

Terapiaperhonen



Terapiaperhonen Oy

TIETOTURVAPOLITIikka

30.1.2023

Tämä asiakirja on tarkoitettu ylle kirjatun kohteen toiminnan läpinäkyvyyden lisäämiseksi. Tässä dokumentissa kerromme asiakkaille ja yhteistyökumppaneillemme, miten yrityksemme hoitaa tietoturvaan liittyviä asioita.

LISÄTIETOJA

Tietosuojavastaava

Henna Kekkonen

henna.kekkonen@terapiaperhonen.com

1. JOHDANTO

Tietojenkäsittely tukee Terapiaperhonen Oy:n palvelujen tuottamista, ja palveluiden tehokkuus riippuu osaltaan tietojenkäsittelystä. Tietoaineistot sisältävät potilaisiin, työntekijöihin ja toimintaan liittyvää tietoa, joka on lainsäädännön perusteella suojattava. Tietojenkäsittelyn on oltava tehokasta, virheetöntä ja varmaa.

Tietoturvapoliittikka määrittelee ne periaatteet, vastuut, toimintatavat sekä seurannan ja valvonnan, joita Terapiaperhosessa noudatetaan tietoturvan toteuttamisessa ja kehittämisessä.

2. TIETOTURVALLISUUSPERIAATTEET JA TAVOITTEET

Tietoturva tarkoittaa tietojen käsittelyn ja arkistoinnin turvaamista. Tietoturva rakentuu tiedon luottamuksellisuudesta, eheydestä, saatavuudesta, käytettävyydestä ja kiistämättömyydestä sekä tietojen käsittelyn valvonnasta.

Tietoturvaan kuuluvat tietoturvaorganisaatio, tietojen käsittelijöiden toimintatavat, tietojen turvaamisen menetelmät, välineet ja toimenpiteet, työhön osoitetut resurssit sekä välineistön ja tilojen tietoturvaominaisuudet.

Hyväksytyn tietoturvapoliittikan mukainen tietoturva tulee sisällyttää luonnollisena osana kaikkeen toimintaan. Tietoturvan kehittäminen ja ylläpito ovat osa Terapiaperhosen yleistä turvallisuustoimintaa, riskien hallintaa ja sisäistä valvontaa.

Tietoturvatyö on tietoturvan saavuttamiseksi tehtävien toimenpiteiden suunnittelua ja toteuttamista. Tietoturvatyön tavoite ja päämäärä on turvata yrityksen toiminnalle tärkeiden tietojärjestelmien ja tietoverkkojen keskeytymätön toiminta, estää tietojen ja tietojärjestelmien joutuminen ulkopuolisille sekä estää niiden valtuudeton käyttö, tahaton tai tahallinen tiedon tuhoutuminen tai vääristyminen, sekä minimoida aiheutuvat vahingot. Normaaliajan toiminnan tietojenkäsittelyn turvaamisen lisäksi varaudutaan toiminnan keskeyttäviin uhkatilanteisiin ja niistä toipumiseen.

Yritys vastaa osana tietoturvatyötä myös potilasasiakirjojen ja potilastietoja sisältävien muiden asiakirjojen suojaamiseen liittyvästä tietoturvatyön suunnittelusta ja toteuttamisesta. Tämän vastuun takia yritys toteuttaa tietoturvansa korotetun tietoturvatason käytäntöjen mukaisesti.

Jokaisen Terapiaperhosen työntekijän, sekä yrityksen tietojen ja tietojärjestelmien käyttäjän on tunnettava tämä tietoturvapoliittikka ja noudatettava sen perusteella annettuja ohjeita ja määräyksiä. Yrityksen ulkopuolisten terveydenhuollon toimijoiden, toimittajien ja muiden ulkopuolisten tahojen tulee myös sitoutua noudattamaan tätä tietoturvapoliittikkaa, kansallisia normeja sekä ohjeita ehtona tehtäviensä mukaiselle pääsulle yrityksen tietojärjestelmään ja sen tietoaineistoihin.

3. TIETOTURVATOIMINTAA OHJAAVAT TEKIJÄT

Tietoturvaa ohjaavat muun muassa nämä velvoitteet:

- Laki yksityisestä terveydenhuollosta 9.2.1009/152
- Laki potilaan asemasta ja oikeuksista 17.8.1992/785
- Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä 9.2.2007/159
- Tietosuojalaki (aiempi henkilötietolaki) 5.12.2018/1050
- Laki terveydenhuollon ammattihenkilöistä 28.6.1994/559
- Nämä säännökset koskevat myös ääni-, filmi- ja videotallenteita sekä valokuvia.

