


Tietoturvasuunnitelman koulutustilaisuus sote-palvelunantajille

15.9.2022 - Teams

Juha Mykkänen ja Antti-Olli Taipale

THL, Tiedonvälittäjät -osasto, Tieto ja tiedonhallinnan ohjaus -yksikkö

Tietoturvasuunnitelman koulutustilaisuuden ohjelma 15.9.2022

Klo 9:00-9:05	**Tilaisuuden avaus, tavoitteet ja kulku**
Klo 9:05-9:25	**Yleiskuva voimassa olevasta asiakastietolaista ja THL:n määräyksistä**
Klo 9:25-9:45	**Palvelunantajan velvollisuudet asiakastietolaista, määräyksistä ja suhde muihin säädöksiin**
Klo 9:45-10:05	**Yleiskuva tietoturvasuunnitelmasta ja sen suhteesta tietojärjestelmien olennaisiin vaatimuksiin**
Klo 10:05-10:15	**Tauko**
Klo 10:15-11:15	Tietoturvasuunnitelman laatiminen: läpikäynti uuden mallipohjan kautta sekä koulutustilaisuuden yhteenveto
Klo 11:15-11:30	Kysymyksiä ja keskustelua
Klo 11.30	Tilaisuuden päätös

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

Tilaisuuden tavoitteet ja kulku

- Antaa yleiskuva voimassa olevasta asiakastietolaista ja THL:n määräyksistä 2021
- 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 lisämateriaaleineen (31.3.2022 pidetyssä tietoturvasuunnitelman koulutustilaisuudessa esille nousseet kysymykset) julkaistaan Tiedonhallinta sosiaali- ja terveysalalla kokonaisuuden Koulutusmateriaalit –sivulla

- Tilaisuus nauhoitetaan. Nauhoituksesta mainitaan ennen sen aloittamista sekä sen loputtua. Lisäksi nauhoituksen aikana Teams näyttää käyttöliittymässään tiedon nauhoituksesta.

Yleiskuva voimassa olevasta asiakastietolaista ja THL:n määräyksistä

Uusia ja vanhoja riskejä ja uhkia…

POTILASTIETOJÄRJESTELMÄT

Potilastietojärjestelmien päivitys ongelmissa Kanta-Hämeessä: ajanvaraustekstiviestit eivät kulje ja terveysasemille vain kiireellisissä tapauksissa

Potilastietojen kirjaamisen hidastuminen vaikuttaa … Hämeenlinnan ja Riihimäen alueella.

TIETOTURVA

Venäläisyhtiö saa ihmisten sijaintitiedot ja paljon muuta

YLE 2.3.2022

Nordeaan kohdistunut kyberhyökkäys oli "poikkeuksellisen hyvin toteutettu", sanoo asiantuntija – hyökkääjän taustoista ei tietoa

TIETOSUOJARIKOS

Yksi klikkaus maksoi sosiaalialan työntekijöille 4800 euroa – tutkivat vieraan perheenäidin tietoja, kun tämä

Ovatko henkilökoh… terveystied… turvassa? - Yhdysvalloiss… miljoonaa tietorikkom…

DIGITODAY

Vakuutusyhtiöille kerättiin väärin potilastietoja: ”Järjestelm… pitkäkestoista”

Liikennevakuutuskeskus käsitteli potilastietoja … tietosuojavaltuutettu päätti. Myös yhdelle mat… sakko.

JAA KOMMENTIT

Nato-johtaja vertasi Huawein verkkolaitteita Venäjän kaasuputkeen – Elisa: Huaweilla on innovatiivista voimaa

27.5.2022 09:18 | päivitetty 27.5.2022 09:32 MAANPUOLUSTUS TIETOTURVA

Rovaniemi tänään 10.12

It-vika pysäytti Lapin keskussairaalan

Lapin keskuss… poliklinikkakäy… tietojärjestelmä…

Vika havaittiin tiist… potilastietojärjeste… …ttömiä leikkauksia ja …ikkona sairaala

UUTISET | KOTIMAA

Vastaamon tietomurto: kolmea …päillään törkeistä rikoksista

…kintaan syyskuun aikan…

TIETOTURVA

Kyberhyökkäys kaatoi Irlannin terveydenhuollon – tietokoneet pimeinä sairaalassa

Vain kor…

TIETOTURVA

Onko kiinalainen puhelin vaarallinen? Näin kommentoivat viranomainen ja tietoturva-asiantuntija

Liettualaisten löydökset herättivät pelkoa kiinalaispuhelimiin. Asiantuntijoiden mukaan kyse ei ole yhteen maahan liittyvästä ongelmasta. Kuluttajan asema on kuitenkin vaikea.

