1.4.2025

Tietoturva- ja tietosuojapolitiikka

1. Johdanto ja yleiset periaatteet

Tietoturva- ja tietosuojapolitiikka määrittelee ne periaatteet, vastuut, toimintatavat sekä seurannan ja valvonnan, joita Pipolakodin palveluissa noudatetaan tietoturvan toteuttamisessa ja kehittämisessä.

Tietoturva- ja tietosuojapolitiikkaa täydentävät tietoturva- ja tietosuojaohjeistus- sekä potilastiedon käsittely– dokumentti sekä koko henkilökunnalle annetut ohjeet.

Tietoaineistot sisältävät potilaisiin, asiakkaisiin, työntekijöihin ja toimintaan liittyvää tietoa, joka on lainsäädännön perusteella suojattava. Tietojenkäsittelyn on oltava mahdollisimman luotettavaa, tehokasta ja virheetöntä. Tietojenkäsittelyyn liittyy aina inhimillisenä toimintana riskejä, joita minimoidaan mm. ohjeistuksilla, teknisillä ratkaisuilla ja koulutuksella. Vain pieni osa tietoturvariskeistä pystytään välttämään teknisillä ratkaisuilla. Tärkeintä on jokaisen henkilön päivittäisessä tietojen käsittelyssä tekemät ratkaisut ja toimenpiteet, jotka pohjautuvat lainsäädännön ja ohjeiden noudattamiseen.

Tietoturvalla tarkoitetaan tietojen, palvelujen, järjestelmien ja tietoliikenteen suojaamista. Tietosuoja on oleellinen osa tietoturvallisuutta. Tietosuojalla tarkoitetaan henkilötietojen ja muiden henkilön luottamuksellisten tai arkaluonteisten tietojen suojaamista ja rekisteröidyn henkilön oikeutettujen oikeuksien ja vapauksien tehokasta toteuttamista.

Pipolakodin henkilökunnan ja sen luottamushenkilöiden sekä ulkopuolisten terveydenhuollon toimijoiden, toimittajien ja muiden ulkopuolisten tahojen tulee sitoutua noudattamaan tätä tietoturva- ja tietosuojapolitiikkaa.

2. Määritelmät

Tietoturvallisuuden keskeisillä käsitteillä tarkoitetaan seuraavaa:
Käytettävyys eli tieto on siihen oikeutettujen hyödynnettävissä haluttuna aikana.
Todentaminen (autentikointi) eli varmistuminen kohteen todenmukaisuudesta, oikeellisuudesta, alkuperästä tai varmistuminen käyttäjän aitoudesta halutulla luottamustasolla.
Kiistämättömyys ilmentää sitä, että tiedon lähettäjä tai vastaanottaja tai tietoon liittyvä tapahtuma voidaan varmistaa luotettavasti myös jälkikäteen.
Tietosuojaan liittyvät käsitteet **henkilötieto, henkilötietojen käsittely, henkilörekisteri, rekisterinpitäjä, rekisteröity ja suostumus** määritellään ja yleisessä tietosuoja-asetuksessa (2016/679).
Yksityisyyden suoja on tietoturvan ja tietosuojan toteuttamista organisaatiossa.

Tietoturva tarkoittaa tietojen käsittelyn turvaamista.
Tietosuojan keskeisiä periaatteita ovat: **lainmukaisuus, kohtuullisuus ja läpinäkyvyys**; **käyttötarkoitussidonnaisuus; (**Henkilötietoja käytetään vain siihen käyttötarkoitukseen, joihin tiedot on kerätty)
tietojen minimointi; (Henkilötietoja kerätään vain siinä määrin, kuin on välttämätöntä kyseessä olevan tehtävän hoitamiseksi)
täsmällisyys;(Tietojen on oltava paikkansapitäviä ja täsmällisiä)
säilytyksen rajoittaminen; (Tietojen säilyttämiselle on asetettava aika, jonka jälkeen tiedot on hävitettävä tai ainakin määriteltävä peruste, jonka mukaan säilytysaika määräytyy)
eheys ja luottamuksellisuus; (Tiedot on säilytettävä muuttumattomina ja turvallisesti niin, että niihin pääsee käsiksi vain sellaiset henkilöt, joiden tehtävien hoitamiseksi tiedot ovat välttämättömiä.)