4. RISKIEN HALLINTA

Terapiaperhosessa on tehty koko yrityksen voimin riskianalyysi kattavasti kaikesta kuntoutustoiminnasta sekä tietoturvaan liittyvistä riskeistä. Riskianalyysia tehdään ja päivitetään yhdessä työntekijöiden kanssa kerran vuodessa. Riskitilanteista ja Läheltä piti -tilanteista pidetään kirjaa, jota tarkastellaan vuosittain toiminnan kehittämiseksi ja parantamiseksi.

5. TIETOTURVALLISUUDEN MERKITYS ORGANISAATIOLE

Terapiaperhosessa tehdään kuntoutustyötä, jossa ollaan potilaiden, potilastietojen ja tietojärjestelmän kanssa tekemisissä joka päivä. Tämä on edellytys sille, että tällaista työtä voi ylipäätään tehdä. Tästä syystä tietoturvallisuuteen ja siihen liittyviin riskeihin tulee kiinnittää erityistä huomiota.

5.1. Toiminnan kannalta elintärkeät tehtävät ja turvattavat kohteet

Terapiaperhosen yritysten toiminnan tietoturvallisuuden kannalta tärkeimmät turvattavat kohteet ovat henkilöt, tilat, laitteet, tietoliikenne, tietojärjestelmä, palvelut sekä potilastiedot ja tietoaineistot kaikissa olomuodoissaan.

Näiden kohteiden turvaamisen tavoitteena on toiminnan onnistumisen turvaaminen Terapiaperhossa ja kaikissa paikoissa, joissa yritysten työntekijät työskentelevät ja näin ollen palveluiden tuottaminen niitä ostaville tahoille.

5.2. Tietoturvaperiaatteet

Tietojenkäsittelyn turvaamisperiaatteita ovat ennaltaehkäisy, turvatoimien ajantasainen seuranta ja kehittäminen sekä tietojärjestelmän toiminnan ja käytön valvonta.

Terapiaperhosen potilastietojen ja muiden salassa pidettävien tietojen käsittelyssä, niin tietojärjestelmää käyttäen, kuin muutenkin, on huomioitava mahdolliset tietojen käsittelyyn kohdistuvat riskit ja varauduttava niiden ennaltaehkäisyyn. Yritysten työtehtäviä toteutettaessa varmistetaan tarkoituksenmukaiset suojausmenettelyt. Työntekijöillä on käytössään tarvittava tieto, työkalut ja ympäristö, jotta työtä voidaan tehdä tietoturvallisesti.

5.3. Tietoturvallisuuden toteutumista tukevia käytäntöjä

Terapiaperhosessa on aktiivisesti käytössä henkilökunnan ja johdon tietoturvavelvoitteet ja ohjeistukset.

6. TURVATOIMIEN PRIORISOINTI

Terapiaperhosen turvatoimien järjestys tilanteissa, joissa joudutaan toteuttamaan priorisointia:

- henkilön hengen tai terveyden turvaaminen
- potilastietojen luottamuksellisuuden turvaaminen
- potilastietojärjestelmän ja arkiston eheyden turvaaminen
- käyttö- ja toimintaympäristön käytettävyyden turvaaminen.

Pelastuslaki (379/2011)

7. TIETOTURVALLISUUDEN HALLINTA

Tietoturvan toteuttamisen perusta on tämä tietoturvapoliittikka sekä tarkempi Tietoturvasuunnitelma (vain yrityksen sisäisessä käytössä oleva kattava dokumentti)

Yrityksen tietoturvaperiaatteet perustuvat kansallisiin, yleisiin ja toimialakohtaisiin tietoturva, henkilörekistereitä, hyvää tiedonhallintatapaa ja tiedon laatua ohjaaviin ja velvoittaviin säädöksiin, ohjeisiin ja standardeihin. Lainsäädännön ja ohjeistuksen muutokset otetaan huomioon yrityksen tietoturvan kehittämisessä.

Tietoturvan toteutuksen tulee perustua niihin vaatimuksiin, joita toiminta ja palvelut sekä kunkin tiedon ja tietojärjestelmän turvallisuusluokka asettavat tietojenkäsittelyn varmuudelle, käytettävyydelle, salassapidolle, laadulle ja toiminnan jatkuvuudelle sekä toimintaan kohdistuvien riskien arvioinnille. Vaatimusten selvittäminen, riskien arvioiminen ja niiden perusteella turvallisuustoimenpiteiden määrittäminen tapahtuu säännöllisesti Terapiaperhosen tiimissä suoritettavilla riskianalyysillä.

Tietoturvan ylläpitäminen on jatkuva prosessi, joka tapahtuu hallinnollisten ja teknisten ratkaisujen avulla. Jokainen käyttäjä allekirjoittaa salassapito- ja käyttäjäsitoumuksen, sekä tutustuu tietoturvapoliittikkaan ja henkilökunnan tietoturvaohjeisiin ja sitoumuksen saadessaan oikeuden tehtäviensä mukaiseen tietojärjestelmien ja tietoaineistojen käyttöön.