TIETOSUOJA

Tyhjistä sairaalatiloista löytyi taas salaiseksi tarkoitettuja tietoja – TAYS: "Jossakin prosessi oli katkennut"

Lukituista tiloista löytynyt tietosuojattava materiaali on tuhottu ja tietoturvaloukkauksista on tehty ilmoitukset tietosuojavaltuutetun toimistoon.

TIETOTURVA

Karmea saldo yhdelle päivälle: Kiristäjät iskivät 6 sairaalaan

Verkkokiristyksen iljettävä muoto on yleistynyt Yhdysvalloissa ja vaarantaa ihmishenkiä.

…rosoftilta varoitus Azure-käyttäjil… pilvikontissa oli vuoto

9.9.2021 13:08 | päivitetty 9.9.2021 13:08

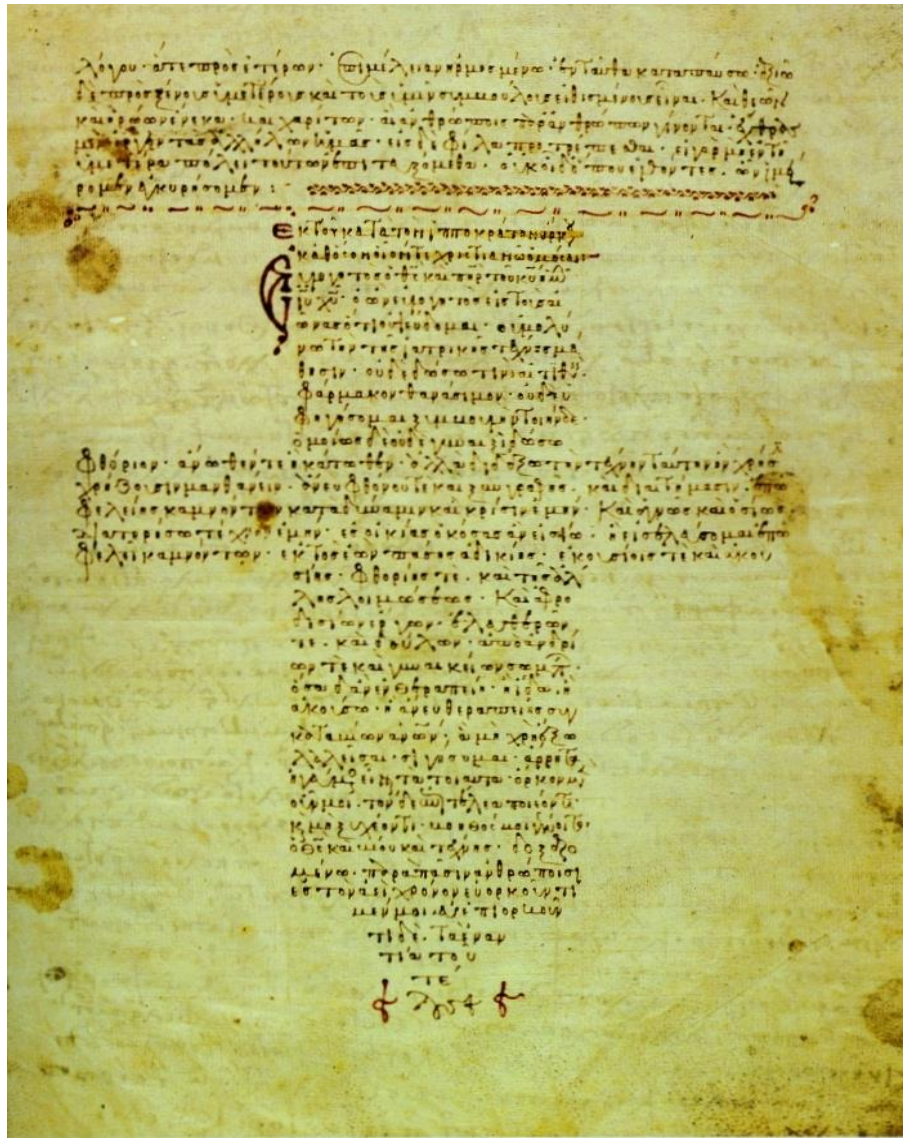
Azuren konttipalvelun aukko on onneksi jo kor…

…mutta perusasiat pysyvät.

