Palvelusetelin sääntökirjan salassapito- ja turvallisuusliite

1 Tarkoitus ja soveltaminen

1.1 Tässä liitteessä (”Salassapito- ja Turvallisuusliite”) Palvelunjärjestäjällä tarkoitetaan Pirkanmaan hyvinvointialuetta ja Palveluntuottajalla Pirkanmaan hyvinvointialueen palveluntuottajaksi hyväksymää palveluntuottajaa. Palvelunjärjestäjästä ja Palveluntuottajasta käytetään erikseen viitattuina termiä ”Osapuoli” ja yhdessä ”Osapuolet”.

1.2 Tämä Salassapito- ja Turvallisuusliite on osa Palvelusetelin sääntökirjaa (”Sääntökirja”). Hyväksymällä Sääntökirjan ehdot, Palveluntuottaja hyväksyy tämän Salassapito- ja Turvallisuusliitteen mukaiset Palvelunjärjestäjän Luottamuksellisen tiedon käsittelyä koskevat ehdot.

1.3 Tässä Salassapito- ja Turvallisuusliitteessä määritellään Palvelunjärjestäjää ja Palveluntuottajaa sitovasti ne Luottamuksellisen tiedon käsittelyä ja tietoturvallisuutta koskevat ehdot, joiden mukaisesti Palveluntuottaja käsittelee Palvelunjärjestäjän Luottamuksellista tietoa (kuten jäljempänä määritelty). Selvyyden vuoksi todetaan, että Sääntökirja sekä tämä Salassapito- ja Turvallisuusliite täydentävät toisiaan salassapitoa ja turvallisuutta koskevien ehtojen osalta. Mikäli niiden ehdot ovat keskenään ristiriidassa, sovelletaan salassapitoon ja turvallisuuteen liittyvissä asioissa ensisijaisesti tätä Salassapito- ja Turvallisuusliitettä, ellei erikseen toisin Sääntökirjassa tai tässä Salassapito- ja Turvallisuusliitteessä todeta.

1.4 Palveluntuottaja noudattaa kulloinkin voimassa olevaa tietoturvallisuutta, tietosuojaa, asiakas- ja potilastietoa, julkisuutta ja salassapitoa koskevaa lainsäädäntöä. Käsitellessään Luottamuksellista tietoa Palveluntuottaja noudattaa yleisiä hyviä tietoturvaperiaatteita, joilla varmistetaan toiminnan jatkuvuus sekä poikkeamiin varautuminen.

1.5 Tässä Salassapito- ja Turvallisuusliitteessä määritellyt vaatimukset asettavat vähimmäistason palvelusetelillä toteutettavia sosiaali- ja terveydenhuollon palveluiden tuottamisen tietoturvallisuudelle.

1.6 Palveluntuottajalla tulee olla Luottamuksellisen tiedon käsittelylle ohjeistus, jonka mukaisesti Palveluntuottajan henkilöstö ja asianosaiset ulkopuoliset tahot käsittelevät Luottamuksellista tietoa.

1.7 Sääntökirjan mukaisten palveluiden tuotannon päättyessä Palveluntuottaja sitoutuu viivytyksettä Palvelunjärjestäjän antaman ohjeistuksen mukaisesti joko palauttamaan tai poistamaan Luottamuksellisen tiedon ja siitä mahdollisesti tekemänsä kopiot. Mikäli Euroopan unionin oikeudessa tai jäsenvaltion lainsäädännössä vaaditaan säilyttämään Luottamukselliset tiedot, velvollisuutta tietojen poistamiseen ei ole, ja Palveluntuottajan on kiellettyä poistaa tiedot. Palveluntuottajan tulee Palvelunjärjestäjän pyynnöstä esittää poistamisesta kohtuullinen selvitys. Palvelunjärjestäjä voi antaa tältä osin tarkempia ohjeita Palveluntuottajalle. Palvelunjärjestäjän pyynnöstä Palveluntuottaja tulee arkistoida henkilötietoja Palvelunjärjestäjän määrittämän ajan ennen niiden palautusta tai poistamista. Tällöin Osapuolet sopivat erikseen arkistoinnista aiheutuvien kulujen korvaamisesta. Selvyyden vuoksi todetaan, tätä Salassapito- ja

Turvallisuusliitettä sovelletaan myös Luottamuksellisten tietojen käsittelyyn arkistointitarkoituksessa.

