirja-asetus (298/2009)
- STM:n opas terveydenhuollolle, Potilasasiakirjojen laatiminen ja käsittely (2012:4)
- Laki sosiaali-ja terveydenhuollon palveluseteleistä (569/2009)
- Laki viranomaisen toiminnan julkisuudesta (621/1999)

Potilastietoja voidaan käyttää myös tilastointiin ja määrälliseen tutkimukseen. Mikäli käytämme tietoja tällaisiin tarkoituksiin, käyttämämme tiedot ovat anonyymeja tai pseudonymisoituja yleisen tietosuoja- asetuksen edellyttämällä tavalla.

Hoidollisista potilastiedoista erillisenä käsittelemme yhteystietoja sekä laskutustietoja. Laskutuksen ja perinnän osalta käsittelemme tietoja lakisääteisen perusteen vuoksi ja erityisesti kirjanpitolain perusteella (1339/1997) soveltuvin osin.

Potilaille suunnattu viestintä on asiakasviestintää, jossa on kyse joko terveydenhuollon ammattilaisen ja potilaan välisestä viestinnästä tai asiakkaillemme merkittäviä tietoja sisältävistä, palveluntuottajan toimintaa koskevista muutoksista tai tiedotteista.

5. Rekisterin tietolähteet ja tietosisältö

DiabetesSaran potilasrekisterin sisältämät henkilötiedot saadaan DiabetesSaran terveyspalveluita ostavilta tahoilta (yksilö, yritys tai organisaatio) ja DiabetesSara toimii näiden tietojen käsittelijänä. Kun asiakastaho solmii sopimuksen DiabetesSaran kanssa, asiakastaho toimittaa DiabetesSaran palveluita tarvitsevien henkilöiden henkilötiedot DiabetesSaralle lainsäädännön asettamissa rajoissa. Lisäksi tietoja saadaan potilaalta itseltään eri muodoissa tapahtuvien potilaskontaktien

kautta sekä hoitohenkilökunnalta, jotka laativat kirjauksia osallistuessaan potilaan hoitoon ja näiden tietojen osalta DiabetesSara toimii rekisterinpitäjänä. Tietoja voidaan saada asiakkaan suostumuksella myös toisilta terveydenhuollon yksiköiltä tai ammattihenkilöiltä esimerkiksi kansallisen terveysarkiston (KANTA) kautta.

Lakisääteisen velvoitteen perusteella kirjaamme kaikki tiedot, jotka ovat tarpeen potilaan hoidon suunnittelemiseksi, järjestämiseksi, toteuttamiseksi ja seurannan turvaamiseksi. Näihin tietoihin lukeutuu muun muassa esitiedot sekä tutkimuksen ja hoidon yhteydessä kirjattavat terveystiedot. Rekisteri sisältää myös muita potilaan hoidon kannalta oleellisia terveydenhuollon toteutukseen liittyviä tietoja. Hoitoon osallistuvan terveydenhoitohenkilöstön tiedot ja potilaan ajanvaraustiedot tallennetaan.

6. Käsiteltävät henkilötietoryhmät ja niiden säilytysajat

Näiden tietojen osalta DiabetesSara Oy toimii tietojen käsittelijänä:

- Asiakkaan yksilöintitiedot, kuten; nimi, henkilötunnus, sukupuoli, kieli, osoite, ikä, puhelinnumero, sähköpostiosoite ja muut tarpeelliset yhteystiedot. Asiakkaan mahdollisesti nimeämä lähiomainen ja hänen henkilötietonsa
- Tietoja rekisteröidyn käyttämistä palveluista
- Rekisteröidyn suostumuksia ja rekisteröidyn tekemiä muita valintoja koskevat tiedot
- Maksutiedot
- Tunnistamis- ja varmentamisvälineiden ja -palveluiden käyttöön liittyvät tiedot

Näiden tietojen osalta DiabetesSara Oy toimii rekisterin pitäjänä:

- Rekisteröidyn terveyttä koskevat tiedot, sekä muut rekisteröidyn käyttäjän terveydentilaa koskevat tiedot, jotka rekisteröity käyttäjä antaa itse DiabetesSaran palveluiden käytön yhteydessä.
- Tiedon käsittelyyn liittyviä tietoja, kuten tallennuspäivämäärä, tietolähde ja lokitiedot
- Rekisteröidyn käyttäjän ja hoitohenkilökunnan välillä käytyä viestintää koskevat tiedot
- Terveydenhuollon ammattilaisten kirjaamat muut potilaan hoidon kannalta välttämättömät tiedot, kuten työtehtävissä laatimat tiedot.