Hippokrateen vala, ote:

”Mikäli parannustyössäni tai sen ulkopuolella ihmisten keskuudessa näen tai kuulen sellaista, mitä ei pidä levitettämän, vaikenen ja pidän sen salaisuutena.”

- Hippokrates (n. 460-370 eKr)



Esimerkki: Kanta-volyymit

Kanta-palveluita käyttävät:

- kaikki julkisen terveydenhuollon organisaatiot
- noin 1 700 yksityisen terveydenhuollon organisaatiota
- kaikki apteekit
- kasvava joukko sosiaalihuollon organisaatioita

2,7 mrd
asiakirjaa potilastiedon arkistossa

6,4 milj
henkilöä joiden terveystietoa arkistoitu

27,1 milj
sähköistä lääkemääräystä vuonna 2021

18,5 milj
asiakirjaa sosiaalihuollon asiakastiedon arkistossa

71,5 milj
lääketoimitusta vuonna 2021

thl

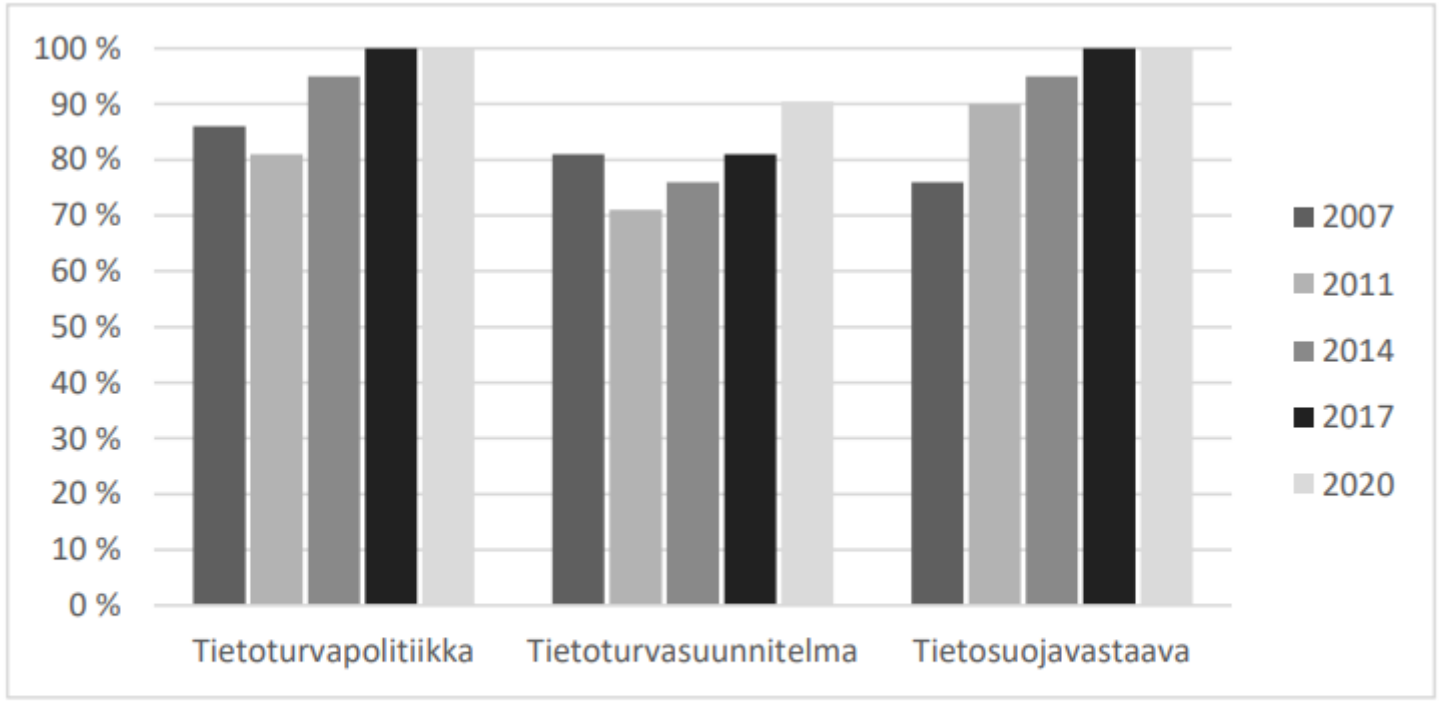
Tietoturvallisuuden perusperiaatteet

- 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 5/2021 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

