Tietoturva-suunnitelman koulutus-tilaisuus

THL:n määräys 3/2024 tietoturvasuunnitelmaan sisällytettävistä selvityksistä ja vaatimuksista

Terveyden ja hyvinvoinnin laitos

Tietoturvasuunnitelman koulutustilaisuuden ohjelma 4.6.2024

Klo 9:00-9:05	Tilaisuuden avaus, tavoitteet ja kulku
Klo 9:05-9:20	Taustoitusta sosiaali- ja terveydenhuollon digitaalisen kehittämisen ja jatkuvan toiminnan riskien hallintaan
Klo 9:20-9:45	Määräykset, säädösympäristö ja palvelunantajan velvollisuudet asiakastietolaissa
Klo 9:45-9:55	Tauko
Klo 9:55-10:20	Palvelunantajan, apteekin, välittäjän ja Kelan velvollisuus laatia, katselmoida ja ylläpitää THL:n määräyksen 3/2024 mukaista tietoturvasuunnitelmaa sekä seurata suunnitelman toteutumista – määräyksen 3/2024 keskeisten asioiden läpikäynti
Klo 10:20-11:05	Vinkkejä ja linkkejä suunnitelman laadintaan ja päivittämiseen määräyksen liitteen, tietoturvasuunnitelman mallipohjan avulla
Klo 11:05-11:15	Tilaisuuden yhteenveto
Klo 11:15-11:30	Kysymyksiä ja keskustelua
Klo 11:30	Tilaisuuden päätös

Tilaisuuden tavoitteet ja kulku

- Taustoittaa sosiaali- ja terveydenhuollon digi-kehittämistä ja riskien hallintaa
- Antaa yleiskuva voimassa olevasta asiakastietolaista ja THL:n määräyksistä 2024
- Antaa yleiskuva tietoturvasuunnitelmasta ja sen suhteesta tietojärjestelmien olennaisiin vaatimuksiin
- Esitellä tietoturvasuunnitelman sisältöä ja laadintaa käytännössä

- Tilaisuuden jälkeen vastaukset kootaan tilaisuuden aikana chattiin mahdollisesti nouseviin aiheeseen liittyviin kysymyksiin. Vastaukset, kuten tämä esityskin julkaistaan Tiedonhallinta sosiaali- ja terveysalalla kokonaisuuden Koulutusmateriaalit –sivulla

- Koulutuksen aikana saa esittää kysymyksiä Teams-chatin kautta tai jälkikäteen lähettämällä kysymyksiä osoitteeseen sotetiedonhallinta@thl.fi.

Taustoitusta sosiaali- ja terveydenhuollon digitaalisen kehittämisen ja jatkuvan toiminnan riskien hallintaan

- Klo 9:05-9:25
- Antti-Olli Taipale

Alkuun vähän historiaa 1.7.2007 – nykypäivä 4.6.2024

Kumoutuneet

- Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä 159/2007

X
  - Ollut voimassa 1.7.2007-31.10.2021
  - THL:n määräys 2/2015 Omavalvontasuunnitelmaan sisällytettävistä selvityksistä ja vaatimuksista.

- Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä 784/2021

X
  - Ollut voimassa 1.11.2021-31.12.2023
  - THL:n määräys 3/2021 **Tietoturvasuunnitelmaan** sisällytettävistä selvityksistä ja vaatimuksista.

Voimassa

- Laki sosiaali- ja terveydenhuollon asiakastietojen käsittelystä 703/2023 – 1.1.2024 lähtien
  - THL:n määräys 3/2024 **Tietoturvasuunnitelmaan** sisällytettävistä selvityksistä ja vaatimuksista – 22.2.2024 lähtien

Tietoturvasuunnitelman perustana 1.1.2024 voimaan tullut asiakastietolaki

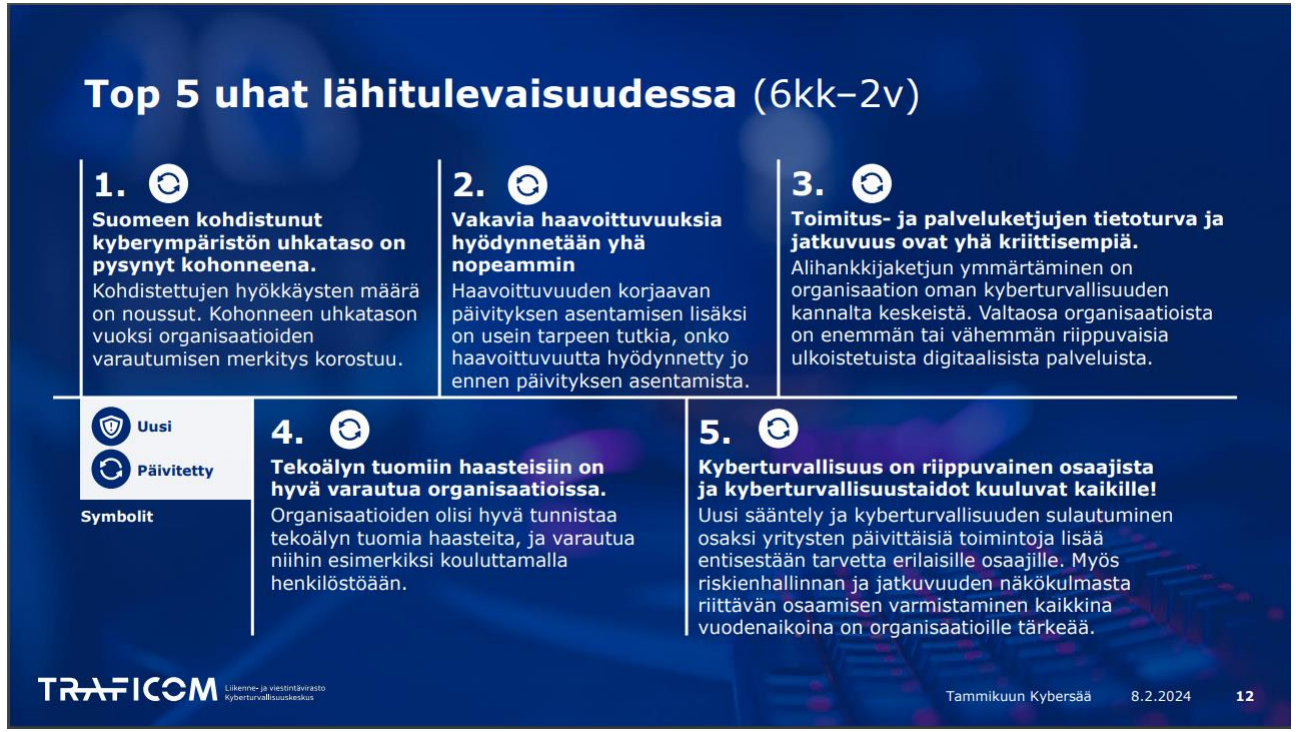
- Laki sosiaali- ja terveydenhuollon asiakastietojen käsittelystä 703/2023 ja sieltä erityisesti **pykälät 77** ja **78**:

- 77 §: ”**Palvelunantajan, apteekin, välittäjän ja Kansaneläkelaitoksen on laadittava** tietoturvaan ja tietosuojaan sekä tietojärjestelmien käyttöön liittyvä tietoturvasuunnitelma. Tietoturvasuunnitelmassa on selvitettävä, miten asiakas- ja potilastietojen käsittelyyn ja tietojärjestelmiin liittyvät vaatimukset varmistetaan:…”

- 78 §: ”Sosiaali- ja terveydenhuollon **palvelunantajan vastaavan johtajan ja apteekkarin on huolehdittava**, että 77 §:ssä tarkoitettu **tietoturvasuunnitelma laaditaan ja sitä noudatetaan**. Palvelunantajan, apteekin ja Kansaneläkelaitoksen tulee oma-aloitteisesti ryhtyä tarvittaviin toimenpiteisiin, jos joku on lainvastaisesti käsitellyt asiakastietoja. …”.

Minkälaisessa maailmassa elämme vs. digiturvallisuus 1/2?

- Traficomin Kyberturvallisuuskeskuksen tammikuun Kybersää nosti esille vuoden 2023 trendit ja Top 5 uhat lähitulevaisuudessa 2024-2026.



Minkälaisessa maailmassa elämme vs. digiturvallisuus 2/2?

17.1.2024

mtv UUTISET

Tena-tuotteiden valmistajan toimet syynissä – taustalla jättimäinen tietomurto

LEHTIKUVA

JULKAISTU 1701.2024 13:58

MTV UUTISET – STT

Tietosuojavaltuutetun toimisto selvittää parhaillaan Tenan inkontinenssisuojia valmistavan Essity-yhtiön ja lääkealan yhtiön Roche Diagnosticsin toimintaa Westlog-yhtiöön tehdyn tietomurron vuoksi.

24.1.2024

ILTA-SANOMAT

TIETOTURVA

OmaKanta-huijaus yrittää viedä rahasi – näin sen erottaa aidosta sivusta

Huijaussivu näyttää varsin aidolta.

JAA TALLENNA KOMMENTIT

IL 21.5.2024

KOTIMAA

Uutta tietoa: Helsingin tietomurto pelättyäkin laajempi – Näitä tietoja viety

Helsingin kaupunki kertoi uutta tietoa vappuaattona havaitusta tietomurrosta.

Näin tietomurrosta kerrottiin Helsingin kaupungin tiedotustilaisuudessa 13. toukokuuta.
HELSINKI-KANAVA

Jussi Korhonen
Eilen klo 15:45

4.5.2024

ILTA-SANOMAT

DIGITODAY

Osa Vastaamo-potilaista sai vasta tietää kuuluvansa tietomurron uhreihin – ”Valtava järkytys”

Tuhannet ihmiset eivät tehneet rikosilmoitusta Vastaamo-jutussa. Nyt on paljastunut, että osa ei edes tiennyt olleensa kiristysviestin vastaanottajien joukossa.

JAA TALLENNA

Syyttäjälaitos opastaa ihmisiä tekemään tietopyynnön Kelaan, jos he haluavat selvittää, mitä tietoja heistä oli tallennettu Vastaamon rekisterelhin marraskuussa 2018 tapahtuneeseen tietomurtoon mennessä. KUVA: EMMI KORHONEN / LEHTIKUVA

STT, Maria Rosvall
4.5. 12:55

Tekoälypohjaiset huijaukset kiihtyvät – uutisotsikot hämmentävät

9.3.2024

ILTA-SANOMAT

TIETOTURVA

Ann-Lisin tytär pyysi 15 000 kruunua – pelätty huijaus saapui Ruotsiin, ja suomalaisilla on vain hetki aikaa

Hei äiti -huijaukset ottivat merkittävän askeleen naapurissa. Nainen vakuuttui puhuvansa tyttärensä kanssa ja suostui rahansiirtoon.

JAA TALLENNA KOMMENTIT

Vieras numero on oiva merkki mahdollisesta huijauksesta. KUVA: COLOURBOX

Henrik Kärkkäinen, Tuomas Linnake
9.3. 8:40

RUOTSISSA Malmössä todistettiin uudenlaista versiota niin sanotusta Hei äiti -huijauksesta, joissa rikolliset tekeytyvät uhrin lapseksi ja pyytävät jollakin verukkeella pikaisesti rahaa. Tapauksesta uutisoivat Dagens Nyheter ja TV4 Nyheterna. Alun perin tapauksesta kertoi Sydsvenskan.

Häijy tekoälyllä tehty huijausyritys paljastui Suomessa – "Hyvin aidon kuuloinen"

mtv UUTISET

25.2.2024

Kuvituskuva. LEHTIKUVA

JULKAISTU 25.02.2024 10:18

MTV UUTISET – STT

Suomalaisen yrityksen toimitusjohtaja pyytää Whatsappilla lähetetyssä ääniviestissä työntekijöitä tekemään ison rahasiirron.