Potilaan mahdollisuus käyttää oikeuksiaan turvataan. Potilaan mahdollisuus valvoa ja määrätä häntä koskevien henkilötietojen käytöstä täydentää Pipolakodin toteuttamaa valvontaa.

Henkilötietojen käsittelyn on oltava läpinäkyvää ja potilaan luottamusta edistävää. Tietoturva rakentuu tiedon luottamuksellisuudesta, eheydestä, saatavuudesta, käytettävyydestä ja kiistämättömyydestä sekä tietojen käsittelyn valvonnasta.

Tietoturvan hallintaan liittyvät tietojen käsittelijöiden toimintatavat, tietojen turvaamisen menetelmät, välineet ja toimenpiteet, työhön osoitetut resurssit sekä välineistön ja tilojen tietoturvaominaisuudet. Hyväksytyn tietoturva- ja tietosuojapolitiikan mukaisen tietoturvan ja tietosuojan tulee olla luonnollisena lähtökohtana kaikessa toiminnassa. Tietoturvan ja tietosuojan kehittäminen ja ylläpito sekä sen seuranta ovat osa Pipolakodin yleistä turvallisuustoimintaa, riskien hallintaa ja sisäistä valvontaa.

Toimintalähtöisesti painottuvalla tietoturva- ja tietosuoja -asioiden hoidolla tuetaan oman organisaation toiminnalle asetettuja vaatimuksia. Lisäksi tietojen ja tietojärjestelmien huolellinen käsittely takaa osaltaan asiakkaiden yksityisyyden suojaa. Tietoturvatyö on tietoturvan saavuttamiseksi tehtävien toimenpiteiden suunnittelua ja toteuttamista.

Tietosuoja on oleellinen osa tietoturvallisuutta. Tietosuojalla tarkoitetaan henkilötietojen ja muiden henkilön luottamuksellisten tai arkaluonteisten tietojen suojaamista ja rekisteröidyn oikeuksien tehokasta toteuttamista. Lainsäädännön perusteella henkilötietoja suojataan usein tarkemmin kuin organisaation käytössä olevia muita luottamuksellisia tietoja. Tietosuojalainsäädäntö edellyttää, että henkilötietojen käsittely on turvattava ja henkilötiedot on suojattava asiattomalta käsittelyltä. Henkilötietojen oikeellisuus on varmistettava, ne on pidettävä salassa ulkopuolisilta, niitä ei saa tuhota tai käsitellä asiattomasti ja niiden on oltava tarpeen mukaan käytettävissä. Tietosuojalainsäädännössä säädetään lisäksi monista oikeuksista, joita henkilöllä on omiin tietoihinsa. Terveyden- ja sosiaalihuollon ammattihenkilökunnan toimintaa ohjaavat lain- ja määräysten mukaiset velvollisuudet ja oikeudet sekä näiden lisäksi ammattietiikka, johon sisältyy vastuu hyvästä toimintatavasta ja velvollisuus tietojen salassapidosta ja vaitiolosta.

3. Tietoturvan ja tietosuojan toimintaa ohjaavat tekijät

Tietoturvatoimintaa ohjataan sekä EU:n että kansallisin säädöksin, määräyksin, ohjein ja suosituksin. Näihin liittyviä päätöksiä tehdään sekä omassa organisaatiossa että sen ulkopuolella. Lainsäädännön lisäksi tulee noudattaa muita omalle organisaatiolle hyväksyttyjä tietoturvaan ja tietosuojaan liittyviä ohjeita ja määräyksiä. Organisaation omat päätökset, määräykset ja ohjeet eivät saa olla ristiriidassa tämän tietoturvapolitiikan tai organisaation ylemmän tason määräysten kanssa siten, että tietoturva tai tietosuoja heikkenee.