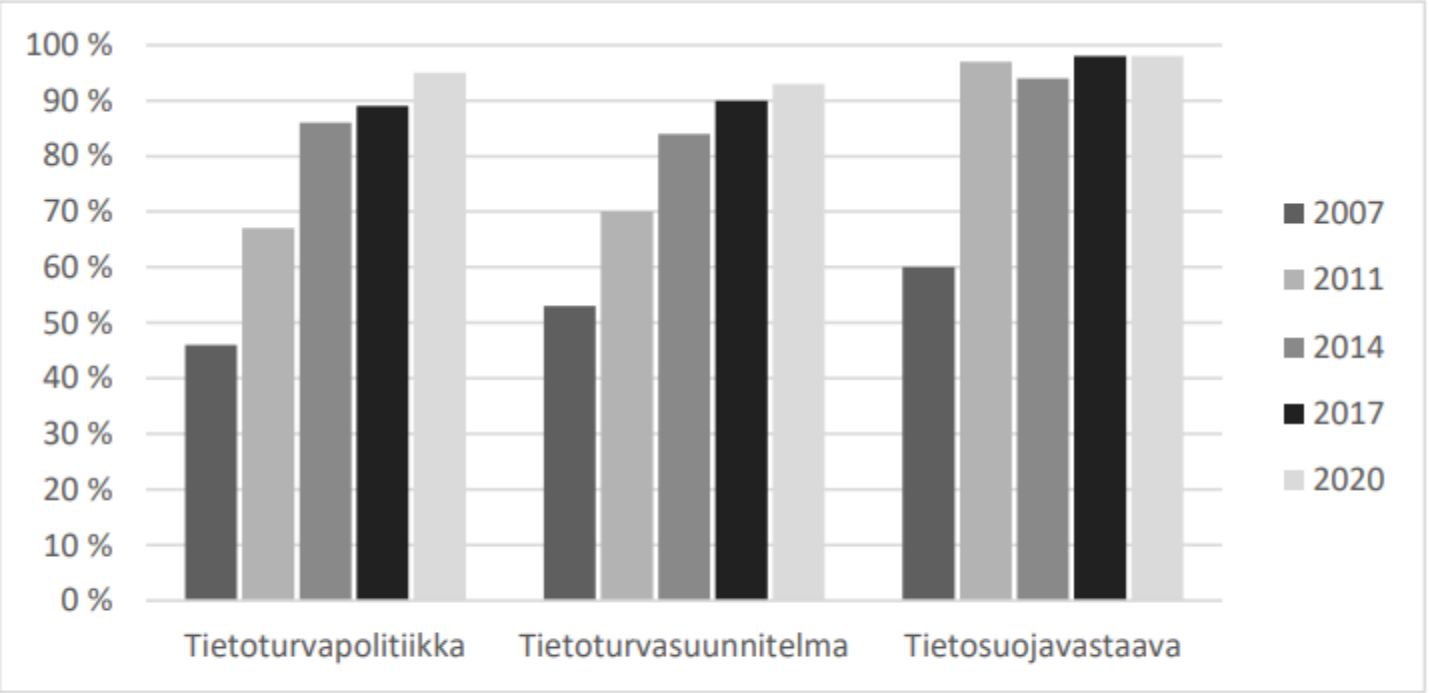
Tietoturvan järjestelyt sairaanhoitopiireissä



Kuvio 9. Tietoturvan järjestelyt sairaanhoitopiireissä vuosina 2007–2020, osuus sairaanhoitopiireistä (%), jotka ilmoittivat kyseisen toiminnallisuuden.

- Jarmo Reponen, Niina Keränen, Ronja Ruotanen, Timo Tuovinen, Jari Haverinen, Maarit Kangas: Tieto- ja viestintäteknologian käyttö terveydenhuollossa vuonna 2020 - Tilanne ja kehityksen suunta –THL Raportti 11/2021

