TIETOTILINPÄÄTÖS 18.4.2018

EST 1994

CITYKLINIKKA

ANNA HYVINVOINTISI NÄKYÄ.

1. Johdanto

Tämä on Medipol Oy:n (myöhemmin ”Cityklinikka”) ensimmäinen tietotilinpäätös, joka laadittiin huhtikuussa 2018, ennen EU:n tietosuoja-asetuksen (”GDPR”) voimaan tuloa. Tilinpäätöksen tehtävänä on osoittaa, että Cityklinikka noudattaa vuonna 2018 sovellettavaksi tulevan yleisen tietosuoja-asetuksen mukaista tilintekovelvollisuusperiaatetta.

Esteettisen lääketieteen ja plastiikkakirurgian alalla toimivalle yritykselle tietojenkäsittelyn lainmukaisuus on ollut aina erityisen tärkeää, koska alan yrityksessä käsitellään luottamuksellista ja salassa pidettävää tietoa.

Potilastietoja Cityklinikalla käsitellään Skalpell-potilastietojärjestelmässä ja Visiatietojärjestelmässä. Laki määrittelee yleiset vaatimukset tietojärjestelmille ja niiden valmistajille. Potilastietojärjestelmä Skalpell on luokiteltu Euroopan Unionissa terveydenhuollon laitteeksi (luokka 1), ja tietojärjestelmän valmistaja Metodika on vastuussa järjestelmän vaatimustenmukaisuuden osoittamisesta. Visia-järjestelmän vaatimustenmukaisuuden osoittamisesta vastaavat Canfield ja järjestelmän suomalainen maahantuoja Melon Oy.

Asiakkaat ottavat yhteyttä Cityklinikkaan puhelimitse, sähköpostitse sekä verkkosivujen yhteydenottolomakkeiden avulla. SSL-suojattujen verkkosivujen kautta tulleista yhteydenotoista on tehty tietosuojaa koskeva sopimus verkkosivuston ylläpidon (Applari Oy) kanssa. Yhteydenottopyyntöä säilytetään vuoden ajan, ellei pyyntö johda asiakassuhteeseen.

Osa toimenpiteistä on myynnissä Cityklinikan SSL-suojatussa verkkokaupassa. Cityklinikan verkkosivusto on SSL-suojattu. Tietojen käsittelijänä toimivan suomalaisen MyCashflow´n kanssa on tehty tietosuojaa koskeva sopimus.

Myös sähköpostiliikenteessä Cityklinikka käyttää suojattua yhteyttä. Suojatun sivuston tunnistaa selaimen osoitekentän vieressä olevasta lukon kuvasta sekä https-alkuisesta osoitteesta.

Cityklinikka kerää tietoa ensisijaisesti potilaiden/asiakkaiden hoidon suunnittelua, toteutusta, seurantaa ja laskutusta varten. Yritystoiminnan laajentumisen myötä tietoa on alettu kerätä myös yhteistyöhankkeiden toteuttamista varten. Lisäksi tietoa kerätään asiakaspalvelun ja liiketoiminnan kehittämistä varten sekä viestinnän tarpeisiin. Henkilöstöasioiden hoitamisessa hyödynnetään rekisteriä, joka sisältää tietoa Cityklinikan ammattihenkilöstöstä.

2. Uusi lainsäädäntö

EU:ssa hyväksytty tietosuoja-asetus tulee sovellettavaksi 25.5.2018 alkaen. Asetuksen tavoitteena

on luoda EU-kansalaisia koskeva yhtenäinen tietosuojasääntely. Tässä tietotilinpäätöksessä arvioidaan tulevan tietosuoja-asetuksen vaatimuksia Cityklinikan henkilötietojen käsittelylle.

Cityklinikan toiminnan kannalta uusi asetus ei vaadi laajamittaisia toimenpiteitä, koska jo nyt alaa säädellään varsin yksiselitteisillä laeilla. Laissa potilaan asema ja oikeudet on tarkoin määritelty. Muun muassa potilasasiakirjojen käsittelyä, hallintaa ja säilytystä koskeva lainsäädäntö vaikuttaa Cityklinikan tietojen käsittelemiseen jo nyt laajemmin kuin sovellettavaksi tuleva tietosuoja-asetus. Uusi asetus ei tämän vuoksi tuo varsinaisia muutoksia Cityklinikan toimintaan.

Merkittävin muutos on rekisterinpitäjän (Cityklinikka) osoitusvelvollisuus: Cityklinikan tulee kyetä luotettavasti osoittamaan, että yrityksessä toimitaan asetuksen ja muun lainsäädännön mukaisesti. Toinen muutos entiseen on se, että uuden asetuksen lähtökohtana on riskipohjainen lähestymistapa: henkilötietojen käsittelemiseen liittyvät riskit on arvioitava jo etukäteen, ennen käsittelyn alkamista.