Viesti on englanniksi, ja se tulee toimitusjohtajan kuvalla varustetusta profiilista. Useissa maissa toimiva yritys käyttää englantia sisäisessä viestinnässään.

Työntekijöille selviää kuitenkin nopeasti, että kyseessä on huijaus, eikä rahoja siirretä. Viesti ei ollut johtajan itsensä äänittämä.

Huijarit olivat luoneen tekoälyn avulla yrityksen johtajan puheelta kuulostavan ääniviestin. Myös Whatsapp-profiili oli tekaistu.

4.12.2023

yle Etusivu Vaalikone Venäjän hyökkäys UMK24

Turvallisuus

Romanssihuijarit ovat jo valjastaneet tekoälyn käyttöönsä – videopuhelussa näkemääsi ihastusta ei ehkä ole olemassakaan

Järjestäytynyt rikollisuus kouluttaa jäseniään hyödyntämään uusinta teknologiaa. Jo verkon ilmaisohjelmat ja diginatiivius tarjoavat valmiudet huijauksiin.

11.9.2023

mtv UUTISET

Asiantuntija varoittaa yhä uskottavammista tekoälyn luomista huijauksista: "Minua on huijattu ja tullaan huijaamaan"

14.8.2023

yle Etusivu Vaalikone Venäjän hyökkäys UMK24

Teknologia

Tekoälyn tekemät monimutkaiset huijaukset lisääntyvät Suomessakin muutaman vuoden sisään, asiantuntija ennakoi

Tekoäly pystyy jo matkimaan ihmisääntä keräämänsä aineiston pohjalta. Hädissään soittava "lapsi" voi olla huijausta.

thl

Tietoturvasuunnitelma

- edistää asiakas- ja potilastietojen turvallista käsittelyä
- parantaa ja yhdenmukaistaa sote-toimijoiden tietosuojaa ja tietoturvaa
- vahvistaa tietoturvallisuuden ja tietosuojan suunnittelun ja toteuttamisen käytäntöjä
- auttaa erityisesti hallitsemaan tämän päivän **digitaaliseen turvallisuuteen liittyviä riskejä**.

- Tietoturvasuunnitelman laativat kaikki sosiaali- ja terveydenhuollon palvelunantajat, apteekit, välittäjät ja Kansaneläkelaitos.
- Organisaation **velvollisuutena** on **toimia tietoturvasuunnitelman mukaisesti**, **katselmoida** ja ylläpitää suunnitelmaa säännöllisesti sekä **seurata aktiivisesti** sen toteutumista.

! **Tietoturvasuunnitelman laatimiseen velvoitetuista tahoista** eli sosiaali- ja terveydenhuollon palvelunantajista, apteekeista, välittäjistä ja Kansaneläkelaitoksesta (Kela), käytetään määräyksessä ja määräyksen liitteessä yleisnimeä tietoturvallisuuden omavalvonnan kohde.

Mitä tietoturvasuunnitelma sisältää 1/3?

- Tietoturvasuunnitelma kuvaa, miten organisaatio järjestää toiminnassaan tietoturvan ja -suojan omavalvonnan

- Tietoturvasuunnitelmasta tulee selvitä, miten tietoturvallisuuden omavalvonnan kohde täyttää tietoturvaan ja tietosuojaan liittyvät asiakastietolain vaatimukset ja velvoitteet

- Tietoturvasuunnitelmaa ja siitä viitattuja liitedokumentteja tulee käsitellä ja säilyttää tietoturvallisesti. Ne tulee suojata sivullisilta, ja tarvittaessa niihin tulee merkitä salassa pidettävä -tieto. Tietoturvasuunnitelma on aina ei-julkinen asiakirja. Tietoturvasuunnitelmaa ei tule sisällyttää tai yhdistää julkaistaviin tai julkisesti saatavilla oleviin omavalvontasuunnitelmiin.

Mitä tietoturvasuunnitelma sisältää 2/3?

- Asiakastietolain (77 §) vaatimukset kiteytettyinä tietoturvasuunnitelmalle:
  - ▶ tietojärjestelmien käyttäjillä on käytön vaatima koulutus
  - ▶ käyttöohjeet ovat saatavilla järjestelmän yhteydessä
  - ▶ käyttäjät noudattavat tietojärjestelmäpalvelun tuottajan ohjeita
  - ▶ tietojärjestelmiä ylläpidetään ja päivitetään tietojärjestelmäpalvelun tuottajan ohjeistuksen mukaisesti…

Mitä tietoturvasuunnitelma sisältää 3/3?

- ...käyttöympäristö soveltuu tietojärjestelmien asianmukaiseen käyttöön ja varmistaa tietoturvan ja tietosuojan ja tietojärjestelmiin kohdistuvien riskien hallinnasta huolehditaan
- tietojärjestelmiin liitetyt muut järjestelmät eivät vaaranna tietojärjestelmien suorituskykyä eivätkä niiden tietoturva- tai tietosuojaominaisuuksia
- tietojärjestelmiä asentaa, ylläpitää ja päivittää vain henkilö, jolla on siihen tarvittava ammattitaito ja asiantuntemus ja tietojärjestelmiä asentavan henkilön luotettavuus on varmistettu, jos henkilö tehtävissään pääsee käsittelemään asiakastietoja tai jos hän muuten tehtävissään voi vaarantaa sosiaali- ja terveydenhuollon jatkuvuuden kannalta kriittisten tietojärjestelmien toimintaa
- tietojärjestelmät täyttävät käyttötarkoituksensa mukaiset olennaiset vaatimukset.

Riskit hallintaan tietoturvasuunnitelmalla 1/3

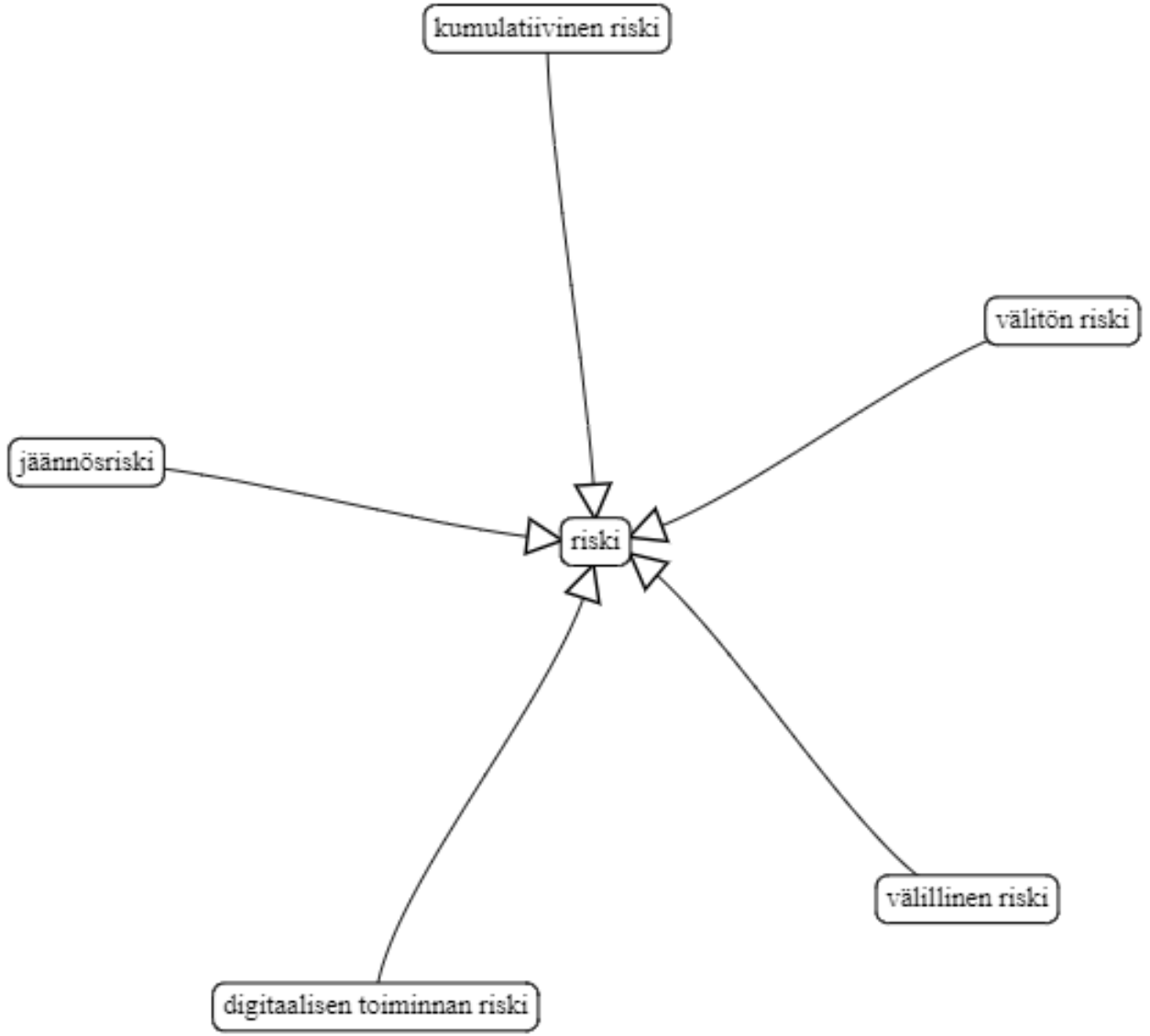
- **Kumulatiivinen riski** – riski, jonka suuruus muodostuu useiden riskitekijöiden yhteisvaikutuksista
- **Välitön riski** – riski, jonka lähde vaikuttaa suoraan kohteeseen
- **Välillinen riski** – riski, jonka lähde vaikuttaa epäsuorasti kohteeseen
- **Digitaalisen toiminnan riski** – digitaalisessa toimintaympäristössä vaikuttava, digitaaliseen toimintaympäristöön kohdistuva tai siitä johtuva riski
- **Jäännösriski** – riskin käsittelyn jälkeen jäljellä oleva riski.

Riskimäärittelyjen lähde, VAHTI-riskienhallintasanasto digitaaliseen toimintaympäristöön (DVV)

Riskit hallintaan tietoturvasuunnitelmalla 2/3

”Tietoturvallisuuden omavalvonnan kohteen **velvollisuutena** on toimia laatimansa tietoturvasuunnitelman mukaisesti, **säännöllisesti ylläpitää ja katselmoida** suunnitelmaansa sekä seurata aktiivisesti sen toteutumista.

Kyse on jatkuvasta ja säännöllisestä riskienhallinnasta, asianmukaisten tietoturvallisuuden ja asiakastietojen käyttöön liittyvien käytäntöjen varmistamisesta sekä niiden toteuttamisesta.”



Kuvan lähde, VAHTI-riskienhallintasanasto digitaaliseen toimintaympäristöön (DVV)

Riskit hallintaan tietoturvasuunnitelmalla 3/3

- Tietoturvasuunnitelman tavoitteena on varmistaa, että asiakastiedon käsittelyssä otetaan riskilähtöisesti ja kattavasti huomioon tietosuojaan ja tietoturvaan liittyvät asiat tietoturvallisuuden omavalvonnan kohteen toiminnassa ja tietojärjestelmien käyttöympäristössä.
- Tietoturvasuunnitelmassa kuvattujen menettelyiden ja keinojen avulla voidaan ehkäistä riskien toteumista osana riskien hallintaa.
- Tietoturvasuunnitelma tulee laatia arvioiden mahdollisia riskejä, niihin liittyviä todennäköisyyksiä sekä todettujen riskien vaikutuksia.
- Tietoturvasuunnitelmassa tulee arvioida riskien vähentämisen (hyväksyttävät jäännösriskit) tai niiden kokonaan poistamisen seuraukset.
- Tietoturvasuunnitelmassa kuvatuilla menettelyillä ja keinoilla myös varmistetaan, että tietojärjestelmiin liitetyt muut kuin asiakastietojen käsittelyyn tarkoitetut tietojärjestelmät tai sovellukset eivät vaaranna tietojärjestelmien suorituskykyä eivätkä niiden tietoturva- tai tietosuojaominaisuuksia. Käyttöympäristöön ja tietojärjestelmiin kohdistuvien riskien hallinnasta on huolehdittava.