2 Salassapito

2.1 ”Luottamuksellisella tiedolla” tarkoitetaan kaikkea Palvelunjärjestäjän luottamuksellista tietoa, jollaista on henkilötieto, henkilöstön tieto, sosiaalihuollon asiakastieto, potilastieto, pelastustoiminnan tieto sekä muu Palvelunjärjestäjän toiminnan järjestämiseen ja luonteeseen liittyvä tieto, joka ei ole yleisesti tiedossa. Tällaista tietoa tyypillisesti on Palvelunjärjestäjän tietotekniikkainfrastruktuuriin, tietoturvahallintoon, sovelluksiin, järjestelmiin, toimintatapoihin ja käytänteisiin liittyvä tieto, tietoturvasta ja sovelluksista vastuullisiin ja niitä ylläpitäviin liittyvä tieto sekä kaikki sellainen Palvelunjärjestäjän toimintaan liittyvä tieto, joka ei ole yleisesti tiedossa ja joka annetaan Palveluntuottajan tietoon Sääntökirjan perusteella tai syntyy sovitun palvelun yhteydessä. Luottamuksellinen tieto voidaan ilmaista suullisesti, kirjallisesti tai sähköisesti.

2.2 Palveluntuottaja sitoutuu pitämään salassa kaiken Luottamuksellisen tiedon ja käsittelemään sitä tämän Salassapito- ja Turvallisuusliitteen vaatimusten mukaisesti. Palveluntuottaja ei käytä, käsittele tai talleta Luottamuksellista tietoa muutoin kuin Sääntökirjan mukaisten palveluiden toteuttamiseksi.

2.3 Palveluntuottaja ei paljasta tai luovuta Luottamuksellista tietoa ulkopuolisille tahoille ilman Palvelunjärjestäjän kirjallista suostumusta. Palveluntuottajalla on kuitenkin oikeus luovuttaa viranomaisille tietoja, jotka se on velvollinen lain tai oikeuden päätöksen perusteella luovuttamaan. Palveluntuottajan tulee ilmoittaa tästä välittömästi ja kirjallisesti Palvelunjärjestäjälle sekä kertoa kenelle ja mitä tietoja on luovutettu.

2.4 Mikäli Palveluntuottaja käsittelee Palvelunjärjestäjän Luottamuksellista tietoa Sääntökirjan palveluiden toteuttamiseksi sähköpostissa, pilvipalveluratkaisuissa taikka muilla tavoin Palveluntuottajan sisäverkon ulkopuolelta, tulee Palveluntuottajan käyttää monimenetelmäistä todentamista (MFA) Luottamuksellisen tiedon suojaamiseksi.

2.5 Palveluntuottaja saattaa Sääntökirjan mukaisten palveluiden toteuttamiseen osallistuvan henkilöstönsä ja käyttämänsä alihankkijat tietoisiksi tämän Salassapito- ja Turvallisuusliitteen salassapitovelvoitteista sekä vastaa siitä, että he noudattavat näitä salassapitoehtoja tai heitä koskee lakisääteinen salassapitovelvollisuus.

2.6 Palveluntuottaja sitoutuu lisäksi noudattamaan Palvelunjärjestäjän luottamuksellisuuteen ja turvallisuuteen liittyviä ohjeita, jotka on saatettu Palveluntuottajan tietoon.

2.7 Salassapitovelvollisuus ei koske tietoa, joka on yleisesti saatavilla tai julkista tai jonka Palveluntuottaja on saanut laillisesti haltuunsa muuten kuin Palvelunjärjestäjältä.

3 Hallinnollinen ja fyysinen tietoturva

3.1 Palveluntuottaja toteuttaa asianmukaiset toimenpiteet, joita tarvitaan Luottamuksellisen tiedon suojaamiseksi luvattomalta tietoihin pääsyltä tai tietojen tuhoutumiselta tai muuttumiselta.