Tietoturvan järjestelyt terveyskeskuksissa



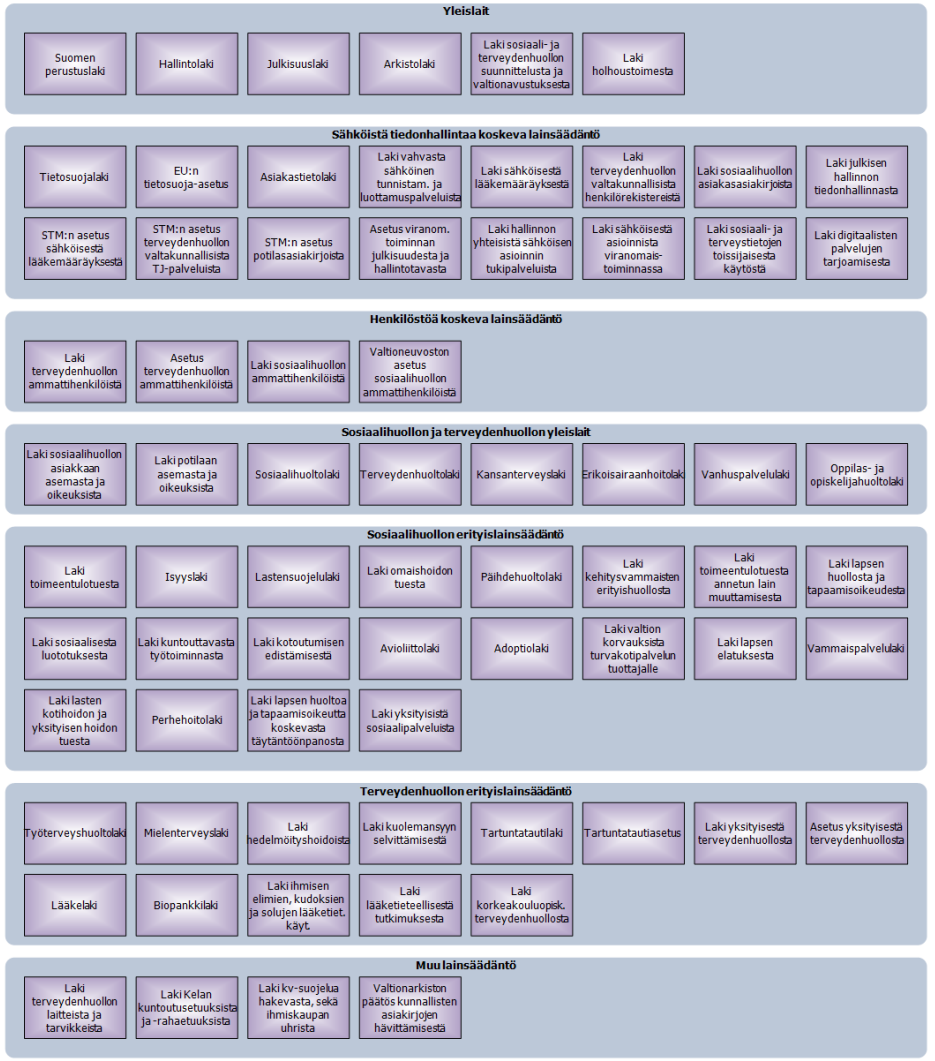
Kuvio 10. Tietoturvan järjestelyt terveyskeskuksissa vuosina 2007–2020, osuus terveyskeskuksista (%), jotka ilmoittivat kyseisen toiminnallisuuden.

- Jarmo Reponen, Niina Keränen, Ronja Ruotanen, Timo Tuovinen, Jari Haverinen, Maarit Kangas: Tieto- ja viestintäteknologian käyttö terveydenhuollossa vuonna 2020 - Tilanne ja kehityksen suunta –THL Raportti 11/2021

Sote-tiedonhallinnan sääntely-ympäristö

- Yleislait ja julkista hallintoa koskevat säädökset
- Tietosuojasäädökset, mm. GDPR
  - Henkilötietojen suojaaminen
- Sosiaali- ja terveydenhuollon yleis- ja erityislainsäädäntö
- Lääkinnällisten laitteiden säädökset, mm. MDR, laki terveydenhuollon laitteista ja tarvikkeista
  - Kansainvälinen pohja, laadunvarmistus, potilasturvallisuus, terveysteknologia ja laitteet, soveltamista myös ohjelmistoihin
- **Sote-tiedonhallinnan säädökset, mm. asiakastietolaki ja toisiolaki**
  - **Asiakastietolain painopisteitä mm. kansallisten tietojärjestelmäpalvelujen hyödyntäminen, yhteentoimivuus, asiakastietojen tietosuoja, tietoturvallisuus <u>Suomen sote-palveluissa ja niihin tehtävissä tietojärjestelmäratkaisuissa</u>**