Rekisteriä suojaavien toimien tarkoituksena on turvata DiabetesSaran palveluiden luottamuksellisuus, tietojen saatavuus sekä rekisteröityjen oikeuksien toteutuminen.

Potilastiedon kohdalla kyse on niin sanotusta erityisestä henkilötiedosta, jolla tarkoitetaan arkaluonteista tietoa. Arkaluonteisen tiedon suojaamiseen on kiinnitetty erityistä huomioita.

DiabetesSara noudattaa tiukasti lainsäädännön asettamia huolellisuus- ja suojaamisuusvelvoitteita sekä hyvää tiedonhallintatapaa käsitellessään potilastietoja.

DiabetesSaran potilasrekisteriin tallennetut potilastiedot ovat lain nojalla salassa pidettäviä. Säilytämme henkilötietoja niin kauan kuin henkilötiedon käyttötarkoituksen vuoksi on tarpeellista, esimerkiksi asiakassuhteen voimassaolon ajan ja nimenomaisen lainsäädännön antaman säilytysajan perusteella. Potilastietoja säilytetään sosiaali- ja terveysministeriön potilasasiakirjoista annetun asetuksen mukaisesti ja tästä tulevia säilytysaikoja noudattaen. Potilasrekisteriin tallennettujen potilastietojen säilytysaika on säädetty sosiaali- ja terveysministeriön asetuksessa 298/2009. Säilytysajan päätyttyä potilastiedot hävitetään. Potilastietojen käsittelyä koskeva lokitiedot säilytetään vähintään 12 vuotta niiden syntymisestä. Lisäksi säilytämme esimerkiksi laskutukseen liittyviä tietoja kirjanpitolainsäädännön mukaisesti ja vakuutuksiin liittyviä tietoja vakuutuksiin liittyvän lainsäädännön perusteella.

DiabetesSara kehittää ja ylläpitää henkilöstön ymmärrystä tietosuojasta mm. osana uuden työntekijän perehdytystä ja tarjoamalla mahdollisuuksia kouluttautumiseen. Salassa pidettävien potilastietojen käsittelyyn osallistuvat henkilöt allekirjoittavat salassapitositoumuksen ennen pääsyoikeuden saamista suojattavaan tietoon. Salassapito- ja vaitiolovelvollisuus jatkuu palvelussuhteen päätyttyäkin.

7. Tietojen luovutukset ja siirrot

DiabetesSaran potilasrekisterin potilastiedot ovat salassa pidettäviä. Tietoja saavat käsitellä vain hoidon ja palvelun toteutukseen tai asian käsittelyyn osallistuvat henkilöt. Potilastietoja käsittelevillä on vaitiolovelvollisuus. Tietojen tallentaja ei voi luovuttaa tietoja itse.

Potilastietoja luovutetaan ensisijaisesti potilaan suostumuksella. Potilastietoja voidaan luovuttaa myös nimenomaisen lainsäännöksen perusteella.

DiabetesSara voi lisäksi luovuttaa potilastietoja seuraaville tahoille:

- Jatkohoitotilanteessa tietoja voidaan luovuttaa potilaan yksilöimälle toiselle terveydenhuollon toimintayksikölle tai terveydenhuollon ammattihenkilölle potilaan potilasasiakirjoihin merkityllä suostumuksella.
- Potilaan tutkimuksen ja hoidon järjestämiseksi tai toteuttamiseksi välttämättömiä tietoja voidaan luovuttaa toiselle suomalaiselle tai ulkomaiselle terveydenhuollon toimintayksikölle tai terveydenhuollon ammattihenkilölle ilman potilaan suostumusta, jos potilaalla ei ole mielenterveydenhäiriön, kehitysvammaisuuden tai muun vastaavan syyn vuoksi edellytyksiä arvioida annettavan suostumuksen merkitystä eikä hänellä ole laillista edustajaa.