Mitä sote-kentällä ajatellaan riskeistä?

Riskien ”hillotaulu” -yhteenveto RRP:n investointi 4:n verkostotapaamisesta 1.2.2024

Määräykset, säädösympäristö ja palvelunantajan velvollisuudet asiakastietolaissa

- Klo 9:20-9:45
- Juha Mykkänen

Säädösten pohja: tietoturvallisuuden perusperiaatteet

- Eheys
  - tarkkuus ja yhdenmukaisuus säilyvät tiedon elinkaaren ajan
  - luvaton muokkaaminen ei onnistu tai se havaitaan
- Luottamuksellisuus
- Saatavuus ja luotettavuus
  - tieto on saatavilla, kun sitä tarvitaan
  - ohjelmistot, laitteet, turvallisuus ja viestinvälitykset toimivat
- Autenttisuus
  - tiedon alkuperä on tiedossa
  - tiedonvaihdon osapuolet tunnistetaan luotettavasti
- Kiistämättömyys ja velvoittavuus
  - sopimuksen velvoitteet täytetään
  - osapuoli ei voi kiistää osallistumistaan tapahtumaan

Monet tietoturvallisuustoimenpiteet palvelevat useita tavoitteita (esimerkkinä olennaisten tietoturvavaatimusten luokat / THL määräys 5/2024 liite 2)

- Eheys
  - tarkkuus ja yhdenmukaisuus säilyvät tiedon elinkaaren ajan
  - luvaton muokkaaminen ei onnistu tai se havaitaan
- Luottamuksellisuus
- Saatavuus ja luotettavuus
  - tieto on saatavilla, kun sitä tarvitaan
  - ohjelmistot, laitteet, turvallisuus ja viestinvälitykset toimivat
- Autenttisuus
  - tiedon alkuperä on tiedossa
  - tiedonvaihdon osapuolet tunnistetaan luotettavasti
- Kiistämättömyys ja velvoittavuus
  - sopimuksen velvoitteet täytetään
  - osapuoli ei voi kiistää osallistumistaan tapahtumaan

Sote-tiedonhallinnan sääntely-ympäristö

- Yleislait ja julkista hallintoa koskevat säädökset (4)
- **Sähköistä tiedonhallintaa koskeva lainsäädäntö (13)**
- Henkilöstöä koskeva lainsäädäntö (5)
- Toimijoita ohjaava lainsäädäntö (10)
- Sosiaalihuollon ja terveydenhuollon yleislait (8+3)
- Sosiaalihuollon erityislainsäädäntö (20)
- Terveydenhuollon erityislainsäädäntö (15)
  - mukaan lukien lääkinnällisten laitteiden säädökset
- Muu lainsäädäntö (5)

”Säädöksiä on suuri määrä, mutta keskeisimpien hallitseminen riittää pitkälle.”

Koosteen lähde:
Sosiaali- ja terveydenhuollon kokonaisarkkitehtuuri: tiedonhallinnan yhteiset periaatteet ja kuvaukset, liite 1 Sosiaali- ja terveydenhuollon lainsäädäntö (2022)

Sähköistä tiedonhallintaa koskeva lainsäädäntö

- Tietosuojalaki
- EU:n yleinen tietosuoja-asetus
- **Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (Asiakastietolaki)**
- Laki julkisen hallinnon tiedonhallinnasta
- Laki sähköisestä asioinnista viranomaistoiminnassa
- Laki digitaalisten palvelujen tarjoamisesta
- Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (Tunnistuslaki)
- Laki hallinnon yhteisistä sähköisen asioinnin tukipalveluista
- Laki sosiaalihuollon asiakasasiakirjoista (kumottu)
- Laki sähköisestä lääkemääräyksestä
- STM:n asetus sähköisestä lääkemääräyksestä
- STM:n asetus potilasasiakirjoista (kumoutunut)
- Laki sosiaali- ja terveystietojen toissijaisesta käytöstä

Koosteen lähde:
Sosiaali- ja terveydenhuollon kokonaisarkkitehtuuri: tiedonhallinnan yhteiset periaatteet ja kuvaukset, liite 1 Sosiaali- ja terveydenhuollon lainsäädäntö (2022)

Tietoturvasuunnitelman ja sote-tietojärjestelmien olennaisten vaatimusten säädökset

Lait (STM)

- Laki sosiaali- ja terveydenhuollon asiakastietojen käsittelystä 703/2023
  - Aiemmat versiot ja päivitykset 159/2007, 1227/2010, 250/2014, 784/2021
- Laki sähköisestä lääkemääräyksestä 61/2007
  - Päivitykset: 251/2014, 786/2021 ja 706/2023

Määräykset (THL)

- Määräys 3/2024: Määräys tietoturvasuunnitelmaan sisällytettävistä selvityksistä ja vaatimuksista
  - Aiemmat versiot ja edeltäjät: Määräykset 3/2021 ja 2/2015
- Määräys 4/2024: Määräys sosiaali- ja terveydenhuollon tietojärjestelmien ja hyvinvointisovellusten luokittelusta ja sertifioinnista
- Määräys 5/2024: Määräys sosiaali- ja terveydenhuollon tietojärjestelmien ja hyvinvointisovellusten olennaisista vaatimuksista
  - Aiemmat versiot ja edeltäjät ja aiempia täydentäneet määräykset: Määräykset 1/2015, 2/2016, 4/2021, 5/2021, 6/2021, 1/2022, 1/2023

23

Tietoturvasuunnitelman suhde tietojärjestelmien olennaisiin vaatimuksiin

Perusperiaate: tietojärjestelmien olennaiset vaatimukset (määräykset 4 ja 5) sekä tietoturvan ja tietosuojan omavalvonta (määräys 3) muodostavat **jatkumon** teknisistä järjestelmäratkaisuista **turvallisiin käytäntöihin ja toimintatapoihin sote-toimijoiden arjen päivittäisessä työssä**

Tietojärjestelmän valmistajan ja tietojärjestelmäpalvelun tuottajan (yleensä tietojärjestelmätoimittaja) on suunniteltava ja toteutettava järjestelmänsä niin että se täyttää järjestelmää koskevat olennaiset vaatimukset
- myös järjestelmän luokittelu
-tarvittaessa järjestelmän sertifiointi
-järjestelmän rekisteröinti

Palvelunantajan on mm.:
-varmistettava, että tietosuoja ja tietoturvallisuus toteutuvat sen omassa toiminnassa
-varmistettava osaltaan, että toiminnassa käytettävät tietojärjestelmät täyttävät olennaiset vaatimukset
-**tietoturvasuunnitelma** keskeinen väline

Tulossa koulutus:
Sote-tietojärjestelmien olennaiset vaatimukset ja sertifiointi
pe 14.6.2024 klo 9-12

Miten varmistan palvelunantajana olennaisten vaatimusten täyttämisen käyttämissäni tietojärjestelmissä?

- Hankintojen yhteydessä
  - Osana tarjouspyynnön pakollisia vaatimuksia erittely, mitä kansallisesti määriteltyjä käyttötarkoituksia (profiileja) järjestelmässä on täytettävä
  - Oikeus saada tietojärjestelmätoimittajalta selvitys (järjestelmälomake) kansallisten olennaisten vaatimusten täyttämisestä
  - Sertifioitu on turvallisempi kuin sertifioimaton!
- Tietoturvasuunnitelman ylläpidossa ja päivittämisessä
- Valviran tietojärjestelmärekisteri sisältää
  - tiedot tietojärjestelmistä ja niiden käyttötarkoituksista
  - tiedot kunkin järjestelmän vaatimustenmukaisuuden voimassa olosta (tietoturvallisuustodistuksen voimassa olo, Kanta-palveluihin liittyville järjestelmille suoritetut yhteistestaukset)
- Määräys 5/2024 Liite 1 luku 4: Olennaisten vaatimusten ja profiilien hyödyntäminen sote-organisaatioissa

thl

Tulossa koulutus:

Sote-tietojärjestelmien olennaiset vaatimukset ja sertifiointi

pe 14.6.2024 klo 9-12

Keskeisiä asiakastietolain 703/2023 kohtia tietoturvasuunnitelman näkökulmasta 1/2

1 luku Yleiset säännökset

- 2 § Soveltamisala ja suhde muuhun lainsäädäntöön
- 3 § Määritelmät

10 luku Tietoturvallisuuden ja tietosuojan omavalvonta

- 77 § Tietoturvasuunnitelma
- 78 § Tietoturvallisuuden omavalvonnan toteuttaminen ja vastuu

Keskeisiä asiakastietolain 703/2023 kohtia tietoturvasuunnitelman näkökulmasta 2/2

11 luku Tietojärjestelmien ja hyvinvointisovellusten käyttötarkoitus ja käyttöönotto

- 79 § Tietojärjestelmien ja hyvinvointisovellusten käyttötarkoitus ja luokittelu
- 80 § Tietojärjestelmien ja hyvinvointisovellusten rekisteröinti
- **81 § Tietojärjestelmän ja hyvinvointisovelluksen ottaminen tuotantokäyttöön**
- 82 § Tietojärjestelmän ja hyvinvointisovelluksen käyttöönoton jälkeinen seuranta

12 luku Tietojärjestelmien ja hyvinvointisovellusten olennaiset vaatimukset

Määritelmät: tiedot ja asiakirjat (AsTL 3 §)

(tarkoitetaan…):

2) *asiakirjalla* kirjallista ja kuvallista esitystä sekä sellaista käyttönsä vuoksi yhteen kuuluviksi tarkoitetuista merkeistä muodostuvaa tiettyä kohdetta tai asiaa koskevaa viestiä, joka on saatavissa selville vain automaattisen tietojenkäsittelyn tai äänen- ja kuvantoistolaitteiden taikka muiden apuvälineiden avulla;

3) *asiakasasiakirjalla* asiakirjaa, joka on laadittu tai vastaanotettu tai joka sisältää tietoja asiakkaan sosiaali- tai terveyspalvelujen tarpeen arviointia varten, tarvittavien palvelujen järjestämistä tai toteuttamista varten taikka lääkkeen toimittamista varten;

6) *asiakastiedolla* potilastietoa ja sosiaalihuollon asiakastietoa;

7) *potilastiedolla* potilasasiakirjaan ja muuhun terveydenhuollossa laadittuun asiakirjaan sisältyvää potilaan terveydentilaa tai toimintakykyä tai tämän saamaa terveyspalvelua koskevaa asiakastietoa;

8) *sosiaalihuollon asiakastiedolla* sosiaalihuollon asiakasasiakirjaan ja muuhun sosiaalihuollossa laadittuun asiakirjaan sisältyvää sosiaalihuollon asiakkaan tuen tarvetta, hänen asiansa käsittelyä tai hänelle annettavaa sosiaalipalvelua koskevaa asiakastietoa;

9) *hyvinvointitiedolla* henkilön itsensä tuottamaa ja hallinnoimaa ja hänen terveyttään ja hyvinvointiaan koskevaa tietoa, jonka henkilö on tallentanut 18 kohdassa tarkoitettuun omatietovarantoon;

thl

Määritelmät: tietojärjestelmä (AsTL 3 §)

19) *tietojärjestelmällä* ohjelmistoa, järjestelmää tai osajärjestelmää, jota valmistajan suunnittelemien ominaisuuksien mukaisesti on tarkoitettu käytettäväksi asiakasasiakirjojen sähköiseen käsittelyyn, asiakirjojen tallentamiseen valtakunnallisiin tietojärjestelmäpalveluihin tai valtakunnallisiin tietojärjestelmäpalveluihin liittämiseen tai jolla sosiaali- ja terveydenhuollon ammattihenkilö voi hyödyntää hyvinvointitietoja

- Asiakastietolain tarkoittama tietojärjestelmä on ohjelmisto, joka on suunniteltu nimenomaan *asiakastietojen* käsittelyyn
  - Henkilö- ja asiakastietojen käsittelyä voi tapahtua myös muissa kuin nimenomaan asiakastietojen käsittelyä varten tehdyissä järjestelmissä
  - Lisäksi asiakastietolaissa on erikseen määritelty hyvinvointisovellukset
  - Myös nämä on tärkeää huomioida tietoturvasuunnitelmassa, jos niitä käytetään palvelunantajan toiminnassa!