3.2 Palveluntuottajalla on tietoturvan hallintamalli, jonka avulla toteutetaan Palvelunjärjestäjän asettamia tietoturvatavoitteita ja vaatimuksia. Palveluntuottaja määrittelee ja nimittää organisaatiossaan tietoturvallisuuteen liittyvät roolit ja vastuut yleisesti tai Sääntökirjan mukaisten palveluiden toteuttamiseksi.

3.3 Palveluntuottaja tunnistaa ja dokumentoi Sääntökirjan kohteeseen liittyvät järjestelmät ja huolehtii niiden sisältämien tietojen luottamuksellisuuden, eheyden, saatavuuden, käytettävyyden ja kiistämättömyyden toteuttamisesta Sääntökirjan ja tässä Salassapito- ja Turvallisuusliitteessä esitettyjen vaatimusten mukaisesti.

3.4 Palveluntuottaja sitoutuu jatkuvasti kehittämään ja vastaa tuottamansa palvelun tietoturvallisuuden ja jatkuvuuden jatkuvasta kehittämisestä.

3.5 Palveluntuottajan toimitilojen turvallisuus, kun Palvelusetelikäsikirjan mukaisiin palveluihin liittyvä työ suoritetaan Palveluntuottajan tai sen alihankkijan tiloissa, riippumatta siitä ovatko Palveluntuottajan tilat omia vai Palveluntuottajan hallinnoimia.

3.6 Palveluntuottajan tulee toteuttaa ja ylläpitää asianmukaiset fyysisen turvallisuuden toimenpiteet kaikissa tiloissaan, joissa käsitellään Palvelunjärjestäjän Luottamuksellista tietoa. Tämä sisältää pääsynvalvontajärjestelmät, kuten kulunvalvonta- ja henkilötunnistusjärjestelmät, joilla varmistetaan, että vain valtuutetut henkilöt pääsevät käsiksi Luottamukselliseen tietoon.

3.7 Palveluntuottajan on varmistettava, että kaikki työtilat, joissa käsitellään Palvelunjärjestäjän Luottamuksellista tietoa, ovat valvottuja ja suojattuja. Tämä voi sisältää jatkuvan videovalvonnan, vartioinnin ja muiden valvontamenetelmien käytön, joilla estetään luvaton pääsy tiloihin.

3.8 Palveluntuottajan on toteutettava säännölliset fyysisen turvallisuuden tarkastukset ja riskienarvioinnit tiloissaan varmistaakseen, että kaikki turvatoimenpiteet ovat ajantasaisia ja tehokkaita. Mahdolliset havaittavat puutteet on korjattava viipymättä.

3.9 Palveluntuottajan on noudatettava kaikkia sovellettavia lakeja ja määräyksiä, jotka koskevat fyysistä turvallisuutta ja tietosuojaa, ja varmistettava, että kaikki toimenpiteet ja käytännöt täyttävät nämä vaatimukset.

3.10 Palveluntuottajan tulee varmistaa tilojen tarkoituksenmukainen fyysinen turvallisuus tulipalon, sähkökatkosten, vesivaurioiden, ulkopuolisten häiriötekijöiden ja muiden vastaavien erityistilanteiden varalta.

3.11 Palveluntuottajan on varmistettava, että kaikki Luottamuksellista tietoa käsittelevät laitteet, kuten tietokoneet, palvelimet ja tallennusvälineet, ovat suojattuja asianmukaisin fyysisin turvatoimenpitein. Tämä sisältää laitteiden lukitsemisen, niiden sijoittamisen turvallisiin tiloihin ja pääsyn rajoittamisen vain valtuutetuille henkilöille.

3.12 Henkilöt, joille ei ole myönnetty oikeutta Luottamukselliseen tietoon, saavat oleskella tiloissa ainoastaan valvonnan alaisina. Valvontaa ei edellytetä, mikäli Luottamuksellista tietoa säilytetään tai käsitellään tiloissa siten, että nämä henkilöt eivät voi päästä niihin käsiksi. Palveluntuottaja arvioi ja toteuttaa riittävän valvontaratkaisun kuhunkin tarpeeseen.