- Kansallinen terveysarkisto (KANTA-arkisto). Potilastiedot siirretään potilaan itse suorittaman hyväksynnän jälkeen KANTA-arkistoon ja potilaan tulee hallinnoida näitä tietoja OMAKANTA-järjestelmästä www.omakanta.fi
- Vakuutusyhtiölle, jos potilas on antanut suostumuksen.
- Potilaan huoltajalle, muulle lailliselle edustajalle tai potilaan lähiomaiselle, jos potilas on antanut tähän suostumuksensa.
- Tajuttomuuden tai muun siihen verrattavan syyn vuoksi hoidettavana olevan potilaan lähiomaiselle tai muulle hänen läheiselleen tieto potilaan henkilöstä ja hänen terveydentilastaan, jollei ole syytä olettaa, että potilas kieltäisi näin menettelemästä.

DiabetesSara ei siirrä potilastietoja EU/ETA-alueen ulkopuolelle.

Terve Päivä -palvelu

- Palvelun käytön hyväksymällä DiabetesSaralla on oikeus siirtää asiakastiedot Terve Päivä -palveluun.
- Asiakkaalla on oikeus lopettaa palvelun käyttö milloin tahansa, perumalla asiakkuuden osoitteeseen asiakaspalvelu@diabetessara.fi. Asiakkuus päätetään kuluvan laskutusjakson loppuun.

8. DiabetesSaran potilas- ja asiakastiedon käsittelijät ja käsittelyssä käytettävät järjestelmät

Hoidollista potilastietoa käsitellään vain DiabetesSaran potilastietojärjestelmässä (Diarium).

Alla mainitut toimittajat käsittelevät laskutukseen, perintään ja asiakasviestintään liittyviä henkilötietoja DiabetesSaran toimeksiannosta ja lukuun omia tietojärjestelmiään hyödyntäen:

- Nordhealth Oy, Y-2162673-1 (Diarium ja Navisec Health)
- Lahden Tulosdata Oy, Y-0958770-9 (Taloushallinto)
- Synlab Suomi Oy, Y-2674625-7 (Laboratoriopalvelut)
- Platta Martetplaces Oy, Y-3087782-3 (Epassi)
- Paytrail Oy, Y-2122839-7 (Maksunvälitys)
- Finqu Oy, Y-2764177-2 (Verkkokauppa)

Toimittajilla on oikeus käyttää alihankkijoita henkilötietojen käsittelijöinä. Toimittaja vastaa lainsäädännön velvoittamalla tavalla omien alihankkijoidensa toimista ja tämän sopimuksen tai tietosuojalainsäädännön laiminlyönneistä suhteessa DiabetesSaraan.

9. Henkilötietojen käsittelyyn liittyvät rekisteröidyn oikeudet

Potilaan oikeus saada pääsy tietoihin (tarkastusoikeus)

Jokaisella potilaalla on oikeus tarkastaa DiabetesSaran potilastietorekisteriin tallennetut potilasta itseään koskevat henkilötiedot. Potilaalla on myös oikeus tarkastaa potilastietojensa käsittelyä koskevat lokitiedot. Tarkastuspyyntö tehdään lähettämällä tarkastuspyyntö sähköisesti allekirjoitettuna DiabetesSara Oy:lle. Yhteystiedot löytyvät tästä selosteesta. Pyynnön voi myös esittää henkilökohtaisesti jokaiselle DiabetesSaran työntekijälle. Potilaan henkilöllisyys varmennetaan luotettavalla tavalla riippumatta siitä, millä edellä mainituilla tavoilla pyyntö tehdään. Tarkastuspyynnön voi tehdä maksutta kerran vuodessa. Tarkastuspyyntöön vastataan viivytyksettä, yleensä kahden viikon kuluttua pyynnön esittämisestä. Tarkastusprosessin hoitaa, ja tiedot luovuttaa tietosuojavastaava.