Määritelmät: palvelunantaja (AsTL 3 §)

11) *palvelunantajalla* viranomaista, julkisoikeudellista yhteisöä ja yksityistä elinkeinonharjoittajaa, joka järjestää tai toteuttaa sosiaalipalveluja tai terveyspalveluja sekä työterveyshuoltolain (1383/2001) 7 §:n 1 momentin 2 kohdassa tarkoitettua työnantajaa

- Sosiaali- ja terveyspalvelujen järjestäjät tai tuottajat
- Julkiset ja yksityiset
- Isot ja pienet
- Useimmat palvelunantajaa koskevat velvoitteet (myös tietoturvasuunnitelman suhteen) koskevat myös apteekkia

30

Määritelmät: välittäjä, tietojärjestelmän valmistaja, tietojärjestelmäpalvelun tuottaja (AsTL 3 §)

20) *tietojärjestelmäpalvelun tuottajalla* tahoa, joka tarjoaa tai toteuttaa palvelunantajalle kohdassa 20 tarkoitettua tietojärjestelmää ja joka vastaa tietojärjestelmän valmistajana, valmistajan lukuun tai yhden tai useamman valmistajan puolesta tietojärjestelmälle asetetuista vaatimuksista;

21) *tietojärjestelmän valmistajalla* tahoa, joka on vastuussa sosiaali- ja terveydenhuollon tietojärjestelmän suunnittelusta ja valmistuksesta;

22) *välittäjällä* palvelunantajan tietojärjestelmäpalvelujen tuottamisessa, tietojärjestelmien teknisen tai fyysisen käyttöympäristön toteuttamisessa tai valtakunnallisiin tietojärjestelmäpalveluihin liittymisessä käyttämää palveluntarjoajaa, jolla on tässä roolissa mahdollisuus nähdä ylläpitotoimien yhteydessä tai muutoin salaamattomia asiakastietoja

- Tietojärjestelmäpalvelun tuottaja, valmistaja ja välittäjä ovat yleensä tietojärjestelmä- tai ict-palvelutoimittajia
  - Joissakin tapauksissa sama yritys voi toimia useissa rooleissa, joissakin tapauksissa voi olla esim. erikseen ulkomainen valmistaja, kotimainen ”maahantuoja”, integraattori, joka toimii myös välittäjänä järjestelmien liittämisessä Kanta-palveluihin, jne.

Palvelunantajan velvoitteita asiakastietolaista ja määräyksistä – kooste 1/4: Kanta

Asiakastietolaissa mainittuja palvelunantajan velvoitteita ovat muun muassa

- **liittyä Kanta-palvelujen käyttäjäksi** säädöksissä kerrottujen määräaikojen mukaisesti (67 §)
  - myös yksityiset, jos käytössä on asiakas- ja potilastietojen käsittelyyn tarkoitettu tietojärjestelmä
- tallentaa asiakasasiakirjat Kanta-palveluihin (69 §)
  - huomioiden siirtymäsäännöksissä asetetut määräajat (102 §)
- vastata Kanta-palveluihin tallennettavien tietojen **oikeellisuudesta (70 §, 71 §, 72 §)**
- laatia ja tallentaa asiakasasiakirjat Kantaan **viivytyksettä (21 §)**
- huolehtia osaltaan asiakkaan **informoinnista** Kanta-palveluihin liittyen (68 §)

Palvelunantajan velvoitteita asiakastietolaista ja määräyksistä – kooste 2/4: Tietojärjestelmät ja olennaiset vaatimukset

Asiakastietolaissa mainittuja palvelunantajan velvoitteita ovat muun muassa

- varmistaa, että käytettävät tietojärjestelmät vastaavat **käyttötarkoitukseltaan** palvelunantajan toimintaa ja täyttävät **olennaiset vaatimukset** ja ja jonka tiedot löytyvät Valviran tietojärjestelmärekisteristä (84 §)
  - olennaiset vaatimukset voidaan täyttää yhden tai useamman tietojärjestelmän kautta
  - ilmoittaa tietojärjestelmäpalvelun tuottajalle ja Valviralle, jos olennaisten vaatimusten täyttymisessä on merkittävä poikkeama
  - ottaa käyttöön säädösten edellyttämät uudet toiminnot määräaikojen mukaisesti
- huomioida, että se ei saa **ottaa käyttöön** tietojärjestelmää (81 §)
  - jonka ajantasaisia tietoja ei löydy Valviran tietojärjestelmärekisteristä
  - jonka tietoturvallisuustodistus (luokan A järjestelmät) on vanhentunut
  - jota ei ole hyväksytysti testattu suhteessa Kanta-palveluihin (Kanta-palveluihin liittyvät luokan A2 tai A3 järjestelmät)
- **ilmoittaa** merkittävä poikkeama tietojärjestelmän olennaisten vaatimusten täyttymisessä tai merkittävä tietoturvallisuuteen liittyvä häiriö (90 §)
  - tietojärjestelmäpalvelun tuottajalle
  - Valviralle jos poikkeama voi aiheuttaa merkittävän riskin asiakasturvallisuudelle tai tietoturvalle

Palvelunantajan velvoitteita asiakastietolaista ja määräyksistä – kooste 3/4: Tietosuoja ja lokiseuranta

- Asiakastietolaissa mainittuja palvelunantajan velvoitteita ovat muun muassa
  - huolehtia henkilö- ja asiakastietojen **salassa pidosta** (5 §)
  - määritellä **oikeudet asiakastietojen käyttöön** ammattihenkilölle ja muille asiakastietoja käsitteleville henkilöille, pidettävä rekisteriä käyttäjistä ja oikeuksista (9 §)
  - huolehtia siitä että asiakastietojen sähköisessä käsittelyssä eri toimijat **tunnistetaan luotettavasti** (8 §)
  - kerätä **lokitiedot** rekisterikohtaisesti kaikesta asiakas- ja potilastietojen **käytöstä ja luovutuksesta** seurantaa ja valvontaa varten (10 §, 70 §)
  - vastata **asiakkaiden tietopyyntöihin ja selvityspyyntöihin** siitä, kuka on käyttänyt tai kenelle luovutettu asiakasta koskevia tietoja sekä **viranomaisten tietopyyntöihin** (11 §, 63 §)
  - nimittää **tietosuojavastaava** (tietosuoja-asetus 37-39 artikla)

Palvelunantajan velvoitteita asiakastietolaista ja määräyksistä – kooste 4/4: Informoinnit ja ohjeistukset

Asiakastietolaissa mainittuja palvelunantajan velvoitteita ovat muun muassa

- huolehtia asiakastietojen käsittelyn ohjeistuksista ja menettelytavoista sekä henkilökunnan asiantuntemuksesta ja osaamisesta (7 §)
- antaa asiakkaalle tiedot asiakkaan oikeuksista ja Kanta-palveluista (informointi) (68 §)
- huolehtia asiakastietojen luovuttamista koskevan luovutusluvan ja kiellon vastaanottamisesta ja tallentamisesta (58 §)

- tietoturvasuunnitelma tukee käytännössä monien edellä kuvattujen velvoitteiden täyttämistä (77 §, 78 §)

Myös muut lainsäädännön vaatimukset huomioitava

Palvelunantajan on sosiaali- ja terveyspalvelujen järjestäjänä tai niiden tuottajana huolehdittava mm. tietosuoja-asetuksen mukaisesti henkilötietojen käsittelyssä rekisterinpitäjän (mm. palvelunjärjestäjä) ja henkilötietojen käsittelijän velvoitteista

- EU:n **tietosuoja-asetuksen** (GDPR) periaatteet
  - Käsittelyn **lainmukaisuus, kohtuullisuus ja läpinäkyvyys**
  - **Käyttötarkoitussidonnaisuus** (tietoa ei saa käyttää ilman potilaan suostumusta tai laista johtuvaa perustetta toiseen tarkoitukseen kuin mihin se on kerätty)
  - Tietojen **minimointi**: vain tarpeelliset tiedot kerätään
  - Tietojen **täsmällisyys**
  - Tietojen **säilytyksen rajoittaminen**
  - Tietojen **eheys ja luottamuksellisuus**
  - Rekisterinpitäjän **osoitusvelvollisuus**
- Tietosuojalaki 1050/2018
- Tiedonhallintalaki HE 284/2018
- Euroopan verkko- ja tietoturvadirektiivi (NIS-direktiivi)

Käytännön välineitä mm. vaikutustenarviointi, seloste käsittelytoimista ja tietotilinpäätös

Tietoturvasuunnitelman ja sen pohjalta toteutettavan omavalvonnan kautta täytettävissä ja osoitettavissa myös näiden säädösten mukaisia vaatimuksia.

Väliyhteenveto

- **Asiakastietolain uusi versio** 703/2023 astui voimaan 1.1.2024
- Asiakastietolain (myös muutosten ja lisäysten) **toimeenpano** edellyttää tarkempaa sääntelyä, johon kuuluvat **THL määräykset**
  - Uudet palvelut, (mm. sosiaalihuollon asiakastiedon arkisto, digipalvelut)
  - Muutokset olemassa oleviin velvoitteisiin (mm. toimijoiden velvoitteisiin, tietoturvasuunnitelmiin ja järjestelmiin kohdistuviin vaatimuksiin)
- Määräyksillä tuetaan uuden asiakastietolain ja kansallisten kehittämistavoitteiden toimeenpanoa, huomioiden myös mm. sote-uudistuksen vaikutukset ja kansallisten strategioiden ja ohjelmien tavoitteet
- Lähtökohtana ollut **nojautuminen aiempiin määräyksiin ja säädöksiin** (edelliset määräykset vuodelta 2021)
  - Huomioitu myös aiempien määräysten soveltamisesta esiin nousseet täsmennys- ja täydennystarpeet
- Säädöksissä on hierarkia: vastaukset moniin kysymyksiin löytyvät usein suoraan esimerkiksi lain määritelmistä

