TIETOSUOJASELOSTE

Päivitetty: 21.12.2018

Tämä tietosuojaseloste kuvaa, kuinka käytämme ja käsittelemme BuddyCare-sovelluksen rekisteröidyistä keräämiämme tietoja.

1. Yleiset määritelmät

“Palvelulla” tai “sovelluksella” tarkoitetaan tämän tietosuojaselosteen osalta BuddyCare-sovellusta kattaen mobiilisovelluksen ja mahdollisen verkkosovelluksen.

“Rekisteröidyllä” tarkoitetaan tämän tietosuojaselosteen osalta henkilö(it)ä, jo(t)ka rekisteröidään palveluun. Rekisteröity voi olla esimerkiksi hoitoon tuleva potilas.

“Käyttäjällä” tarkoitetaan tämän tietosuojaselosteen osalta palvelua käyttävää tahoa. Palvelua käyttävä taho voi olla esimerkiksi alaikäisen potilaan laillinen huoltaja, joka käyttää palvelua jonkun toisen rekisteröidyn puolesta.

“Henkilötiedoilla” tarkoitetaan yleisesti kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön, jäljempänä ’rekisteröity’, liittyviä tietoja; tunnistettavissa olevana pidetään luonnollista henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen, kuten nimen, henkilötunnuksen, sijaintitiedon, verkkotunnistetietojen taikka yhden tai useamman hänelle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella.

“Rekisterinpitäjällä” tarkoitetaan tämän tietosuojaselosteen osalta tahoa, joka vastaa sovelluksen avulla tuotettavasta palvelusta rekisteröidylle. Rekisterinpitäjä määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot. Rekisterinpitäjä voi olla esimerkiksi hoitoyksikkö, johon potilas tulee hoitoon.

“Palveluntarjoajalla” tarkoitetaan tämän tietosuojaselosteen osalta tahoa, jonka nimissä palvelu tarjotaan sovelluskaupoissa tai verkkosivuilla.

“Palveluntuottajalla” tarkoitetaan tämän tietosuojaselosteen osalta Buddy Healthcare Ltd Oy:tä (www.buddyhealthcare.com) ja mahdollisesti sen samaan konserniin kuuluvia yhtiöitä, jotka kehittävät ja ylläpitävät palvelua, jota palveluntarjoaja tarjoaa käyttäjillensä.

“Terveystiedoilla” tarkoitetaan yleisesti luonnollisen henkilön fyysiseen tai psyykkiseen terveyteen liittyviä henkilötietoja, mukaan lukien tiedot terveyspalvelujen tarjoamisesta, mitkä ilmaisevat hänen terveydentilansa.

“Profiloinnilla” tarkoitetaan yleisesti mitä tahansa henkilötietojen automaattista käsittelyä, jossa henkilötietoja käyttämällä arvioidaan luonnollisen henkilön tiettyjä henkilökohtaisia ominaisuuksia. Erityisesti tämän tietosuojaselosteen osalta tarkoitetaan seuraavien piirteiden analysointia tai ennakointia, jotka liittyvät kyseisen luonnollisen henkilön terveyteen ja käyttäytymiseen.

2. Rekisterinpitäjä ja rekisterinpitäjän yhteystiedot

Rekisterinpitäjän vastuulla on määritellä henkilötietojen käsittelyn tarkoitukset ja keinot palvelun osalta.

Rekisterinpitäjänä toimii se taho, jonka asiakkaana käyttäjä tai rekisteröity rekisteröityy palveluun.

Rekisterinpitäjän yhteystiedot löytyvät sovelluksesta siihen kirjautumisen jälkeen.

3. Palveluntuottaja ja palveluntuottajan yhteystiedot

Palveluntuottaja vastaa palvelun tuottamisesta ja käsittelee henkilötietoja rekisterinpitäjän lukuun.