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



Sosiaali- ja terveydenhuollon asiakas- ja potilastietojen kansallinen kokonaisarkkitehtuuri 2.1

Tietoturvan ja tietosuojan omavalvonnan ja olennaisten vaatimusten säädökset

- Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä 784/2021 (Asiakastietolaki, AsTL)
- Laki sähköisestä lääkemääräyksestä 61/2007 – päivitykset: 251/2014 ja 786/2021

- **Määräys 3/2021 tietoturvasuunnitelmaan sisällytettävistä selvityksistä ja vaatimuksista**
- **Määräys 4/2021 sosiaali- ja terveydenhuollon tietojärjestelmien luokittelusta ja sertifioinnista**
- **Määräys 5/2021 sosiaali- ja terveydenhuollon tietojärjestelmien olennaisista toiminnallisista ja tietoturvavaatimuksista**
- Määräys 6/2021 omatietovarantoon liitettävien hyvinvointitietoja käsittelevien hyvinvointisovellusten olennaisista vaatimuksista ja sertifioinnista
- Lisäksi saatavilla ohjeita ja tukimateriaalia

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

Keskeisiä asiakastietolain 784/2021 kohtia tietoturvasuunnitelman näkökulmasta 1/2

- 2 § Soveltamisala ja suhde muuhun lainsäädäntöön
- **3 § Määritelmät**
- **27 § Tietoturvasuunnitelma**
- **28 § Tietoturvallisuuden omavalvonnan toteuttaminen ja vastuu**
- 29 § Tietojärjestelmien ja hyvinvointisovellusten käyttötarkoitus ja luokittelu

Keskeisiä asiakastietolain 784/2021 kohtia tietoturvasuunnitelman näkökulmasta 2/2

- 31 § Tietojärjestelmän ja hyvinvointisovelluksen ottaminen tuotantokäyttöön
- 34 § Tietojärjestelmälle ja hyvinvointisovellukselle asetettavat olennaiset vaatimukset
- 41 § Ilmoittaminen tietojärjestelmän olennaisten vaatimusten poikkeamista
- 52 § Siirtymäsäännökset

Määritelmät: asiakastiedot (AsTL 3 §)

(tarkoitetaan…):

3) **sosiaalihuollon asiakastiedolla** asiakasta koskevaa henkilötietoa, joka sisältyy asiakaslaissa ja asiakasasiakirjalaissa tarkoitettuun asiakirjaan;
4) **potilastiedolla** potilasta koskevaa henkilötietoa, joka sisältyy potilaslaissa tarkoitettuun potilasasiakirjaan;
5) **asiakastiedolla** 3 ja 4 kohdassa tarkoitettua sosiaalihuollon asiakastietoa ja potilastietoa

Määritelmät: tietojärjestelmä (AsTL 3 §)

- **tietojärjestelmällä** (tarkoitetaan) tietojenkäsittelylaitteista, ohjelmistoista ja muusta tietojenkäsittelystä koostuvaa kokonaisjärjestelyä, jota valmistajan suunnittelemien ominaisuuksien mukaisesti on **tarkoitettu käytettäväksi asiakastietojen sähköiseen käsittelyyn, asiakasasiakirjojen tallentamiseen ja ylläpitoon tai valtakunnallisiin tietojärjestelmäpalveluihin liittämiseen** tai jolla sosiaali- ja terveydenhuollon ammattihenkilö voi hyödyntää hyvinvointitietoja

Määritelmät: palvelunantaja (AsTL 3 §, Määräys 3/2021 luku 3)

Palvelunantajalla tarkoitetaan sosiaali- ja terveyspalvelujen **järjestäjää** ja sosiaali- ja terveyspalvelun**tuottajaa**:

- **terveydenhuollon toimintayksikköä** (potilaslaki 785/1992 2 §:n 1 mom. 4 kohta)
- sosiaalihuollon asiakasasiakirjalain 254/2015 3 §:n 1. mom. 3 kohdan mukaan **sosiaalihuoltoa tai sosiaalipalveluja järjestävää, tuottavaa tai toteuttavaa viranomaista** taikka yksityisistä sosiaalipalveluista annetussa laissa (922/2011) tarkoitettua **palvelujen tuottajaa**
- **työnantajaa** (työterveyshuoltolaki 1383/2001 7 § 2 mom.)
- **itsenäisenä ammatinharjoittajana toimivaa** terveydenhuollon ammattihenkilöä (laki yksityisestä terveydenhuollosta 152/1990 2 § 3 mom.)
- asiakastietolain mukaisen määritelmän lisäksi [määräyksessä 3/2021] palvelunantajaan kohdistuvat velvoitteet koskevat vastaavalla tavalla ja lain sähköisestä lääkemääräyksestä (61/2007, mukaan lukien lain 786/2021 mukaiset muutokset) mukaisessa laajuudessa myös lääkelain (395/1987) 38 §:n mukaista **apteekkia**