Tauko

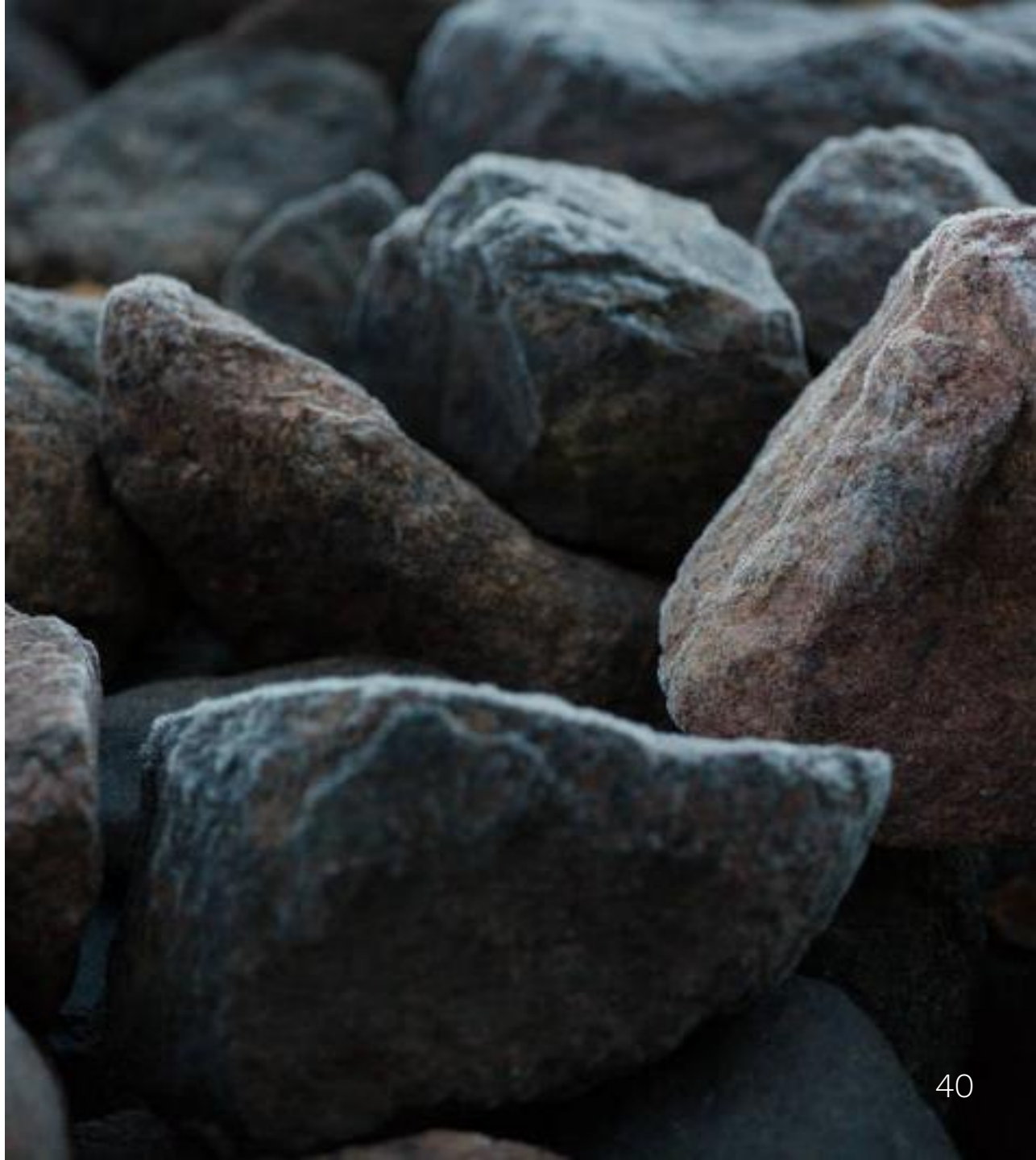
- Klo 9:45-9:55

Tietoturvasuunnitelman koulutustilaisuuden ohjelma jatkuu

Klo 9:55-10:20	Palvelunantajan, apteekin, välittäjän ja Kelan velvollisuus laatia, katselmoida ja ylläpitää THL:n määräyksen 3/2024 mukaista tietoturvasuunnitelmaa sekä seurata suunnitelman toteutumista – määräyksen 3/2024 keskeisten asioiden läpikäynti
Klo 10:20-11:05	Vinkkejä ja linkkejä suunnitelman laadintaan ja päivittämiseen määräyksen liitteen, tietoturvasuunnitelman mallipohjan avulla
Klo 11:05-11:15	Tilaisuuden yhteenveto
Klo 11:15-11:30	Kysymyksiä ja keskustelua
Klo 11:30	Tilaisuuden päätös

Palvelunantajan, apteekin, välittäjän ja Kelan velvollisuus laatia, katselmoida ja ylläpitää THL:n määräyksen 3/2024 mukaista tietoturvasuunnitelmaa sekä seurata suunnitelman toteutumista – määräyksen 3/2024 keskeisten asioiden läpikäynti

- Klo 9:55-10:20
- Antti-Olli Taipale



Tietoturvasuunnitelma – keille ja mitä? 1/2

- THL:n määräys 3/2024: ”Määräys tietoturvasuunnitelmaan sisällytettävistä selvityksistä ja vaatimuksista koskee sosiaali- ja terveydenhuollon palvelunantajia, apteekkeja, välittäjiä ja Kansaneläkelaitosta (Kela), joiden on laadittava tietoturvaan ja tietosuojaan sekä tietojärjestelmien käyttöön liittyvä tietoturvasuunnitelma”

- THL:n määräys 3/2024: ”Tietoturvasuunnitelman avulla kootaan sosiaali- ja terveydenhuollon toimijoiden tietoturvallisuuskäytäntöjä. Palvelunantajien, apteekkien, välittäjien ja Kelan laatimissa tietoturvasuunnitelmissa on oltava selvitykset siitä, miten asiakastietojen käsittelyyn ja tietojärjestelmiin liittyvät vaatimukset varmistetaan asiakastietolain 77 §:n 1 momentin kohtien 1–9 mukaisesti”

- THL:n määräys 3/2024: ”Tietoturvallisuuden omavalvonnan kohteen velvollisuutena on toimia laatimansa tietoturvasuunnitelman mukaisesti, säännöllisesti ylläpitää ja katselmoida suunnitelmaansa sekä seurata aktiivisesti sen toteutumista. Kyse on jatkuvasta ja säännöllisestä riskienhallinnasta, asianmukaisten tietoturvallisuuden ja asiakastietojen käyttöön liittyvien käytäntöjen varmistamisesta sekä niiden toteuttamisesta”.

Tietoturvasuunnitelma – keille ja mitä? 2/2

- ”Määräyksen tarkoituksena ei ole tarkasti määrätä vaatimus vaatimukselta kaikista yksityiskohtaisista tietoturvallisuuskäytännöistä”:

  ▶ Sote-organisaatioita yhden henkilön yrityksistä useiden tuhansien henkilöiden yksityisiin ja julkisiin organisaatioihin

  ▶ Oleellista on varmistua siitä, miten asiakastietojen käsittelyyn ja tietojärjestelmiin liittyvät vaatimukset käytännössä varmistetaan asiakastietolain 77 §:n 1 momentin kohtien 1–9 ja tämän THL:n määräyksen 3/2024 mukaisesti tietoturvallisuuden omavalvonnan kohteessa

  ▶ Määräyksen liitteenä on tietoturvasuunnitelman mallipohja, joka on tietoturvallisuuden omavalvonnan kohteiden tietoturvasuunnitelman laatimisen tueksi tarkoitettu esimerkinomainen dokumenttipohja

  ▶ Tietoturvasuunnitelman sisältö tulee suhteuttaa tietoturvallisuuden omavalvonnan kohteen oman toiminnan laajuuteen ja organisaation toimintaympäristössä tarvittaviin asianmukaisiin tietoturva- ja tietosuojakäytäntöihin

  ▶ Kertauksena (vrt. dia 11): tietoturvasuunnitelmaa ja siitä viitattuja liitedokumentteja tulee käsitellä ja säilyttää tietoturvallisesti. Ne tulee suojata sivullisilta, ja tarvittaessa niihin tulee merkitä salassa pidettävä -tieto. Tietoturvasuunnitelma on aina ei-julkinen asiakirja.

Tietoturvasuunnitelma – miksi?

- Parantaa ja yhdenmukaistaa sosiaali- ja terveydenhuollon tietosuoja- ja tietoturvakäytäntöjä oli sitten kyseessä ”suuri tai pieni” toimija

- Varmistaa, että henkilöstö tietää tietosuojaan ja tietoturvaan liittyvät menettelyt sekä käytännössä arkityössään noudattaa niitä asiakas- ja potilastietojen käsittelyssä

- Ottaa huomioon arkaluonteisen tiedon salassapidon ja helpottaa ymmärtämään väärinkäytöksien seuraamukset

- Ohjaa ja tukee toimimaan tietoturvallisten käytäntöjen mukaisesti niin normaaleissa kuin normaaleista poikkeavissa olosuhteissa

- Helpottaa ja tukee riskienhallintaa sote-asiakastietojen käsittelyssä erilaisissa tilanteissa ja käyttöympäristöissä

- Auttaa seuraamaan toimintaa käytännössä – tietoturvan, tietosuojan ja myös kyberturvallisuuden tilannekuva

- Auttaa varmistamaan myös muiden palveluiden tuottamiseen osallistuvien tahojen tietoturvallisen toiminnan

- Selkiyttää eri toimijoiden roolit ja **vastuut**.

Tietoturvasuunnitelma – vastuut tietoturvan sekä asiakastietojen asianmukaisen käsittelyn varmistamisessa 1/2

- THL:n määräys 3/2024: ”Tietoturvallisuuden omavalvonnan kohteen tulee varmistaa, että tietoturvasuunnitelmaan sisällytettävät **vaatimukset toteutuvat kaikissa sen omissa palveluyksiköissä ja kaikessa muiden sen lukuun palveluiden tuottamiseen tai toteuttamiseen osallistuvien palvelunantajien toiminnassa mukaan lukien mahdollisten alihankintapalveluntuottajien toiminnassa**. Tietoturvasuunnitelmassa olevista selvityksistä tulee näkyä kaikkien edellä kuvattujen yksiköiden ja alihankintapalveluntuottajien vastuut.”

- THL:n määräys 3/2024: ”**Riippumatta tietoturvallisuuden omavalvonnan kohteen organisaation koosta** sillä tulee olla käytössä asianmukaiset käytännöt arkaluonteisten **asiakastietojen suojaamiseksi digitaalisissa ja ei-digitaalisissa ympäristöissä**. Näitä tietoturvallisuuden omavalvonnan kohteen omia käytäntöjä on myös noudatettava käsiteltäessä kyseisessä organisaatiossa asiakas- tai potilastietoja.”

Tietoturvasuunnitelma – vastuut tietoturvan sekä asiakastietojen asianmukaisen käsittelyn varmistamisessa 2/2

▶ Osa kuvatuista tai vaadituista asioista voi olla jonkun muun kuin tietoturvallisuuden omavalvonnan kohteen itsensä vastuulla (sopimus- ja hankintajärjestelyt, kuten esimerkiksi palveluhankinta, sovellusvuokraus tai alihankinta)

▶ Tietoturvallisuuden omavalvonnan kohde vastaa tietoturvasuunnitelmasta myös tilanteissa, joissa se hankkii käyttöympäristön tai tietotekniikkapalveluita esimerkiksi ostopalveluina muilta palvelunantajilta tai asiakastietolain mukaisilta tai muilta tietojärjestelmäpalvelujen tuottajilta

▶ Kaikkien asiakastietojen käsittelyn osapuolien vastuut tulee olla selkeästi määritelty

▶ Vastuut on määriteltävä osapuolten välisissä toimeksianto- tai muissa sopimuksissa

▶ Sopimuksista tulee ilmetä, mihin toimiin osapuolet yhdessä tai erikseen tahoillaan ryhtyvät, jos tietoturvassa ilmenee puutteita, ongelmia tai toteutuneita riskejä

▶ Keskinäisillä sopimuksilla ei kuitenkaan voida määritellä tai sopia vastuista asiakastietolaissa säädetystä poikkeavasti.