Palveluntuottajan yhteystiedot:

Nimi: Buddy Healthcare Ltd Oy

Osoite: Kuortaneenkatu 2, 00510 Helsinki

Tietosuojavastaavan nimi: Jukka Hassinen

Sähköposti: privacy@buddyhealthcare.com

Puhelin: +358 20 735 2310

4. Rekisterin nimi

Palvelun käyttäjärekisteri

5. Henkilötietojen käsittelyn tarkoitus sekä käsittelyn oikeusperusta

Henkilötietojen käsittelyn oikeusperuste on rekisterinpitäjän oikeutettu etu ja palvelun käyttäjän antama suostumus palvelun käyttöön. Henkilötietojen käsittelyn tarkoitus on tarjota rekisterinpitäjälle rekisteröidystä hoitoon liittyvää tietoa, jonka palvelu automaattisesti rekisterinpitäjälle välittää, tai jonka käyttäjä itse palvelussa syöttää ja toimittaa rekisterinpitäjälle. Kerättyjä henkilötietoja voidaan käyttää myös yhteydenpitoon rekisteröityyn ja/tai käyttäjiin.

6. Rekisterin tietosisältö

Rekisteri sisältää seuraavat tiedot rekisteröidystä ja käyttäjästä:

Rekisteröidystä tallennetaan:

- Koko nimi (etu- ja sukunimi)
- Henkilötunnus (rekisteröidyn yksilöimiseksi)
- Hoitoon tai sovelluksen käyttöön liittyvien käyntien tarkoitus ja ajat
- Taho, jonka asiakkaana rekisteröity on
- Käyttäjän mahdollisesti lataama kuva rekisteröidystä
- Käyttäjän palvelussa tekemien tehtävien aikaleima
- Käyttäjän palvelussa syöttämät tiedot, kuten lomakkeiden vastaukset

Käyttäjästä tallennetaan lisäksi:

- Puhelinnumero tai sähköpostiosoite
- Käyttäjän mahdollisesti käymät keskustelut esim. oman hoitotahonsa kanssa sovelluksessa.
- Askelmittarin tallentamat tiedot, jos se on osa palvelun hoitopolkua ja käyttäjä on erikseen antanut luvan askeltietojen keräämiselle

Käyttäjästä tallentuu lisäksi seuraavat tekniset tiedot (myöhemmin “tekniset tiedot”) palvelun käytön yhteydessä, jotta mahdolliset väärinkäyttö- ja vikatilanteet saadaan jäljitettyä sekä mahdollisia palvelussa esiintyviä virheitä voidaan selvittää:

- IP-osoitteet, joista palvelua on käytetty
- Käyttäjän mobiililaitteen tai Internet-selaimen valmistaja ja malli
- Päivämäärät ja kellonajat, jolloin sovellusta on käytetty

7. Henkilötietojen säilytysaika

Henkilötietoja säilytetään palvelussa niin kauan kuin esimerkiksi hoidon kannalta on tarpeen, ja tämän jälkeenkin tiettyjä tietoja säilytetään lakien edellyttämällä tavalla. Tällaisia tietoja ovat esimerkiksi lain määräämät lokitiedot ja arkistointivaatimukset.

Palveluntuottaja ja palveluntarjoaja voivat säilyttää palvelussa lisäksi anonymisoitua eli ei-yksilöivää henkilötietoa säilytysajan jälkeenkin. Anonymisoidut tiedot on tarkoitettu käytettäväksi kappaleen 12 mukaiseen profilointiin ja tilastollisiin tarkoituksiin palvelun kehittämistä varten.

8. Säännönmukaiset tietolähteet

Tietolähteitä ovat:

- Hoitotaho, jonka asiakkaana rekisteröity on. Rekisteröidyistä ja palvelun käyttäjistä kerättävät tiedot siirretään joko manuaalisesti palveluun hoitotahon toimesta tai automaattisesti tietojärjestelmäintegraation kautta kutsun yhteydessä.
- Käyttäjän antamat tiedot palvelussa, kuten esimerkiksi rekisteröitymisen yhteydessä antamat yhteystiedot, palvelun käytön yhteydessä annetut vastaukset kyselyihin, hoitopolkujen tehtävien aikaleimat, lataamansa kuvat sekä mahdollisesti erillisten kytkettyjen mittalaitteiden tiedot, kuten askelmittaritiedot.
- Käyttäjästä automaattisesti kerättävät tekniset tiedot palvelun käytön yhteydessä, kuten IP-osoite, palvelun käytön ajankohdat, päätelaitteen malli ja merkki sekä sovellusversio.