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

17) **tietojärjestelmäpalvelun tuottajalla** tahoa, joka tarjoaa tai toteuttaa palvelunantajalle tietojärjestelmää, jossa käsitellään asiakas- tai hyvinvointitietoa, ja joka vastaa tietojärjestelmän valmistajana, valmistajan lukuun tai yhden tai useamman valmistajan puolesta tietojärjestelmälle asetetuista vaatimuksista;

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

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

- 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.

Sote-tiedonhallinnan määräykset 2021 ja 2022

THL:n tiedonhallinnan sivustolla ja viranomaisten säädöskokoelmassa

THL valmisteli vuonna 2021 kuusi määräystä sosiaali- ja terveydenhuollon tiedonhallinnan kokonaisuudesta. Määräyksillä ohjataan **asiakastietolain** 784/2021 täytäntöönpanoa.

- Lausuntoajat päättyivät lokakuun 2021 loppuun mennessä, minkä jälkeen määräykset 1-5 liitteineen saatiin viimeisteltyä ja julkaistua marras- ja joulukuun 2021 aikana. Määräys 6 julkaistiin 16.2.2022.

1. Määräys 1/2021 sosiaalihuollon asiakasasiakirjojen rakenteista ja asiakasasiakirjoihin merkittävistä tiedoista
2. Määräys 2/2021 valtakunnallisten tietojärjestelmäpalveluiden avulla terveydenhuollon ulkopuolelle välitettävistä asiakirjoista
3. **Määräys 3/2021 tietoturvasuunnitelmaan sisällytettävistä selvityksistä ja vaatimuksista**
4. Määräys 4/2021 sosiaali- ja terveydenhuollon tietojärjestelmien luokittelusta ja sertifioinnista
5. Määräys 5/2021 sosiaali- ja terveydenhuollon tietojärjestelmien olennaisista toiminnallisista ja tietoturvavaatimuksista
6. Määräys 6/2021 omatietovarantoon liitettävien hyvinvointitietoja käsittelevien hyvinvointisovellusten olennaisista vaatimuksista ja sertifioinnista (julkaistu 02/2022)

- Voimaan tullut myös (30.3.2022): Määräys 1/2022 tietoturvallisuustodistuksen myöntämiseen liittyvistä menettelyistä sertifiointien loppuun saattamiseksi.

Miksi määräykset uudistuivat?

- **Asiakastietolain** (muutosten ja lisäysten) **toimeenpano** edellyttää tarkempaa sääntelyä
  - Uudet palvelut, (mm. sosiaalihuollon asiakastiedon arkisto, omatietovaranto ja hyvinvointisovellukset)
  - Muutokset olemassa oleviin velvoitteisiin (mm. olennaisten vaatimusten kohdistuminen myös palvelunantajiin, muutokset tietoturvasuunnitelmiin ja järjestelmiin kohdistuviin vaatimuksiin)

- Useiden THL:n määräysten (**2-5**) **pohjana aiemmat määräykset** vuosilta 2015-2018
- Tukevat **sote-uudistuksessa** tarvittavaa tiedonhallintaa
- **Kokoavat** yhteen ja jäsentävät joukon tarkempaa materiaalia, tukevat esim. eri järjestelmissä olennaisten määrittelyjen löytämisessä
- **Korvaavat** joukon aiemmin hajallaan olleita ohjeita ja osin vanhentuneita liitteitä ja materiaaleja
- **Huomioivat:**
  - Muuttuneet ja voimaan tulleet **säädökset** (AsTL lisäksi myös henkilötietojen käsittely, tiedonhallintalaki, rajaukset suhteessa toisiolakiin jne.)
  - **Uudenlaiset tiedonhallinnan ratkaisut**: pilvipalvelut, modulaariset tietojärjestelmät, tietoaltaat ensisijaisessa käytössä, katselin- ja asiointijärjestelmät
  - Aiempien määräysten soveltamisesta esiin nousseet **kehittämistarpeet**

Yleiskuva tietoturvasuunnitelmasta ja sen suhteesta tietojärjestelmien olennaisiin vaatimuksiin

Mikä tietoturvasuunnitelma 1/2?