Koska Cityklinikalla käsitellään terveydentilatietoja, yrityksessä on tehty myös tietosuojaa koskeva, riskiperusteinen vaikutustenarviointi. Mikä tärkeintä, myös potilastietojärjestelmää ylläpitävä yritys on tehnyt tietojärjestelmää koskevan laajan, riskiperusteisen vaikutustenarvioinnin.

2.1 Osoitusvelvollisuus

Uutta asetusta ei voi noudattaa vain käsittelemällä tietoja asianmukaisesti. 25.5.2018 lähtien tietojen lainmukainen käsitteleminen täytyy pystyä myös osoittamaan. Henkilötietojen käsittelemiseen liittyvät prosessit sekä tietosuojatoimenpiteet pitää dokumentoida. Dokumenteista tulee käydä ilmi, että tietoja käsitellään lainmukaisesti. Tietosuojatoimenpiteiden tulee olla läpinäkyviä ja suunnitelmallisia.

Cityklinikka osoittaa noudattavansa lakia monentyyppisillä tietosuojaselosteilla. Tärkein tietosuojaseloste koskee potilastietorekisteriä.

2.2 Sisäänrakennettu ja oletusarvoinen tietosuoja

Tietosuojan tulee olla luovuttamaton osa henkilötietojen käsittelemistä. Puhutaan sisäänrakennetusta tietosuojasta, joka on terveydenhuollon alalla toimiville lähtökohtainen vaatimus.

Uusi tekniikka ja uudet viestintävälineet ovat tuoneet tietosuojaan uusia ulottuvuuksia. Koska esteettisellä lääkäriklinikalla käsitellään potilastietoja, uudet tekniikat ja viestintävälineet tulee arvioida erityisen huolella. Oletusarvoisesti henkilötietoja tulee käsitellä aina niin suppeasti kuin mahdollista.

2.3 Tietoturvaloukkauksista ilmoittaminen

Tietosuoja-asetuksen mukaan henkilötietojen tietoturvaloukkauksesta on tehtävä ilmoitus 72 tunnin kuluessa loukkauksen ilmitulosta. Koska Cityklinikalla käsiteltyjen tietojen loukkaus aiheuttaisi korkean riskin rekisteröityjen oikeuksille, tietoturvaloukkauksesta olisi ilmoitettava myös rekisteröidyille itselleen, vaikka Cityklinikan potilastietojärjestelmässä potilastiedot ovat aina salatussa muodossa.

Tietoturvaloukkauksia varalle on Cityklinikalla luotu prosessit. Potilastietojen osalta suurin osa prosessisuunnitelmasta tulee suoraan potilastietojärjestelmän ylläpitäjältä.

Muihin kuin potilasrekistereihin kohdistuvat tietoturvaloukkaukset käsitellään yrityksen sisällä laadittujen ohjeiden mukaan. Tiedottajan suunnittelema kriisiviestintäsuunnitelma luo pohjan toiminnalle mahdollisissa tietoturvaloukkaustilanteissa.

3. Sopimukset henkilötietojen käsittelijöiden kanssa

Henkilötietojen käsittelijä on uuden asetuksen mukaan luonnollinen tai oikeushenkilö, joka käsittelee rekisteröityjen henkilötietoja rekisterinpitäjän (tässä tapauksessa Cityklinikan) lukuun. Cityklinikalla on kartoitettu kaikkien rekistereiden osalta henkilötietojen käsittelijät. Heidän kanssaan on tehty tai ollaan tekemässä kirjalliset sopimukset tietosuoja-asetuksen noudattamisesta.

Uusissa yhteistyö-, kumppanuus- ja alihankintasopimuksissa tietosuoja-asetuksen vaatimukset tullaan ottamaan huomioon alusta lähtien.

4. Tietosuojavastaava

Cityklinikka on pk-yritys, jonka ydintehtävät eivät muodostu henkilötietojen käsittelystä. Tämän vuoksi yrityksessä ei ole nimetty tietosuojavastaavaa. Tietosuoja-asetuksen noudattamiseen liittyviä tehtäviä on yrityksessä jaettu:

- Vastuu tietosuoja-asetuksen noudattamisesta on yrityksen johdolla.
- Potilasasiamies toimii potilastietorekisterissä olevien henkilöiden yhteyshenkilönä.
- Tiedottaja toimii digiviestintärekisterissä ja muissa ei-potilastietorekistereissä olevien henkilöiden yhteyshenkilönä.
- Henkilöstön tietosuoja-asioissa yhteyshenkilönä toimii toimistovastaava.
- Tiedottajan tehtävänä on pitää yrityksen ylin johto sekä henkilöstö informoituna tietosuojaasetuksen vaatimuksista.