8. TIETOTURVAVASTUUT

8.1. Yritysten tietoturvavastuut

Tietoturvavastaava vastuulla on ohjeiden laatiminen, päivitys, tiedottaminen ja koulutuksen ja opastuksen järjestäminen työntekijöille. Työntekijöiden vastuulla on toimia omassa työssään tietoturvaohjeistusta noudattaen.

8.2. Organisaation yhteistyökumppaneiden vastuut

Yhteistyökumppanit toimivat omien organisaatioidensa tietoturvaohjeistusten mukaan ja niitä säätelevät tässä tapauksessa useimmiten samat lait kuin Terapiaperhosen toimintaa. Asiakkaita ei voi erityisesti vastuuttaa, mutta heille perustellaan tarpeen mukaan tietoturvaperiaatteiden mukaista toimintaa.

9. TIETOTURVAKOULUTUS JA -OHJEET

Tietoturvallisuus on sisällytetty Terapiaperhosen perehdytysprosessiin. Henkilökunta osallistuu vuosittain aktiivisesti tietoturvasuunnitelman päivittämiseen ja läpikäyntiin. Tietoturvaohjeet ovat koko ajan henkilöstön saatavilla.

10. TIETOTURVALLISUUDESTA TIEDOTTAMINEN

Tietoturva-asioista tiedotetaan tarpeen mukaan. Tiedottamisesta vastaavat tietoturvavastaava.

Jokaisella henkilökuntaan kuuluvalla on velvollisuus tiedottaa muita tilanteissa, jossa havaitsee tietoturvallisuuden olevan vaarassa tai jonkin tietoturvallisuuteen liittyvän asian vaativan toimenpiteitä. Poikkeustilanteissa ja tilanteissa, joissa tarvitaan nopeaa reagointia, tiedotetaan henkilökuntaa soittaen, tekstiviestillä tai suojattua viestipalvelua käyttäen.

11. TIETOTURVALLISUUDEN VALVONTA

Käyttäjien ja ylläpitäjien tulee ilmoittaa havaitsemastaan tietoturvan puutteesta, tietoturvaan liittyvästä väärinkäytöksestä tai epäilemästään tietoturvarikkomuksesta esimiehelleen tai tietoturvavastaavalle. Tietoturvavastaavan tehtävänä on seurata ja valvoa tietojärjestelmien tietoturvan toteutumista ja ryhtyä toimenpiteisiin havaittujen tietoturvan heikkouksien korjaamiseksi.

12. TOIMINTA POIKKEUSTILANTEISSA

Tilanteessa, jossa havaitaan uhka tai vaara sähköisessä tietoturvallisuudessa, siirrytään paperikirjaamiseen, kunnes ongelma ratkeaa tai uhka on poistunut. Kun uhka on havaittu, otetaan välittömästi yhteyttä järjestelmän toimittajaan ja tarvittaessa tietoturvayritykseen

13. KÄYTÄNNÖN ASIAT

Miten tietoturvaan ja toimintaamme liittyvät asiat näyttäytyvät asiakkaalle:

Meidän täytyy pitää asiakkaistamme asiakasrekisteriä, jotta pystymme todentamaan valvoville viranomaisille toimintamme läpinäkyvästi ja rehellisesti. Toimintaamme valvovat mm. Valvira ja Aluehallintovirasto AVI.

Terveystieteiden ammatti henkilö, muu terveydenhuollon toimintayksikössä työskentelevä tai sen tehtäviä suorittava ei saa luovuttaa sivulliselle potilasasiakirjoihin sisältyviä tietoja, jos siihen ei ole potilaan kirjallista suostumusta taikka luovutukseen oikeuttavaa tai velvoittavaa lain säännöstä. Tämä tarkoittaa, ettemme pysty luovuttamaan mitään asiakastietoja ilman asiakkaan antamaa kirjallista lupaa

Terapiaperhosen asiakastietojärjestelmänä toimii Kanta-yhteydellä toimiva A-luokan tietojärjestelmä. Siirrämme asiakaskirjaukset Kanta-järjestelmään, joten asiakas pystyy OmaKanta palvelun kautta tarkastelemaan terapiasta kirjattuja käyntejä. Kanta-palveluita käyttävällä henkilöllä tulee olla Väestörekisterikeskuksen myöntämä terveydenhuollon käyttöön tarkoitettu toimikortti, joka löytyy siis kaikilta Terapiaperhosen työntekijöiltä. Kanta-palveluiden käyttäjä tunnustetaan aina ennen palveluiden käyttöä terveydenhuollon varmenteella käyttäjän omalta toimikortilta. Palveluiden käyttö estetään, jos varmente ei ole voimassa tai henkilöllä ei ole ammattioikeutta.

Lisätietoja saat tietoturvavastaavalta Henna Kekkoselta