Palveluun rekisteröidytään käyttäjäksi hoitotahosta riippuen joko vahvalla tunnistautumisella tai hoitotahon aloitteesta käyttäjälle luodulla uniikilla aika- ja käyttökertarajoitetulla aktivointikoodilla, ja käyttäjän puhelinnumerolla tai sähköpostiosoitteella sekä käyttäjän asettamalla salasanalla. Luotua käyttäjätunnusta ja salasanaa käytetään myöhemmin sovellukseen sisäänkirjautumiseen, mikäli käyttäjä kirjautuu sovelluksesta ulos. Käyttäjän vastuulla on huolehtia, että käyttäjätunnus ja salasana eivät joudu väärien henkilöiden käyttöön.

9. Tietojen säännönmukaiset luovutukset

Käyttäjän palvelussa syöttämät ja lähettämät tiedot välitetään hoitotaholle, jonka asiakkaana rekisteröity on. Rekisterinpitäjä huolehtii tästä eteenpäin tietojen käsittelystä omien periaatteidensa mukaisesti.

Rekisteröityjen henkilötiedot tallennetaan palveluntuottajan hallinnoimaan suojatuun palvelinympäristöön.

Palveluntarjoaja käyttää myös osana palvelun tuottamista apuna seuraavan tyyppisiä kolmannen osapuolen palveluita, joiden käytön yhteydessä he käsittelevät osaa henkilötiedoiksi luokiteltavia asioista seuraavasti:

- Pilvipalvelinympäristö ja tietokanta (kaikki tiedot)
- Kuvien säiltytys ja jakeliminen (kuvat)
- Tekstiviestien välittäminen (puhelinnumero)
- Sovelluskaupat kuten App Store ja Play Store
- Push-ilmoitusten lähettäminen Android-laitteisiin (käyttäjän käyttämä laitetyyppi ja IP-osoite)
- Google Maps -karttapalvelun käyttäminen Android-laitteilla (käyttäjän IP-osoite ja käyttäjän Google-tunnus)
- Push-ilmoitusten lähettäminen iOS-laitteisiin (käyttäjän käyttämä laitetyyppi ja IP-osoite)
- Apple Maps -karttapalvelun käyttäminen iOS-laitteilla (käyttäjän IP-osoite ja Apple-tunnus)
- Sähköpostiviestien lähettäminen (nimi ja sähköpostiosoite)
- Järjestelmän lokitiedot (IP-osoite, käyttäjän päätelaitteen malli tyyppi ja käyttöjärjestelmäversio)
- Hälytykset virhetilanteista palveluntuottajan ylläpito- ja sovelluskehityshenkilökunnalle (IP-osoite, käyttäjän päätelaitteen malli tyyppi ja käyttöjärjestelmäversio)
- Vahva tunnistautuminen (henkilötunnus, nimitiedot, IP-tunnus, käyttäjän päätelaitteen malli tyyppi ja käyttöjärjestelmäversio)

10. Tietojen siirto EU:n tai ETA:n ulkopuolelle

Palvelun keräämät henkilötiedot tallennetaan kappaleen 9 mukaisesti pääosin Euroopan unionin alueella oleville palvelimille, mutta osaa henkilötiedoiksi luokiteltavista asioista käsitellään myös EU:n ja Euroopan talousalueen ulkopuolisten organisaatioiden toimesta.

Tietojen siirto osana palvelun käyttöä EU:n ja ETA:n ulkopuolelle perustuu EU:n yleisen tietosuoja-asetuksen (2016/679) edellytyksiin kuten kohdemaan riittävään tietosuojan tasoon (Privacy Shield -mekanismin kautta - https://www.privacyshield.gov) ja EU-komission hyväksymiin vakiosopimuslausekkeisiin.

Applen palveluiden käyttäminen iOS-laitteilla kuten push-ilmoitusten vastaanottaminen Apple Push Notification servicen (APNs) kautta ja Apple Maps -karttapalvelun käyttäminen perustuu käyttäjän antamaan suostumukseen.