5. Rekisteröityjen oikeudet

Tietosuoja-asetuksessa säädetyistä rekisteröityjen oikeuksissa on uusia oikeuksia sekä joitakin tarkennuksia nykyisiin oikeuksiin. Oikeuksien soveltaminen ja tulkinta ei ole kaikilta osin selvää. Muun muassa Cityklinikalla odotetaan EU:n tietosuojaryhmän ohjeita ja tulevaisuuden oikeuskäytäntöjä.

5.1 Oikeus saada tietoa henkilötietojen käsittelystä

Rekisterinpitäjänä Cityklinikalla on velvollisuus tiedottaa avoimesti henkilötietojen käsittelystä. Tiedon tulee olla tiiviissä ja ymmärrettävässä muodossa ja helposti saatavissa. Cityklinikan potilastietorekisteriä ja digiviestinnän rekisteriä koskevat tietosuojaselosteet on pyritty laatimaan hyvällä suomen kielellä. Tietosuojaselosteet löytyvät Cityklinikan kotisivuilta. Molemmat voidaan antaa rekisteröidylle myös tulostettuina tai sähköisessä muodossa. Muut tietosuojaselosteet annetaan rekisteröidylle pyydettäessä. Pyynnön voi esittää nykyisin myös sähköisesti. Cityklinikka voi tarvittaessa edelleen pyytää rekisteröidyltä lisätietoja henkilöllisyyden vahvistamiseksi. Näin rekisteröidyn oikeus voidaan toteuttaa ilman, että muiden rekisteröityjen oikeuksia loukataan.

Uusi viestittävä asia on myös henkilötietojen säilytysajan ilmoittaminen.

5.2 Oikeus saada pääsy tietoihin

Rekisteröidyllä on tarkastusoikeus eli oikeus saada pääsy omiin tietoihinsa. Käytännössä tämä tarkoittaa sitä, että Cityklinikan on rekisteröidyn pyynnöstä ilmoitettava, käsitelläänkö yrityksessä häntä koskevia henkilötietoja vai ei. Tiedot on myös toimitettava rekisteröidyn niin halutessa.

Tarkastuspyynnön voi uuden asetuksen astuttua voimaan tehdä myös sähköisesti. Cityklinikka voi tarvittaessa edelleen pyytää rekisteröidyltä lisätietoja henkilöllisyyden vahvistamiseksi. Näin rekisteröidyn oikeus voidaan toteuttaa ilman, että muiden rekisteröityjen oikeuksia loukataan.

Tietosuoja-asetuksen mukaan rekisteröidyn pyyntöön on vastattava kuukauden kuluessa.

5.3 Oikeus tietojen oikaisemiseen

Jos rekisteröity löytää tiedoistaan virheellisiä henkilötietoja, hänellä on oikeus pyytää Cityklinikkaa oikaisemaan virheelliset tiedot. Tieto toimenpiteistä, joihin yrityksessä on tietojen oikaisemiseksi ryhdytty, on annettava rekisteröidylle kuukauden kuluessa pyynnöstä. Tietosuoja-asetuksessa ei oteta kantaa menettelytapoihin, joilla tietoja oikaistaan.

5.4 Rekisteröidyn oikeus saada ilmoitus tietoturvaloukkauksesta

Cityklinikalla on tehty kaikki mahdollinen tietosuoja- ja tietoturvaloukkauksien ehkäisemiseksi. Mikäli yrityksessä kuitenkin tapahtuisi tietoturvaloukkaus – esim. henkilötietojen vuotaminen ulkopuoliselle – Cityklinikan olisi ilmoitettava asiasta rekisteröidylle.

5.5 Oikeus käsittelyn rajoittamiseen

Rekisteröidyllä on oikeus rajoittaa henkilötietojensa käsittelyä ainakin väliaikaisesti.

5.6 Oikeus tulla unohdetuksi

Potilastietorekisterin ja henkilöstörekisterin tietoja poistetaan, jos rekisteröidyn vaatimus on oikeutettu. Tällaisessa tilanteessa pyyntö tulee lähettää kirjallisesti Cityklinikan toimitusjohtajalle. Muihin rekistereihin sovelletaan rekisteröidyn yksiselitteistä oikeutta poistaa itseään koskevat tiedot.

5.7 Oikeus siirtää tiedot järjestelmästä toiseen

Rekisteröidyllä on joissakin tilanteissa oikeus siirtää häntä koskevat tiedot toiselle rekisterinpitäjälle koneluettavassa muodossa, jos tämä on tietoteknisesti mahdollista. Cityklinikan henkilörekistereissä ei pystytä soveltamaan rekisteröidyn oikeutta siirtää tietojaan järjestelmästä toiseen.