4. Vastuut

Tietoturvallisuudesta vastaa Pipolakodin ylin johto, joka päättää organisaation kokonaisturvallisuuden eri osa-alueiden kehittämistoiminnan tavoitteista, organisoinnista, resursseista ja toimintavaltuuksista sekä nimeää tietoturva/suojavastaavan. Potilastietoja sisältävien henkilörekistereiden suojaamisesta ja valvonnasta sekä tietoturvatyön kokonaisuudesta vastaa tietoturva/tietosuojavastaava johdolta saamiensa resurssien ja toimintavaltuuksien puitteissa

Tietoturva- ja tietosuoja-asioiden toteutumisesta, tiedottamisesta ja valvonnasta vastaa esimies. Esimiehen on huolehdittava, että tietoturva- ja tietosuojamääräykset ja ohjeet koulutetaan ja perehdytetään henkilöstölle. Esimiehen tulee valvoa, että henkilöstö noudattaa tietoturvasta ja tietosuojasta annettuja määräyksiä ja ohjeita.

Jokainen organisaation tietoja ja tietojärjestelmiä käyttävä on velvollinen ilmoittamaan havaitsemistaan tietoturvallisuuden puutteista, uhkista tai menettelyvirheistä eteenpäin tietoturva/suojavastaavalle. Jokainen Pipolakodin työntekijä, tietoja käsittelevä, tietojärjestelmien tai tietoverkkojen ylläpitäjä ja käyttäjä on omalta osaltaan vastuussa tietoturvan toteuttamisesta sekä tietoturvaohjeiden noudattamisesta. Jokaisella Pipolakodin työntekijällä on tietosuoja- ja tietoturva-asioihin liittyvä valvontavastuu. Jokainen henkilö on velvollinen raportoimaan mahdolliset väärinkäytökset tai niiden uhat. Potilastietoihin liittyvät asiat raportoidaan tietosuojavastaavalle. Tietoturvallisuus on koko Pipolakodin yhteinen asia.

5. Käyttöoikeuksien ja käyttövaltuuksien hallinta

Pipolakodissa DomaCarea saa käyttää ainoastaan henkilökohtaisilla tunnuksilla, joihin on liitetty käyttäjän tiedot. Yhteiskäyttötunnuksia ei ole kenelläkään.
Pipolakodissa palveluvastaava ja vastaava ohjaaja ovat DomaCaren pääkäyttäjiä, joilla on valtuudet luoda uusille työntekijöille henkilökohtaiset käyttäjätunnukset. Työntekijöillä on peruskäyttäjän oikeustaso.

Työntekijän lopettaessa työskentelyn Pipolakodissa palveluvastaava tai vastaava ohjaaja huolehtivat työntekijän käyttöoikeuksien päättämisestä välittömästi, kun työntekijän tarve päästä käsiksi asiakastietoihin päättyy.

Kenelläkään työntekijällä ei ole käytössä henkilökohtaista puhelinta, joka olisi aktivoitu DomaCareen.

6. Tehtävät

Tietoturva- ja tietosuojavastaavalla on velvollisuus valvoa, seurata ja raportoida havaittuja tietoturvan heikkouksia. Tietoturva- ja tietosuojavastaava antaa tietotilinpäätöksen raporttina Pipolakodin hallitukselle kerran vuodessa. Tietoturva- ja tietosuojavastaava vastaa tietoturva ja tietosuojaohjeistuksen tekemisestä ja ylläpidosta, toteutuksen valvonnasta ja tietoturvatietouden edistämisestä.

Pipolakodille palveluja tuottavat tahot tulee velvoittaa nimeämään tietoturva- sekä tietosuoja-asioihin yhteyshenkilö, joka heillä vastaa sovitun tietoturva- ja tietosuojatason noudattamisesta. Kumppanien tulee viipymättä ilmoittaa omista organisaatioon vaikuttavista tietoturvapoikkeamistaan ilmoitetuille yhteyshenkilöille.