11. Rekisterin suojauksen periaatteet

Käytämme tarpeellisia teknisiä, fyysisiä, hallinnollisia, sopimuksellisia ja organisatorisia turvakeinoja henkilötietojen suojaamiseksi asiattomalta pääsyltä tietoihin ja vahingossa tai laittomasti tapahtuvalta tietojen hävittämiseltä, muuttamiselta, luovuttamiselta, siirtämiseltä tai muulta laittomalta käsittelyltä.

Henkilötietoihin on pääsy vain siihen oikeutetun työntekijän tai hoitoon osallistuvan ammattihenkilön henkilökohtaisella käyttäjätunnuksella. Käyttöoikeuksia on eritasoisia ja kullekin käyttäjälle annetaan tehtävän hoitamisen kannalta riittävä, mutta mahdollisimman suppea käyttöoikeus. Rekisteröidyllä on oikeus katselmoida palveluun tallennettuja henkilötietoja. Tämän rekisteröity voi sopia esimerkiksi hoitotahon kanssa mahdollisen hoitokäynnin yhteydessä.

Rekisteröity voi myös itse antaa palvelun perheprofiiliin liitetyille henkilöille oikeuden tarkastella ja käsitellä palveluun tallennettuja rekisteröityä koskevia tietoja, sekä oikeuden saada rekisteröidyn henkilötietoihin vastaava rajoitettu katseluoikeus kuin rekisteröidyllä itsellään on. Palvelun perheprofiiliin voidaan liittää vain sellaisia henkilöitä, jotka ovat itse palvelun käyttäjiä ja näin ollen myös rekisteröityjä. Lisääminen tapahtuu henkilötunnuksen avulla. Hoitotaho voi oman käytäntönsä mukaan lisätä alle 18-vuotiaan laillisen huoltajan tämän perheprofiiliin ilman lapsen suostumusta.

12. Profilointi

Palveluntuottaja tallentaa anonymisoitua eli ei-yksilöivää tietoa rekisteröidyistä, jonka perusteella muodostetaan tilastollinen malli. Tämän tilastollisen mallin perusteella arvioidaan rekisteröityjen kuulumista tiettyihin ryhmiin, joihin kuulumisen perusteella palvelussa kohdistetaan erityistä huomiota (kuten tarkistavaa viestintää) tai palvelua personoidaan käyttäjälle.

Palvelu voi pyrkiä tunnistamaan palveluun rekisteröityjen profiilista esimerkiksi sen, milloin rekisteröity kuuluu seuraaviin riskiryhmiin:

- Hoidon tai hoitotapahtuman peruuntuminen tai siirtyminen on todennäköistä palvelun keräämien tietojen perusteella
- Hoitotoimenpiteestä aiheutuva komplikaatio on mahdollinen palvelun keräämien tietojen perusteella

Palvelu tai hoitotaho voi profiilin perusteella kohdentaa riskiryhmiin kuuluviin henkilöihin tarkempaa huomiota esimerkiksi varmentavaa viestintää, jotta hoidon onnistuminen taataan parhaalla mahdollisella tavalla.

13. Rekisteröidyn oikeudet

13.1 Rekisteröidyn oikeus saada pääsy tietoihin (tarkastusoikeus)

Kirjautuessaan sisään palveluun käyttäjällä on aina nähtävillä suurin osa niistä tiedoista, joita palvelu hänestä kerää.

Rekisteröidyllä on myös oikeus tarkastaa, mitä muita häntä koskevia tietoja palveluun on tallennettu. Tarkastuspyyntö tulee tehdä tämän tietosuojaselosteen kohdan 14 mukaisesti. Tarkastusoikeus voidaan evätä laissa säädetyin perustein. Tarkastusoikeuden käyttäminen on lähtökohtaisesti maksutonta, mutta mikäli tietoja pyydetään uudelleen samalta ajanjaksolta, voidaan rekisteröityä laskuttaa siitä aiheutuneista kustannuksista.

13.2 Rekisteröidyn oikeus vaatia tiedon oikaisemista, poistamista tai käsittelyn rajoittamista

Rekisteröity voi päivittää omia perustietojaan palvelussa. Siltä osin kuin rekisteröity voi toimia itse, hänen on ilman aiheetonta viivytystä saatuaan tiedon virheestä tai virheen itse havaittuaan, oma-aloitteisesti oikaistava, poistettava tai täydennettävä rekisterissä oleva, Palvelun tarkoituksen vastainen, virheellinen, tarpeeton, puutteellinen tai vanhentunut tieto.