Potilaan oikeus vaatia tiedon oikaisemista tai käsittelyn rajoittamista

DiabetesSaralla on velvollisuus ilman aiheetonta viivytystä oma-aloitteisesti tai potilaan vaatimuksesta oikaistava tai täydennettävä DiabetesSaran potilasrekisterissä oleva virheellinen henkilötieto. Jokaisella asiakkaalla on oikeus saada epätarkka ja virheellinen tieto oikaistuksi. Asiakkaalla on myös oikeus saada puutteelliset henkilötiedot täydennettyä. Tietojen korjauspyyntö tehdään ottamalla yhteyttä DiabetesSaran tietosuojavastaavaan tai lähettämällä pyyntö sähköisesti allekirjoitettuna DiabetesSara Oy:lle. Korjauspyyntö on yksilöitävä ja perusteltava. Potilaan henkilöllisyys varmennetaan luotettavalla tavalla riippumatta siitä, millä edellä mainituilla tavoilla pyyntö tehdään. Tarkastusprosessin hoitaa ja virheellisen tiedon korjaamisesta vastaa tietosuojavastaava. Potilaalla on myös oikeus vaatia käsittelyn rajoittamista. Tämä oikeus voi tulla kyseeseen esimerkiksi silloin, kun potilas kiistää henkilötietojensa paikkansapitävyyden ja potilas odottaa DiabetesSaran vastausta tietojen oikaisemista koskevaan pyyntöön.

Asiakkaalla on oikeus kieltää rekisterinpitäjää käsittelemästä häntä itseään koskevia tietoja suoramainontaa, etämyyntiä ja muuta suora- markkinointia sekä markkina- ja mielipidetutkimusta tai muuta tutkimusta varten. Tietojen korjauspyyntö tehdään ottamalla yhteyttä DiabetesSaran tietosuojavastaavaan tai lähettämällä pyyntö sähköisesti allekirjoitettuna DiabetesSara Oy:lle. Pyynnön voi myös esittää henkilökohtaisesti DiabetesSaran työntekijälle.

Potilaan oikeus tehdä valitus valvontaviranomaiselle

Potilaalla on oikeus tehdä valitus toimivaltaiselle valvontaviranomaiselle, jos rekisterinpitäjä ei ole noudattanut soveltuvaa tietosuojasääntelyä toiminnassaan. Suomessa toimivaltainen valvontaviranomainen on tietosuojavaltuutettu.

10. Tietoturvaloukkaus, informointivelvollisuus ja yhteydenotot

Jos DiabetesSara havaitsee henkilötietojen tietoturvaloukkauksen, on sen ilmoitettava siitä ilman aiheetonta viivytystä ja viimeistään 72 tunnin sisällä loukkauksen ilmitulosta tietosuojavaltuutetulle ja rekisteröidylle, mikäli tietosuojaloukkauksesta aiheutuu todennäköisesti luonnollisen henkilön oikeuksiin ja vapauksiin kohdistuvaa riskiä. DiabetesSara suojaa kaikki henkilötiedot niin, että suojaustoimenpiteet vastaavat henkilötietojen käsittelyyn liittyvää riskiä. DiabetesSara on varautunut mahdollisiin tietoturvaloukkauksiin laatimalla toimintaohjeet henkilöstölle tietoturvaloukkauksia varten.

Mikäli sinulla on kysyttävää potilastietojesi käsittelystä tai omien oikeuksiesi käyttämisestä, voit olla yhteydessä DiabetesSara tietosuojavastaavaan teija.vorlin@diabetessara.fi.

Arkaluonteisia tietoja ei kuitenkaan tule lähettää sähköpostitse. Arkaluonteista sähköpostiviestintää varten DiabetesSara Oy:llä on käytössä suojattu sähköpostiyhteys, jonne tunnistaudutaan vahvalla tunnistautumisella. Salatun sähköpostisoitteen saamiseksi ota yhteyttä asiakaspalvelu@diabetessara.fi