Pipolakodin organisaatiossa, prosesseissa, projekteissa ja tietojärjestelmissä tulee huolehtia tietoturvaan ja tietosuojaan sekä laajemminkin tietotekniikkaan liittyvien riskien hallinnasta.

7. Tietoturvallisuuden merkitys ja toteuttaminen

Toiminnan tietoturvallisuuden kannalta tärkeimmät turvattavat kohteet ovat henkilöt, tilat, laitteet, tietoliikenne, tietojärjestelmät, ohjelmistot, palvelut sekä tiedot ja tietoaineistot kaikissa olomuodoissaan. Näiden kohteiden turvaamisen tavoitteena on operatiivisten järjestelmien ja sisäisen tietojenkäsittelytoiminnan ja tietosuojan turvaaminen sekä palvelujen tuottaminen normaalioloissa ja normaaliolojen häiriötilanteissa, sekä poikkeusoloissa.

Yhteisesti noudatettavat tietoturva- ja suojaperiaatteet ovat seuraavat:

- Asiat pitää tehdä tietoturvallisesti, millä tarkoitetaan tiedon suojaamista monenlaisilta uhkilta. Tarkoituksena on varmistaa toiminnan jatkuvuus, minimoida toiminnalliset riskit.
- Tietoturva- ja tietosuoja-asiat pitää huomioida välineestä riippumatta eli ne eivät liity vain tietojärjestelmien käyttämiseen.
- Paperiset asiakirjat, sähköiset tietovarannot, tietojärjestelmät, tietotekniset laitteet, tietoverkot ja niihin liittyvät palvelut on pidettävä asianmukaisesti suojattuina sekä normaali- että poikkeusoloissa.
- Tietoturvallisuuden saavuttamiseksi toteutetaan tarvittavia turvamekanismeja, jotka muodostuvat toimintaperiaatteista, prosesseista, organisaatiorakenteista ja ohjelmisto- ja laitteistotoiminnoista.
- On varmistettava, että luottamukselliset, arkaluonteiset ja muut salassa pidettävät asiat kuuluvat vaitiolovelvollisuuden piiriin riippumatta siitä, miten tai mihin niitä on tallennettu tai millä tavalla tiedot on saatu.

- Tietosuojanäkökulma on otettava huomioon kaikessa toiminnassa siten, että henkilötietojen turvallinen käsittely on toiminnan lähtökohtana.
- Pipolakodin valvontaa täydentää rekisteröidyn mahdollisuus itse valvoa ja määrätä henkilötietojensa käytöstä mm. tarkastamalla häntä koskevat tiedot ja vaatimalla virheellisten tietojen korjaamista.

8. Tietoturvallisuuden toteutumista tukevia käytäntöjä

Tietoturvan toteuttamisen perusta on tämä Pipolakodin hallituksen hyväksymä kirjallinen tietoturva- ja tietosuojapolitiikka, joka annetaan tiedoksi jokaiselle Pipolakodin työntekijälle ja liitetään tarvittaessa sopimuksiin. Pipolakodin tietoturvaperiaatteet perustuvat EU:n tasoisiin, kansallisiin, yleisiin ja toimialakohtaisiin tietoturvaa, henkilörekistereitä, hyvää tiedonhallintatapaa ja tiedon laatua ohjaaviin ja velvoittaviin säädöksiin, ohjeisiin ja standardeihin. Lainsäädännön ja ohjeistuksen muutokset otetaan huomioon Pipolakodin tietoturvan kehittämisessä.

Vaatimusten selvittäminen, riskien arvioiminen ja niiden perusteella turvallisuustoimenpiteiden määritteleminen tapahtuvat säännöllisesti suoritettavilla riskianalyyseillä.

Käyttäjien toimintaa ohjataan henkilökohtaisella ja riittävällä perehdytyksellä, saatavilla olevilla toimintaohjeilla sekä koulutuksella. Jokainen käyttäjä sitoutuu noudattamaan tietoturva- ja tietosuojaohjeita saadessaan oikeuden tehtäviensä mukaiseen tietojärjestelmien ja tietoaineistojen käyttöön. Jokainen työntekijä on allekirjoittanut kirjallisen vaitiolo- ja salassapitosopimuksen.