Siltä osin kuin rekisteröity ei pysty korjaamaan tietoja itse, korjauspyyntö tehdään tämän tietosuojaselosteen kohdan 14 mukaisesti.

13.3 Rekisteröidyn oikeus vaatia tiedon poistamista

Rekisteröidyllä on myös oikeus vaatia rekisterinpitäjää poistamaan henkilötietoja siltä osin kuin se on lain mukaan mahdollista.

13.4 Rekisteröidyn oikeus vaatia käsittelyn rajoittamista

Rekisteröidyllä on myös oikeus vaatia rekisterinpitäjää rajoittamaan henkilötietojensa käsittelyä esimerkiksi siinä tilanteessa, kun rekisteröity odottaa rekisterinpitäjän vastausta tietojensa oikaisemista tai poistamista koskevaan pyyntöön.

13.5 Rekisteröidyn oikeus siirtää tiedot järjestelmästä toiseen

Siltä osin kuin rekisteröity on itse syöttänyt palveluun tietoja, joita käsitellään rekisteröidyn antaman suostumuksen nojalla, rekisteröidyllä on oikeus saada tällaiset tiedot itselleen pääsääntöisesti koneluettavassa muodossa. Rekisteröidyllä on myös oikeus siirtää nämä tiedot toiselle rekisterinpitäjälle. Tällaisia tietoja ovat esimerkiksi rekisteröidyn itse palveluun syöttämät rekisteröidyn terveyttä tai aiempaa hoitohistoriaa kuvaavat tiedot.

13.6 Rekisteröidyn oikeus tehdä valitus valvontaviranomaiselle

Rekisteröidyllä on oikeus tehdä valitus toimivaltaiselle valvontaviranomaiselle, jos rekisterinpitäjä ei ole noudattanut toiminnassaan soveltuvaa tietosuojasääntelyä.

13.7 Muut oikeudet

Mikäli henkilötietoja käsitellään rekisteröidyn suostumukseen perustuen, rekisteröidyllä on oikeus peruuttaa suostumuksensa ilmoittamalla tästä rekisterinpitäjälle.

14 Yhteydenotto

Kaikissa henkilötietojen käsittelyyn liittyvissä kysymyksissä ja omien oikeuksien käyttämiseen liittyvissä tilanteissa rekisteröidyn tulee ottaa yhteyttä rekisterinpitäjään. Rekisterinpitäjän yhteystiedot löytyvät palvelusta sisäänkirjautumisen jälkeen.

Pyynnössä tulee tehdä selväksi, mitä tietoa haluatte muuttaa, poistaa, tarkistaa tai päivittää taikka minkä tiedon käsittelylle haluatte asettaa muita rajoituksia. Rekisterinpitäjä pyrkii ottamaan pyyntönne huomioon mahdollisimman nopeasti. Ymmärrättehän, että joidenkin tietojen korjaaminen, päivittäminen tai poistaminen saattaa tarkoittaa sitä, että tilinne joudutaan hetkellisesti poistamaan käytöstä, jolloin pääsynne palveluun ei ole mahdollista. Tässä tapauksessa emme ole korvausvelvollisia aiheuttamastamme haitasta.

Rekisterinpitäjä voi tarvittaessa pyytää rekisteröityä täsmentämään pyyntöään kirjallisesti, ja rekisteröidyn henkilöllisyys voidaan tarpeen vaatiessa varmentaa ennen muihin toimenpiteisiin ryhtymistä.

15 Muutokset tähän tietosuojaselosteeseen

Rekisterinpitäjällä on oikeus tehdä tähän tietosuojaselosteeseen muutoksia osana omia ja/tai palvelun kehitystoimenpiteitä tai lainsäädännön muuttuessa. Päivitetty tietosuojaseloste julkaistaan palvelussa ja jatkaakseen palvelun käyttöä käyttäjän tulee hyväksyä päivitetty tietosuojaseloste, mikäli muutokset tietosuojaselosteeseen vaikuttavat henkilötietojen käsittelyyn tai muuttavat henkilötietojen käsittelyn periaatteita.