5.8 Oikeus vastustaa käsittelyä, automaattista päätöksentekoa ja profilointia

Rekisterissä oleva henkilö on oikeutettu kieltämään kaiken häntä itseään koskevan tiedon käsittelyn, kun tietoa käytetään markkinointiin tai tutkimuksiin.

6. Cityklinikan rekisterit ja muut tietoaineistot

AINEISTO	TIEDON LÄHTEET	TIETOJEN KÄYTTÖ
Cityklinikan ja sen itsenäisten ammatinharjoittajien ylläpitämä potilastietorekisteri (Skalpell- ja Visiajärjestelmät)	Potilaan antamat tiedot, hoidon yhteydessä muodostuneet tiedot, muut potilaan luvalla hankitut asiakirjat	Hoidon suunnittelu, toteutus ja seuranta lain määräämällä tavalla; liiketoiminnan kehittäminen
Cityklinikan digiviestinnän asiakasrekisteri	Asiakkaan antamat tiedot verkkokauppaostojen yhteydessä, uutiskirjeen tilauksen yhteydessä tai asiakkuuden alkamisen yhteydessä	Markkinointiviestintä, asiakaspalvelun kehittäminen, liiketoiminnan kehittäminen
Cityklinikan yhteistyökumppanit	Yhteistyöyrittäjien antamat tiedot	Yhteistyön ylläpito, provisioiden maksaminen
Cityklinikan henkilöstörekisteri	Rekisteröidyn antamat tiedot työnhaun yhteydessä sekä tiedot, jotka rekisteröity on antanut työsopimusta laadittaessa	Työsuhteen ylläpitämiseen liittyvät toimet, palkanmaksu, yhteystietojen hakeminen
Tietojenkäsittelysopimus palkanlaskijan kanssa	Henkilöstörekisteriin kuuluvat ihmiset	Palkanlaskenta, palkan maksaminen
Tietojenkäsittelysopimus yhteistyöyrittäjien kanssa	Yhteistyöyrittäjien antamat tiedot	Vaitiolovelvollisuudesta huolehtiminen
Tietojenkäsittelysopimus verkkosivujen ylläpitäjäyrityksen kanssa	Verkkosivuston kautta tulleet yhteydenottopyynnöt ja valokuvat	Yhteydenottolomakkeiden tietosuojasta huolehtiminen
Tietojenkäsittelysopimus verkkokaupan ylläpitäjäyrityksen kanssa	Verkkokauppaostoksissa annetut henkilötiedot	Verkkokauppaostosten yhteydessä annettujen henkilötietojen tietosuojasta huolehtiminen

7. Tiedon ja riskien hallinta

Cityklinikan rekistereissä oleva tieto on yhtenäistä, mahdollisimman ajantasaista ja yksiselitteistä. Riskianalyysin aikana rekisterit jaoteltiin tietoturvaluokkiin, niin että tietoturvaluokkaan 1 kuuluvat salassa pidettävät tiedot, joiden loukkaus aiheuttaisi korkean riskin rekisteröityjen oikeuksille.

Potilastiedot kuuluvat tietoturvaluokkaan 1. Potilastietoja voivat käsitellä vain hoitoon kulloinkin osallistuvat terveydenhuollon ammattihenkilöt ja heidän avustajansa. Ajanvarauksesta vastaavat saavat käsitellä potilastietoja rajatusti. Verkkokauppamyynnistä vastaava tiedottaja käsittelee asiakkaiden tekemiä ostoksia, ei varsinaisia potilastietoja. Sosiaalisessa mediassa potilastietoja ei käsitellä lainkaan.

Potilastietoja Cityklinikalla saa käsitellä ainoastaan tehtävien edellyttämässä laajuudessa. Kaikki potilastiedot ovat salassa pidettäviä. Henkilöstö tekee vaitiolositoumuksen työsopimuksen alkaessa.

Kaikkiin rekistereihin liittyvät kaikki manuaaliset aineistot säilytetään lukittavissa arkistoissa. Sähköisesti talletetut tiedot on suojattu sähköisellä käyttöoikeudella. Tietoturvasta huolehditaan lain mukaisesti.

Tiedon käyttäjät, heidän käyttöoikeutensa ja tiedon käsittelyssä käytettävät päätelaitteet on määritelty potilastietorekisterin osalta. Potilastietoja voi käsitellä määrätyillä päätelaitteilla.

Tietoturvaan liittyvät riskit arvioidaan puolivuosittain tai tarpeen vaatiessa useammin. Tietoturvaa valvotaan ulkoisesti (ostopalvelut) ja sisäisesti (tietoturvapalaverit).