Pipolakoti toimii henkilörekisterin ylläpitäjänä vain siinä tapauksessa, että se on toiminnan hoitamiseksi välttämätöntä. Tarpeettomat henkilösidonnaiset tiedot poistetaan, kun tiedon säilyttämiselle ei ole enää hyväksyttävää perustetta. Pipolakoti suorittaa tarvittavan käyttäjähallinnan ja valvonnan henkilötietorekistereilleen. Rekisterit on rajattu vain tarvittavien henkilöiden käyttöön. Kyseinen henkilöstö saa jatkuvaa koulutusta henkilötietojen käsittelystä. Kaikista käytössä olevista henkilörekistereistä on tehty rekisteriselosteet ja tietosuojaselosteet.

Tietoturva- ja tietosuojavaatimukset huomioidaan myös hankintojen/sopimusten teko vaiheessa, jolloin sovitaan tietoturvan ja tietosuojan hallinnan menettelyt, mukaan lukien henkilötietojen käsittelyn seuranta ja valvonta sekä tietoturvaraportointi ja tietoturvapoikkeamien hallinta.

9. Jatkuvuus

Toiminnan jatkuvuus tulee turvata toipumissuunnittelulla, joka sisältää häiriöiden ennalta ehkäisemisen ja mahdollistaa niistä nopean toipumisen. Toipumissuunnittelussa tulee erityisesti huomioida mahdolliset liiketoiminnan riskit ja prioriteetit. Tietosuojan näkökulmasta on turvattava rekistereiden palautettavuus ja käytettävyys häiriötilanteissa. Rekisterissä olevan

tiedon on oltava käytettävissä ja ongelmatilanteissa on varmistettava tietojen säilyvyys, eheys, ja palautettavuus mahdollisimman tehokkaasti.

10. Tietoturva- ja tietosuojakoulutus ja -ohjeet sekä tiedotus

Uusien työntekijöiden perehdytysprosessiin tulee olla sisällytettynä tietoturvallisuus. Koulutusta järjestetään ja mahdollistetaan kaikille työntekijöille määräajoin. Koulutukset ovat pakollisia ja niissä läsnäolo on dokumentoitua.

Pipolakodin tietoturva- ja tietosuojaohjeet pidetään ajan tasalla ja niistä kerrotaan työntekijöille. Ohjeistuksiin tehtävistä muutoksista tulee tiedottaa käyttäjiä ja tarvittaessa järjestää lisäkoulutuksia.

Tietoturva- ja tietosuoja-asioista tiedotetaan tarpeen mukaan. Rekisteröidylle tiedottamisessa noudatetaan, mitä lainsäädännössä on määrätty niin säännönmukaisesta tiedottamisesta, kuin myös tiedottamisesta häiriötilanteissa. Rekisteröidyn tiedottaminen on osa rekisteröidyn oikeuksien käyttämisen tehokkuuden toteuttamista.

8. Valvonta ja rikkomusten seuraamukset

Tietojen ja tietojärjestelmien käyttöä valvotaan olemassa olevien lakien ja asetusten mukaisesti huomioiden yksityisyyden suoja työelämässä. Kaikki tietoturvarikkomukset käsitellään asianmukaisesti. Tietoturvarikkomusta lieventää merkittävästi, mikäli rikkomuksen tehnyt henkilö on välittömästi rikkomuksen huomattuaan ottanut yhteyttä esimieheensä sekä tietoturva- ja tietosuojavastaavaan, eikä käytä missään olosuhteissa väärin saamaansa tietoa. Tietoturvarikkomuksesta seuraa varoitus tai sen perusteella on mahdollista päättää työsuhde. Tietoturvarikkomuksesta voi seurata myös rikosoikeudellinen vastuu. Toiminnan oikeellisuus on epävarmuustilanteessa varmistettava ensisijaisesti esihenkilöltä/tietosuojavastaavalta tai tietoturvavastaavalta (Primanetin Jani Havia).