Tietoturvasuunnitelma ”maastokartalla” suhteessa muuhun säädettyyn tai yleisiin viitekehyksiin – ”KYLLÄ” 1/2

- Palvelunantajan ja apteekin tulee käyttää tietojärjestelmiä, joiden käyttötarkoitukset vastaavat palvelunantajan ja apteekin omaa toimintaa sekä niiden on täytettävä toimintaan liittyvät olennaiset vaatimukset:

  ▶ THL:n määräys 5/2024 – sosiaali- ja terveydenhuollon tietojärjestelmien olennaiset toiminnalliset ja tietoturvavaatimukset kohdistuen asiakastietojen käsittelyyn tarkoitettuihin tietojärjestelmiin.

  ▶ Asiakastietolaki 84 § – olennaiset vaatimukset voidaan täyttää yhden tai useamman tietojärjestelmän muodostaman kokonaisuuden kautta.

- Tietoturvasuunnitelman laatimisessa suositellaan käytettäväksi tietoturvallisuuden suunnitteluun tarkoitettuja standardeja ja viitekehyksiä, esimerkiksi:

  ▶ Digi- ja väestötietoviraston julkaisema Digitaalisen turvallisuuden arkkitehtuuri -viitekehys
  ▶ ISO/IEC 27000-sarjan standardit, mm. tietoturvallisuuden hallintajärjestelmän hyödyntäminen (isot organisaatiot)
  ▶ Traficomin Kyberturvallisuuskeskuksen Kybermittarilla tehtävät itsearvioinnit (pienet organisaatiot).

Tietoturvasuunnitelma ”maastokartalla” suhteessa muuhun säädettyyn tai yleisiin viitekehyksiin – ”KYLLÄ” 2/2

- Tietoturvasuunnitelma on tietoturvallisuuden omavalvonnan kohteen dokumentti, jolla rekisterinpitäjä voi täydentää EU:n yleisen tietosuoja-asetuksen mukaista osoitusvelvollisuuttaan (5 artikla 2 kohta):

  ▶ esimerkiksi dokumentoimalla tehtyjä toimenpiteitä, laatimalla vaikutustenarviointi, tietotilinpäätös ja seloste käsittelytoimista. Osoitusvelvollisuutta voidaan toteuttaa myös muilla vastaavilla menettelyillä, joilla osoitetaan rekisterinpitäjän ja henkilötietojen käsittelijän toiminnan säädöstenmukaisuus.

- Asiakastietolain 78 §:n 4 momentin mukaan tietosuojavastaavan nimittämisestä sekä tietosuojavastaavan asemasta ja tehtävistä säädetään EU:n yleisen tietosuoja-asetuksen 37–39 artiklassa:

  ▶ tietoturvallisuuden omavalvonnan kohteella **on oltava** nimitettynä yksi tai useampi tietosuojavastaava.
  ▶ tietosuojavastaavalla **tulee olla** selkeä ja dokumentoitu tehtäväkuva, jossa otetaan huomioon asiakastietojen käsittelyyn liittyvät velvoitteet.
  ▶ tietosuojavastaavalla **tulisi olla** tehtävään soveltuva osaaminen ja resurssit hoitaa tehtävää ottaen huomioon rekisterinpitoon ja henkilötietojen käsittelyyn liittyvät vastuut ja velvoitteet, organisaation koko ja toiminnan laajuus.

Tietoturvasuunnitelma ”maastokartalla” suhteessa muuhun säädettyyn tai yleisiin viitekehyksiin – ”EI”

- THL:n määräyksessä 3/2024 **ei säädetä** siitä, millaiset häiriöt tietojärjestelmien käyttöympäristöissä ja operatiivisissa verkkoympäristöissä ovat merkittäviä tai kuinka häiriöitä koskevat ilmoitukset on tehtävä (Asiakastietolaki 90 §):

  ▶ tietoverkkoihin ja käyttöympäristöihin liittyvästä poikkeamien hallinnasta tullaan mahdollisesti säätämään sosiaali- ja terveydenhuollossa NIS 2-säädösten perusteella valmisteilla olevassa laissa kyberturvallisuuden riskienhallinnasta. NIS2-direktiivi saatetaan osaksi kansallista lainsäädäntöä 17.10.2024 mennessä ja täytäntöönpanoa koskevien säännösten soveltaminen alkaa 18.10.2024.

- THL:n määräyksen 3/2024 **kohdealueena eivät ole** sosiaali- ja terveystietojen toissijaisesta käytöstä annetun lain (552/2019, toisiolaki) mukaiset käyttötarkoitukset:

  ▶ palvelunantajan on kuitenkin mahdollista huomioida myös toisiolakiin liittyviä tiedonkäsittelyn vaatimuksia tietoturvasuunnitelmassaan; joillakin tietojärjestelmillä voi olla sekä asiakastietolain että toisiolain mukaisia käyttötarkoituksia.

- THL:n määräyksen 3/2024 **kohdealueena eivät ole** lääkinnällisten laitteiden säädökset.

Tietoturvasuunnitelma ”maastokartalla” suhteessa muuhun säädettyyn tai yleisiin viitekehyksiin – ”KYLLÄ JA EHKÄ” 1/2

- Laki julkisen hallinnon tiedonhallinnasta (906/2019, tiedonhallintalaki) on **yleislaki**, jota sovelletaan tiedonhallintaan ja tietojärjestelmien käyttöön, kun viranomaiset käsittelevät tietoaineistoja:

  ▶ **asiakastietolaki 77 § 1 momentti kohta 7**: ”tietojärjestelmiä asentaa, ylläpitää ja päivittää vain **henkilö, jolla on siihen tarvittava ammattitaito ja asiantuntemus ja jonka luotettavuus on varmistettu** julkisen hallinnon tiedonhallinnasta annetun lain (906/2019) 12 §:ssä tarkoitetulla tavalla, jos henkilö tehtävissään pääsee käsittelemään asiakastietoja tai jos hän muuten tehtävissään voi vaarantaa sosiaali- ja terveydenhuollon jatkuvuuden kannalta kriittisten tietojärjestelmien toimintaa”.

  ▶ **tiedonhallintalaki 12 § Luotettavuutta edellyttävien tehtävien tunnistaminen ja luotettavuudesta varmistuminen**: ”Tiedonhallintayksikön on tunnistettava ne tehtävät, joiden suorittaminen edellyttää sen palveluksessa olevilta tai sen lukuun toimivilta henkilöiltä erityistä luotettavuutta. Henkilöturvallisuusselvityksen laatimisen edellytyksistä säädetään **turvallisuusselvityslaissa** (726/2014). Työnantajan oikeudesta selvittää työntekijän luotettavuuden arvioimiseksi häntä koskevat luottotiedot ja käsitellä huumausainetestejä koskevia tietoja säädetään **yksityisyyden suojasta työelämässä annetussa laissa** (759/2004).

  ▶▶ asiakastietolain 77 §:ssä säädetty **tietoturvasuunnitelma velvoittaa kaikkia**, sekä julkisia että yksityisiä sosiaali- ja terveydenhuollon palvelunantajia, apteekkeja, välittäjiä sekä Kansaneläkelaitosta laatimaan tietoturvaan ja tietosuojaan sekä tietojärjestelmien käyttöön liittyvän tietoturvasuunnitelman, jolla varmistetaan yhdenmukaiset menettelyt asiakastietojen käsittelyssä.

Tietoturvasuunnitelma ”maastokartalla” suhteessa muuhun säädettyyn tai yleisiin viitekehyksiin – ”KYLLÄ JA EHKÄ” 2/2

- Laki julkisen hallinnon tiedonhallinnasta (906/2019, tiedonhallintalaki) on **yleislaki**, jota sovelletaan tiedonhallintaan ja tietojärjestelmien käyttöön, kun **viranomaiset** käsittelevät tietoaineistoja:

  ▶ **tiedonhallintalaki 13 §** - tiedonhallintayksiköiden velvollisuudet tietoturvallisuuden varmistamiseen niiden toiminnassa

  ▶ tiedonhallintalain luvuissa 2 (Tiedonhallinnan järjestäminen) ja 4 (Tietoturvallisuus) on **viranomaisia velvoittavia** ja **yksityisille toimijoille informatiivisia kohtia**, **joita tulee** tai, **joita on hyvä hyödyntää** tietoturvallisuuden omavalvonnan kohteen tietoturvasuunnitelmassa.

Yleistä tietoturvasuunnitelmasta 1/2

- THL:n määräys 3/2024, keskeisiä kohtia luvuista 5 ja 6.1:

  ▶ Tietoturvasuunnitelma on käytännön työväline, jolla hahmotetaan tietoturvallisuuden kokonaiskuvaa ja toteutetaan asiakastietojen käsittely hyvien käytäntöjen mukaisesti

  ▶ Tietoturvasuunnitelmassa kuvatut selvitykset ja käytännöt voidaan yhdistää muihin tietoturvallisuuden omavalvonnan kohteen tietosuojaa ja tietoturvallisuutta ohjaaviin menettelyohjeisiin, laatukäsikirjoihin tai tietoturvapolitiikkoihin

  ▶ Tietoturvasuunnitelman tavoitteena on varmistaa, että tietoja käyttävät ja tuottavat asiakastietojen käsittelijät ymmärtävät asiakastietojen käsittelyyn liittyvät vastuut ja osaavat kulloinkin toimia siten, että asiakastietojen eheys, luottamuksellisuus, saatavuus, kiistämättömyys ja autenttisuus toteutuvat

  ▶ Asiakastietolain 77 §:n 1 momentin kohdan 5 mukaan tietojärjestelmän käyttöympäristön on sovelluttava tietojärjestelmien asianmukaiseen ja tietoturvan sekä tietosuojan varmistavaan käyttöön.

Yleistä tietoturvasuunnitelmasta 2/2

- THL:n määräys 3/2024, keskeisiä kohtia luvuista 5 ja 6.1:

▶ Tietoturvasuunnitelmaan tulee kuvata tietoturvallisuuden omavalvonnan kohteen yleiset tietoturvakäytännöt ja/tai voimassa olevat digiturvallisuuteen liittyvät politiikat (jos on)

▶ Tietoturvasuunnitelmasta tulee löytyä tieto henkilötietojen käsittelytoimien selosteista, asiakastietojen käsittelyyn liittyvistä sopimuksista, keskeisistä tietoturvallisuusohjeista sekä tietosuojavastaavista

▶ Tietoturvasuunnitelmasta on käytävä ilmi, kuinka dokumentaatiota säännöllisesti tarkistetaan ja kehitetään sekä miten vastuut tietoturvallisuustyössä on jaettu ja organisoitu toiminnan tavoitteiden saavuttamiseksi ja riskien hallitsemiseksi

▶ Tietoturvasuunnitelmaan tai siitä viitattuihin liitteisiin tulee kuvata etä- ja hybridityöohjeistukset liittyen henkilökunnan työskentelyyn etänä (esimerkiksi kotona tai muussa etätyöpisteessä) ja erilaisissa liikkuvissa potilas- ja asiakastyötehtävissä, jos omavalvonnan kohteen toiminnassa on etänä tapahtuvaa asiakastietojen käyttöä

▶ Tietoturvasuunnitelmaan tulee kuvata erilaisissa työtehtävissä toimivan henkilökunnan tarvitsemia asiakastietosisältöjä. Esimerkiksi tietohallinnon asiantuntijoiden ja kehitys- ja hankintatoimen henkilökunnan työssään mahdollisesti käyttämät asiakastiedot tulisi vastata juuri heidän työtehtäviinsä liittyviä tarpeellisia tietoja.