3.13 Alihankkijat

3.13.1 Palveluntuottaja huolehtii, että Palveluntuottajan alihankkijoihin ja heidän palveluksessaan oleviin henkilöihin sovelletaan samoja tai sisällöllisesti saman sisältöisiä ehtoja kuin on tässä Salassapito- ja Turvallisuusliitteessä Palveluntuottajalle asetettu.

3.13.2 Palveluntuottaja vastaa käyttämiensä alihankkijoiden toiminnasta kuin omastaan.

3.14 Auditoinnit

3.14.1 Palvelunjärjestäjällä tai sen nimeämällä riippumattomalla kolmannella osapuolella, joka ei voi olla Palveluntuottajan kilpailija, on oikeus auditoida Palveluntuottajan Sääntökirjan mukaisten

palveluiden toteuttamiseen liittyvät turvallisuusmenettelyt varmistuakseen siitä, että Palveluntuottaja on täyttänyt Sääntökirjan ja tämän Salassapito- ja Turvallisuusliitteen mukaiset velvollisuutensa.

3.14.2 Tarkastus toteutetaan lähtökohtaisesti 30 vuorokauden varoitusaikaa noudattaen. Mikäli Palvelunjärjestäjä voi osoittaa erityisen perusteen tarkastuksen toteuttamiselle, kuten kohtuulliset syyt epäillä Sääntökirjan ehtojen rikkomista tai tietoturvaloukkausta, on Palvelunjärjestäjällä oikeus käynnistää tarkastusmenettely 7 vuorokauden ilmoitusaikaa noudattaen sen lisäksi, mitä tässä Salassapito- ja Turvallisuusliitteessä todetaan muusta avustamisesta. Ilman erityistä perustetta tehtäviä tarkastuksia voidaan suorittaa enintään yksi (1) vuodessa.

3.14.3 Kumpikin Osapuoli vastaa tarkastuksesta itselleen aiheutuneista kustannuksista. Mikäli tarkastuksessa havaitaan merkittäviä puutteita, Palveluntuottaja vastaa tarkastuksesta Palvelunjärjestäjälle ja Palveluntuottajalle aiheutuneista tarkastuksen kohteen mukaan kohtuullisista kustannuksista sekä Palvelunjärjestäjän nimeämän kolmannen osapuolen palkkiosta ja kuluista.

3.14.4 Palveluntuottaja sitoutuu avustamaan Palvelunjärjestäjää ja Palvelunjärjestäjän nimeämää kolmatta osapuolta tarkastuksen suorittamisessa.

4 Palveluntuottajan henkilöstö

4.1 Palveluntuottajan tulee erillisestä pyynnöstä toimittaa listaus palvelusetelillä toteutettavien sosiaali- ja terveydenhuollon palveluiden tuottamiseen käyttämästään henkilöstöstä Palvelunjärjestäjälle. Mikäli Sääntökirjassa on mainittu, että Palveluntuottaja toimittaa listauksen palvelusetelillä toteutettavien sosiaali- ja terveydenhuollon palveluiden tuottamiseen käyttämästään henkilöstöstä, sovelletaan Sääntökäsikirjaa. Palvelunjärjestäjällä on oikeus joko hyväksyä tai hylätä Palveluntuottajan Palvelunjärjestäjälle ehdottama palvelusetelillä toteutettavien sosiaali- ja terveydenhuollon palveluiden tuottamiseen käytettävä henkilöstö perustellusta syystä.

4.2 Palvelunjärjestäjällä on oikeus teettää sille nimetystä Palveluntuottajan henkilöstöstä turvallisuusselvitys sikäli, kun sovellettava lainsäädäntö sen sallii.

4.3 Palvelunjärjestäjä voi erikseen pyytää nimettyjä Palveluntuottajan henkilöstön jäseniä allekirjoittamaan henkilökohtaisen salassapitosopimuksen.

4.4 Palveluntuottaja sitoutuu varmistamaan, että kaikki henkilöt, joilla on oikeus Sääntökirjan mukaisten palveluiden toteuttamiseksi käsitellä Luottamuksellista tietoa, käsittelevät niitä ainoastaan Palvelunjärjestäjän antamien ohjeiden mukaisesti ja Palvelunjärjestäjän asettamien tietoturvallisuusvaatimusten mukaisesti.