Yhteenveto tietoturvasuunnitelman laatimisen peruspilareista 1/2

- Tietoturvasuunnitelma on keskeinen **käytännön työväline** palvelunantajalle ja apteekille sosiaali- ja terveydenhuollon tietosuojan ja tietoturvallisuuden suunnitteluun, toteuttamiseen ja seurantaan

- Tietoturvasuunnitelma **auttaa** muun muassa riskienhallinnassa, tietoturvallisuustyössä, tietojärjestelmien hallinnoinnissa ja varautumisessa

- Syyskuussa 2022 vastaavassa koulutuksessamme todettiin: ”Asiakastietolain toimeenpano ja määräykset luovat pohjaa esim. hyvinvointialueiden tarvitsemalle tiedonhallinnalle – tietoturva- ja tietosuojakäytäntöjen yhdenmukaistaminen ja parantaminen on keskeinen osa suunnittelua myös sote-uudistuksessa”. Väite pätee yhä tänäkin päivänä kesäkuussa 2024.

Yhteenveto tietoturvasuunnitelman laatimisen peruspilareista 2/2

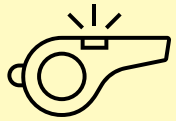
- Tietoturvasuunnitelma on sovitettava organisaation omaan toimintaan ja kokoon – otettava huomioon erityisesti tähän yhteyteen liittyvät sopimukset ja kumppanuudet

- Tietoturvan ja tietosuojan omavalvonta ja sen dokumentointi tietoturvasuunnitelmaan auttaa myös mm. EU:n yleisen tietosuoja-asetuksen mukaisen osoitusvelvollisuuden täyttämisessä

- Vastuu tietoturvasuunnitelman laatimisesta ja noudattamisesta on sote-organisaation vastaavalla johtajalla ja apteekkarilla (Asiakastietolaki 78 §).

Kiteytys – mistä tietoturva-suunnitelman omavalvonnan kohde **vastaa tietoturvan** ja **asiakastietojen asianmukaisen käsittelyn** varmistamisessa?

- **Tietoturvasuunnitelma** on laadittu
- Tietoturvasuunnitelma sisältää suunnitelmalta edellytettävät asiat THL:n määräyksen 3/2024 mukaisesti
- Tietoturvasuunnitelmassa on kuvattu, miten suunnitelmaa säännöllisesti päivitetään, katselmoidaan ja…
- … palvelunantajan henkilökunta ja kaikki ulkoiset kumppanit **käytännössä arjessa** toimivat suunnitelman mukaisesti ja…
- …miten tietoturvasuunnitelman toteutumista **seurataan**?



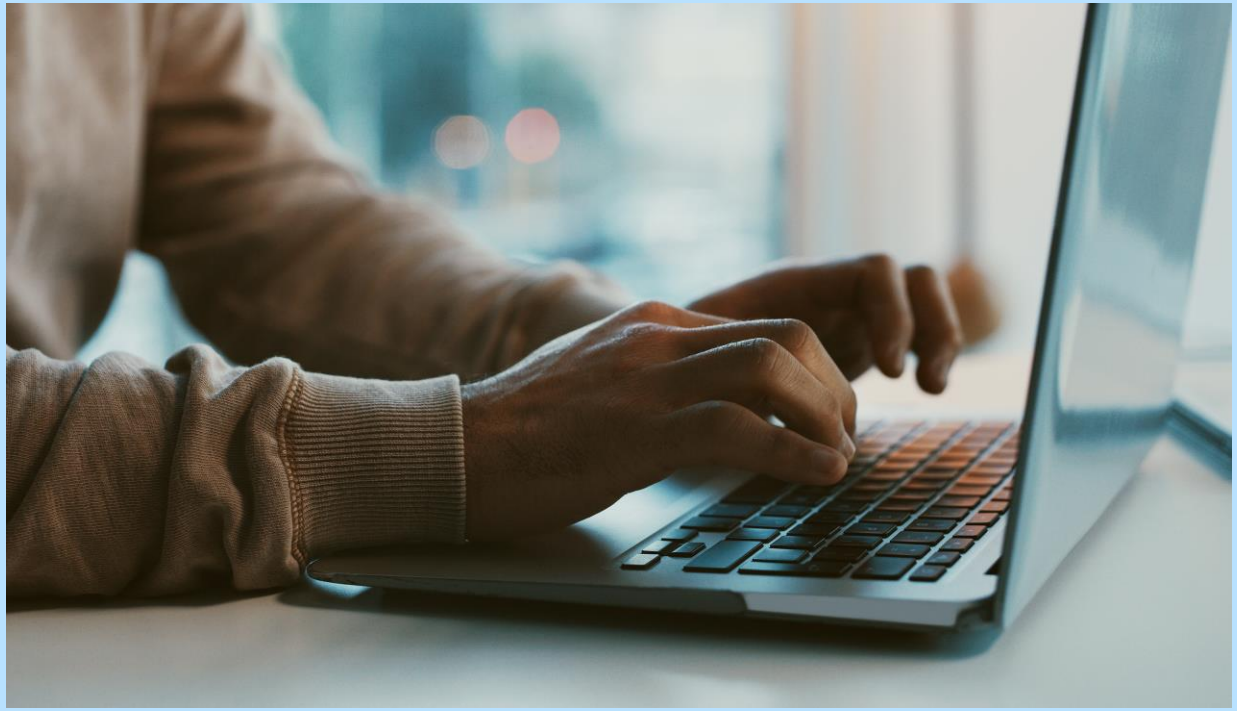
Tietoturvasuunnitelmassa kuvatut asiat **on voitava tarpeen mukaan todentaa** tietoturvallisuuden omavalvonnan toteutumisen tarkastusta tekevälle valvontaviranomaiselle.

Vinkkejä ja linkkejä suunnitelman laadintaan ja päivittämiseen määräyksen liitteen, tietoturvasuunnitelman mallipohjan avulla

- Klo 10:20-11:05
- Tuula Wester

Tietoturvasuunnitelman mallipohja

- Määräyksen 3 liite ”Tietoturvasuunnitelman mallipohja”:
  - On esimerkinomainen dokumenttipohja
  - Helpottaa ja ohjaa suunnitelman laatimista
  - Mallipohjaa voi soveltaa tai täydentää omaan toimintaan peilaten ottaen huomioon oman toiminnan laajuus ja tarvittavat tietoturva- ja tietosuojakäytännöt



Toiminnan jatkuvuus poikkeustilanteissa

- Tunnistetaan poikkeustilanteet
- Toiminta normaalista poikkeavissa tilanteissa
  - Varautuminen erilaisiin poikkeustilanteisiin
  - Arvioidaan eri järjestelmien, sovellusten ja osajärjestelmien riskit
  - Määritellään toimintatavat- ja ohjeet ja vastuut riskiarvioinnit huomioiden
  - Seurataan jatkuvasti tietoturvallisuuden tilaa (Tiedonhallintalaki 13 a §)
- Määräys 3 luku 6.2 ja mallipohja luku 4

Koulutuksella osaaminen kuntoon

- Koulutussuunnitelmaan kuvataan (tai mahdollinen linkki ko. dokumenttiin):
  - Henkilöstön koulutuksen ja osaamisen käytännön toteutus:
    - perehdytys
    - koulutus
    - ylläpito
    - seuranta
    - ja ajantasaisuuden varmistaminen
- Määräys 3 luku 6.3. ja mallipohja luku 5

Ajantasaiset käyttöohjeet saataville

- Huomioitava ohjeistuksessa niiden:
  - Ajantasaisuus
  - Tarvittava kielisyys ja saatavuus
  - Ymmärrettävyys
  - Yksiselitteisyys
  - Sijainti kaikkien tiedossa
  - Erilaiset työtehtävät ja -roolit

- Ohjeet ohjaavat asiakastietoja käsittelyä:
  - Tietojärjestelmien käyttöä
  - Tietoaineistojen käsittelyä
  - Tietojenkäsittelyoikeuksia
  - Tiedonsaantioikeuksien toteuttamista
  - Tiedonhallinnan vastuiden toteuttamista
  - Tietoturvallisuustoimenpiteitä sekä
  - Poikkeusoloihin varautumista

Määräys 3 luku 6.4 ja mallipohja luku 5.2

Järjestelmien perustiedot ja olennaisten vaatimusten täyttyminen

- Perustiedot kaikista käytössä olevista sertifioiduista ja sertifioimattomista, luokitelluista ja luokittelemattomista tietojärjestelmistä ja digipalveluista
- Järjestelmien ja digipalveluiden käyttötarkoitus ja käyttäjäryhmät
- Olennaisten vaatimusten varmistaminen ja menettelyt hankinnoissa, sopimuksissa, kehittämisessä ja ylläpidossa
- Muut tietojärjestelmät ja sovellukset, joissa ei käsitellä asiakastietoja voi myös sisällyttää tietoturvasuunnitelmaan.
- Määräys 3 luku 6.5. ja mallipohja luku 6

Tietojärjestelmien asennus, ylläpito ja päivitys

- Henkilökunnan roolit ja vastuut (oman organisaation vastuu, tietojärjestelmätoimittajan vastuu, kolmannen osapuolen vastuu…jne.)
- Tarvittava ammattitaito ja asiantuntemus
- Henkilön luotettavuuden varmistaminen (asiakastietolaki 77 § 1 mom. 7 kohta)
- Testaus- ja hyväksymismenettelyt asennus-, ylläpito- ja päivitystehtävissä
- Toimintatavat, kun tehdään suunniteltuja tai kiireellisiä versio- ja korjauspäivityksiä
- Tietojärjestelmien suojaus tietoturvapuutteilta ja haavoittuvuuksilta
- Komponenttien huolto-, uusimis-, ylläpito- ja päivitysmenettelyt
- Määräys 3 luku 6.6. ja mallipohja luku 6.2.

Käyttövaltuuksien hallinta ja tunnistautuminen

Kuva 1. Käytönhallinnan osa-alueet

- Kuvataan, kuinka määrittely ja hallinnointi tapahtuu:
    - tietojärjestelmien käyttäjät ja erilaiset käyttäjäryhmät, käyttäjäroolit ja rooleihin liittyvät käyttövaltuudet (myös sijaiset ja opiskelijat)
    - henkilöt tai roolit, joilla on oikeus käsitellä, hylätä ja hyväksyä käyttöoikeuspyyntöjä
    - käyttövaltuuksien hakemisen, myöntämisen, seurannan, tarkistamisen tai varmistamisen ja poistamisen käytännöt ja toimintamallit
    - milloin ja millä tavalla poistuneiden työntekijöiden käyttöoikeudet poistetaan

- Määräys 3 luku 6.7. ja mallipohja luku 6.3.