4.5 Henkilön, joka toimii Palveluntuottajan lukuun Palvelunjärjestäjän tiloissa, on aina pyydettäessä todistettava henkilöllisyytensä Palvelunjärjestäjälle henkilökortilla tai muulla yhdessä sovitulla tavalla ennen Sääntökirjan mukaisen tehtävän suorittamista.

4.6 Palveluntuottaja estää järjestelmien käytön teknisesti, kun henkilön peruste Luottamuksellisen tiedon käsittelylle on päättynyt.

5 Pääsy palvelunjärjestäjän järjestelmiin

5.1 Palveluntuottajan tulee huolehtia sille annetuista salasanoista, tunnistautumisvälineistä ja pääsystä Palvelunjärjestäjän hallinnassa oleviin tietojärjestelmiin, verkkoihin tai sähköisiin ratkaisuihin siten,

että vain niillä Palveluntuottajan henkilöillä on pääsy näihin käsiksi, joiden Palvelunjärjestäjän kanssa palvelusetelillä toteutettavien sosiaali- ja terveydenhuollon palveluiden tuottamiseen liittyvät tehtävät välttämättä tätä edellyttävät.

5.2 Palveluntuottaja huolehtii siitä, että Palvelunjärjestäjän sille luovuttamia tunnuksia käytetään vain niihin tarkoituksiin, joita Palveluntuottajan Palvelunjärjestäjälle suorittamat tehtävät edellyttävät.

5.3 Palveluntuottaja ei saa liittyä Palvelunjärjestäjän järjestelmiin muutoin, kuin erikseen Palvelunjärjestäjän tälle osoittamin henkilökohtaisin tunnuksin ja/tai tunnistautumisvälinein.

6 Tietoturvapoikkeamat

6.1 Palveluntuottaja ilmoittaa kirjallisesti Palvelunjärjestäjän tietoturvavastaavalle osoitteeseen tietoturvavastaava@pirha.fi havaitsemistaan Luottamukselliseen tietoon kohdistuvista tietoturvapoikkeamista ilman aiheetonta viivytystä ja joka tapauksessa viimeistään 72 tunnin kuluessa siitä, kun Palveluntuottaja on tullut tietoiseksi poikkeamasta.

6.2 Tietoturvapoikkeaman havaittuaan Palveluntuottajan tulee ryhtyä viipymättä toimenpiteisiin tietoturvapoikkeaman poistamiseksi ja sen vaikutusten rajoittamiseksi ja korjaamiseksi sekä vastaavan tietoturvapoikkeaman ehkäisemiseksi tulevaisuudessa.

7 Vastuut

7.1 Sääntökirjassa mahdollisesti olevaa vastuunrajoituslauseketta ei sovelleta tähän Salassapito- ja turvallisuusliitteen mukaisten velvoitteiden rikkomiseen.

7.2 Palveluntuottaja on vastuussa kaikista välittömistä vahingoista aiheutuneista kustannuksista täysimääräisesti, jotka ovat aiheutuneet Palvelunjärjestäjälle tästä Salassapito- ja Turvallisuusliitteestä johtuvien velvoitteiden rikkomisesta. Näiden ehtojen mukaiset vahingonkorvausvelvollisuuden rajoitukset eivät koske tapausta, jossa Osapuoli on aiheuttanut vahingon tahallisesti tai törkeällä huolimattomuudella. Palveluntuottajan enimmäisvastuu vahinkotapahtumaa kohden on suurin seuraavista: viisi (5) kertaa 12 kuukauden Sääntökirjan mukaisten palveluiden perusteella suoritettavien toistuvaismaksujen laskennallinen määrä tai 100 000 euroa. Palveluntuottaja ei vastaa välillisistä vahingoista.

7.3 Palveluntuottaja on vahingon havaittuaan velvollinen ryhtymään asianmukaisiin toimenpiteisiin vahingon rajoittamiseksi.

8 Salassapito- ja turvallisuusmääräysten voimassaolo

8.1 Palveluntuottajan salassapitoa ja vastuuta koskevat ehdot sekä muut sellaiset määräykset, joiden on katsottava tarkoitetun jäämään voimaan palvelusetelituottajuuden jälkeenkin, pysyvät voimassa.