Pääsynvalvonta ja käytön seuranta

Kuva 1. Käytönhallinnan osa-alueet

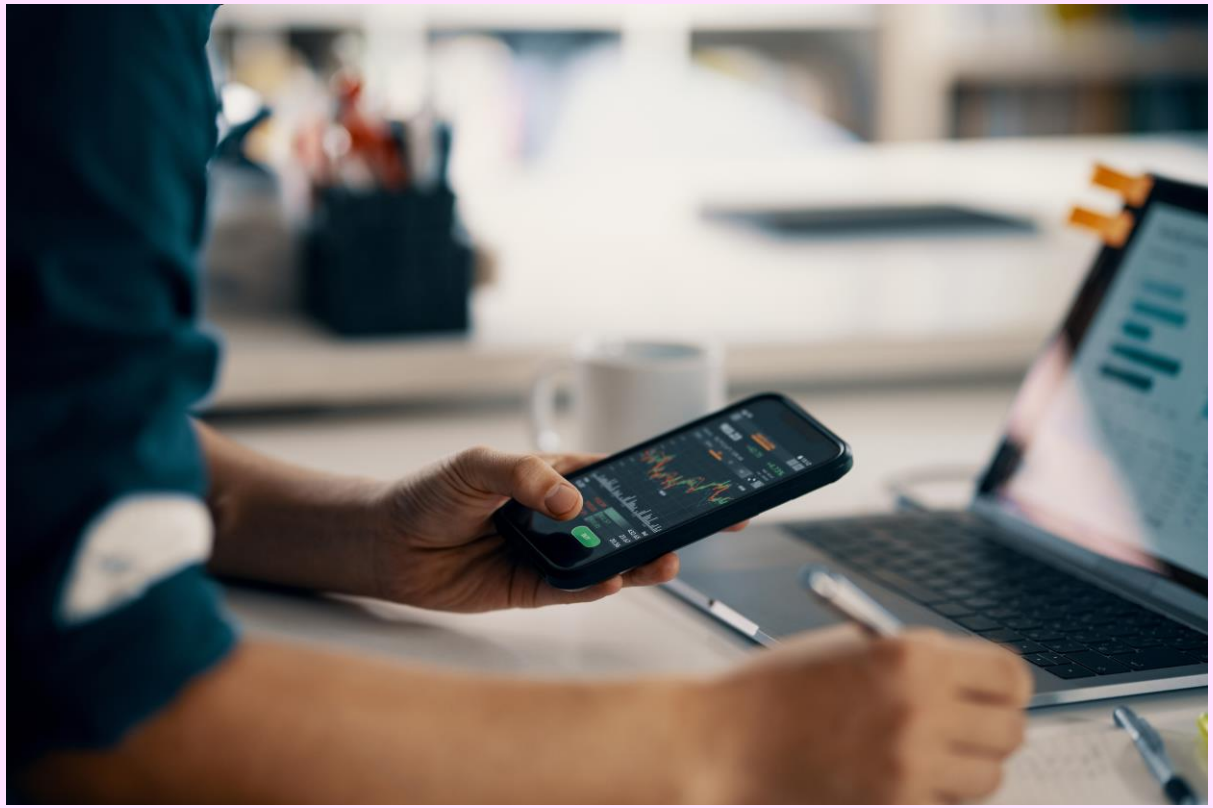
- On oltava seuranta- ja valvontasuunnitelma, jossa kuvataan, miten seurataan rekisterikohtaisesti henkilötietojen ja tietojärjestelmien käyttöä ja luovutuksia.
- Valvontasuunnitelmassa kuvataan miten seuranta toteutetaan, kuinka usein ja miten toimitaan, kun huomataan väärinkäytöksiä tai virhetilanteita.
- Lokitiedoilla seurataan tietojen käyttöä ja luovutuksia ja tietojärjestelmän teknisiä virheitä.
- Lokitietojen kerääminen ja seuranta koskee kaikkia sosiaali- ja terveydenhuollon palvelunantajia, myös yksityisiä ja apteekkeja
- Lokien pitää pysyä muuttumattomina ja todistusvoimaisina
- Määräys 3 luku 6.8. ja mallipohja luku 6.4.

Fyysinen turvallisuus

- Kuvataan toimenpiteet, joilla voidaan käytännössä vaikuttaa erilaisten toimitilojen tietosuojaan ja tietoturvaan, esim.
  - tilaratkaisut, sisustus, äänieristys, kulunvalvonta, paloturvallisuus
  - näyttöjen, työasemien ja tulostinten sijoittelu
  - Paperitulosteiden hävittämiskäytännöt (turvatulostaminen suositeltavaa)
  - Ulkoisten kovalevyjen ja muistitikkujen suojauskäytännöt
  - Palvelinten käyttöympäristön turvallisuus
  - Määräys 3 luku 6.9. ja mallipohja luku 7.1., 7.2. ja 7.3.

Laitteiden ja käyttö-ympäristön hallinta

- Kuvataan:
  - miten virus- ja haittaohjelmilta suojaaminen ja päivitykset on käytännössä varmistettu työasemilla
  - miten mobiililaitteiden (tabletit ja älypuhelimet, kannettavat työasemat) suojauskäytännöt on järjestetty
  - käytössä olleiden laitteiden tietojen poistaminen työsuhteiden päättymisten jälkeen
  - Käyttöympäristön tukipalvelut
  - Käyttöympäristön kokonaisuus, josta selviää vastuun- ja työnjako oman toiminnan ja mahdollisen sopimuskumppanin tai alihankintapalvelun osalta (toimijoiden väliset sopimukset)
  - Määräys 3 luku 6.10 ja mallipohja luku 7.2.

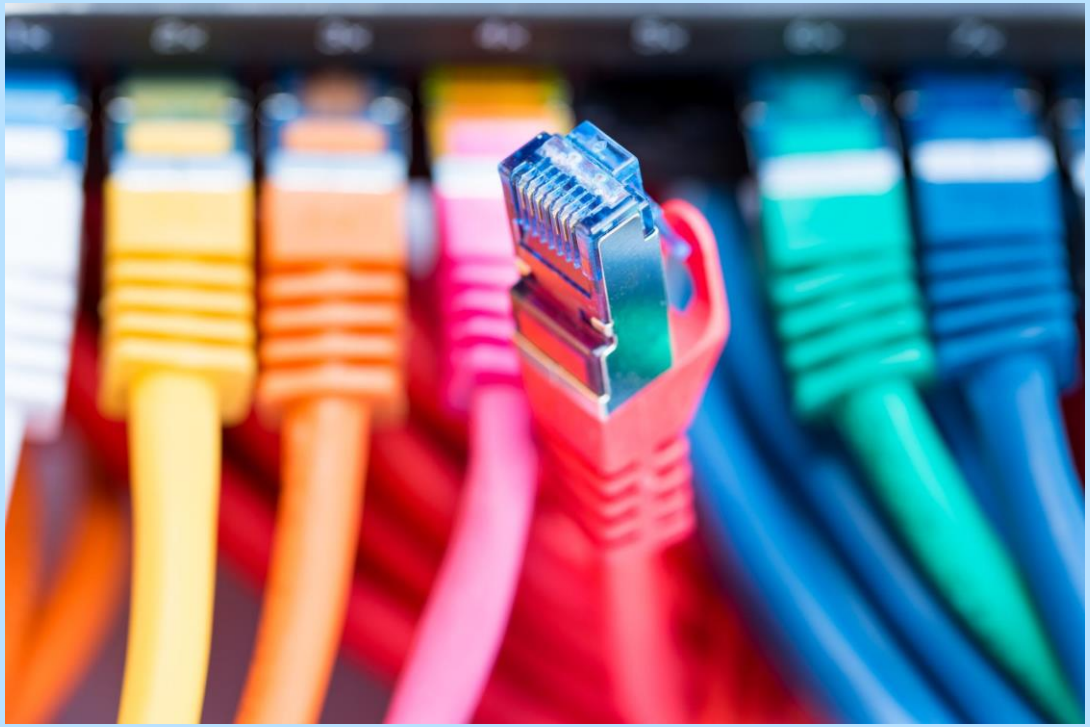


Alusta- ja verkkopalvelut ja niiden vastuut

- Luetteloidaan ja kuvataan käytössä olevat alusta-, verkko- ja pilvipalvelut
- Nimetään vastuutahot: palvelunantaja, tuottaja/valmistaja, alihankkijat, tietoliikenneoperaattorit
- Mahdolliset viittaukset sopimuksiin ja tietoturvakäytänteisiin
- Varautuminen poikkeustilanteisiin ilman tietojärjestelmiä
- Palvelimet ja palvelinympäristöt
- Tietoverkkojen hallinta, verkkolaitteet, langattomat verkot ja reitittimet
- Etäyhteydet ja niiden tietoturva
- Pilvipalveluiden käyttö
- Määräys 3 luku 6.11. ja mallipohja luku 7.3.

Kanta-palvelujen liittymisen ja käytön tietoturvakäytännöt

- Käyttäjien koulutus ja perehdytys Kanta-palveluiden käyttöön
- Asiakkaiden informoinnin toteuttamiskäytännöt
- Kirjautumiskäytännöt ja varmenneratkaisujen toteuttaminen
- Toimintamallit käytön seurannasta ja muutostilanteista
- Palvelunantajan ja apteekin vastuutahot häiriötilanteissa
- Tietoturvallisuustodistuksen voimassaolo
- Tiedot Valviran tietojärjestelmärekisterissä
- Järjestelmään toteutetut olennaisten vaatimusten profiilit
- Yhteistestauksen suorittaminen
- Määräys 3 luku 6.12. ja mallipohja luku 8



Miten saadaan henkilöstö noudattamaan hyvää tietoturvaa?

Laaditaan ymmärrettävä tietoturvasuunnitelma, jossa:

- ✓Suunnitellaan henkilöstön perehdytys ja koulutus

Lisäksi:

- ✓Perustellaan asiat
- ✓Toistetaan koulutus riittävän usein
- ✓Mietitään viestinnän rooli
- ✓Seurataan säännöllisesti: miten on mennyt

Tavoitteena: motivaatio, käytäntöjen juurruttaminen, toimintamallit ja tavat tutuiksi

Tietoturvasuunnitelmaan laatimiseen liittyviä kysymyksiä 1/2

- Pitääkö tietoturvasuunnitelma laatia, jos käytössä ei ole yhtään tietojärjestelmää?
  - Suunnitelma on tehtävä, vaikka käytössä ei olisi yhtään tietojärjestelmää. Tällöin kuvataan manuaalinen toiminta ja siihen liittyvät käytännöt
- Yrityksessä A toimii joukko itsenäisiä ammatinharjoittajia. Pitääkö jokaisen laatia oma tietoturvasuunnitelma?
  - Jokainen itsenäinen ammatinharjoittaja on myös palvelunantaja. Jokaisella **palvelunantajalla** tulee olla tietoturvasuunnitelma, jonka piirissä toimii.
  - Suunnitelmasta tulee **näkyä kaikki toimijat**, joita suunnitelma koskee.
  - Yritys A voi esimerkiksi laatia ns. **kokoavan** tietoturvasuunnitelman, jossa on kaikille palvelunantajille yhteisiä osioita ja jossa voidaan viitata jokaisen palvelunantajan omaan tietoturvaosuuteen.
  - Jokaisen kokoavan tietoturvasuunnitelman piirissä olevan palvelunantajan tulee olla tietoinen sen sisällöstä ja sitoutunut noudattamaan:
    - sekä omaa tietoturvaosiotaan että
    - yhteistä osiota

Tietoturvasuunnitelmaan laatimiseen liittyviä kysymyksiä 2/2

- Pitääkö tietoturvasuunnitelma laatia jos kyseessä on ”yleisjärjestelmä” tai luokittelematon järjestelmä?
  - Tietoturvasuunnitelma on toimija- eikä järjestelmäkohtainen – mukaan ainakin kaikki palvelunantajan käyttämät järjestelmät, joissa käsitellään asiakastietoa
  - Jos järjestelmä sisältää ominaisuuksia sote-asiakastietojen käsittelyä varten, se on oltava mukana tietoturvasuunnitelmassa
    - Asiakastietolain **tietojärjestelmä**-määritelmä:
      - ”Ohjelmistoa, järjestelmä tai osajärjestelmä, jota valmistajan suunnittelemien ominaisuuksien mukaisesti on tarkoitettu käytettäväksi **asiakasasiakirjojen** sähköiseen käsittelyyn, asiakirjojen tallentamiseen valtakunnallisiin tietojärjestelmäpalveluihin tai valtakunnallisiin tietojärjestelmäpalveluihin liittämiseen tai jolla sosiaali- ja terveydenhuollon ammattihenkilö voi hyödyntää **hyvinvointitietoja**.”

Tilaisuuden yhteenveto

- Klo 11:05-11:15

Kysymyksiä ja keskustelua

- Klo 11:15-11:30

Tilaisuus on päättynyt – kiitos!

Kiitos