Määräys 3/2021 tietoturvasuunnitelmaan sisällytettävistä selvityksistä ja vaatimuksista on osa laajempaa määräysten kokonaisuutta, jolla toimeenpannaan uutta **asiakastietolakia 784/2021**
THL:n uutinen 20.12.2021: **Tietoturvasuunnitelmaan sisällytettävien selvitysten ja vaatimusten määräys on julkaistu**

- Vuonna 2021 voimaantulleessa **asiakastietolaissa** aiemman lain tietosuojan ja tietoturvallisuuden sekä tietojärjestelmien käytön omavalvontasuunnitelma **on korvautunut tietoturvasuunnitelmalla**
- Sosiaali- ja terveydenhuollon toimijat **velvoitetaan laatimaan** tietoturvasuunnitelma
  - aiempi tietosuojan, tietoturvallisuuden ja tietojärjestelmien käytön omavalvontasuunnitelma on pohja uuden lain mukaiselle tietoturvasuunnitelmalle: sisältö pääosin vastaava kuin aiemman asiakastietolain edellyttämässä omavalvontasuunnitelmassa
- Tietoturvasuunnitelma **edistää asiakas- ja potilastietojen turvallista käsittelyä sekä sote-toimijoiden tietosuojaa ja tietoturvaa** – vahvistaa tietoturvallisuuden ja tietosuojan suunnittelun ja toteuttamisen käytäntöjä
- Määräys **tarkentaa tietoturvasuunnitelmaan tarvittavien** selvitysten **sisältöä** ja tietoturvallisuudelle sosiaali- ja terveyspalveluissa asetettavia **vaatimuksia**.

Mikä tietoturvasuunnitelma 2/2?

- Uuden asiakastietolain ja määräysten kautta täsmennetään myös **tietojärjestelmiin** kohdistuvien **olennaisten vaatimusten** toteutumista **sote-palveluiden järjestäjien ja tuottajien näkökulmasta**
  - tietoturvasuunnitelma on myös palvelunantajan väline olennaisten vaatimusten täyttämisen varmistamisessa
  - sitoo yhteen sekä palvelunantajan omat käytännöt että kaikki käytössä olevat tietojärjestelmät ja ICT-palvelut
- **Tietoturvasuunnitelma ei ole julkinen** asiakirja
  - ”Tämän määräyksen mukaista tietoturvasuunnitelmaa **ei tule sisällyttää tai yhdistää** julkaistaviin tai julkisesti saatavilla oleviin omavalvontasuunnitelmiin.”
  - ”Tietoturvasuunnitelmaa ja siinä viitattuja liitedokumentteja **tulee käsitellä ja säilyttää ottaen huomioon tarvittava suojaaminen sivullisilta** ja tarvittaessa niihin tulee merkitä salassa pidettävä -tieto.”
- Tietoturvasuunnitelman voi laatia eri tavoin, myös koostuvaksi **useista dokumenteista**
  - Esimerkiksi erikseen kaikille työntekijöille suunnatut osuudet ja tietohallinnon / ylläpidon tai johdon järjestelyt kuvaavat osuudet
- Tietoturvasuunnitelma on **käytännön työväline** – kokoava dokumentti, ”**kokonaisturvallisuuden** toimeenpanon ja seurannan suunnitelma”

Tietoturvasuunnitelmaan liittyvät velvoitteet ja suunnitelman sisältö (Asiakastietolaki 27 §) 1/2

Palvelunantajan, välittäjän ja Kansaneläkelaitoksen on laadittava tietoturvaan ja tietosuojaan sekä tietojärjestelmien käyttöön liittyvä **tietoturvasuunnitelma**.

Tietoturvasuunnitelmassa on oltava selvitykset, miten seuraavat **asiakas- ja potilastietojen** ja **järjestelmien** käsittelyyn liittyvät vaatimukset varmistetaan:

Tietoturvasuunnitelmaan liittyvät velvoitteet ja suunnitelman sisältö (Asiakastietolaki 27 §) 2/2

1) henkilöillä, jotka käyttävät tietojärjestelmiä, on niiden käytön vaatima **koulutus**;
2) tietojärjestelmien yhteydessä on saatavilla niiden asianmukaisen käytön kannalta tarpeelliset **käyttöohjeet**;
3) tietojärjestelmiä **käytetään** tietojärjestelmäpalvelun tuottajan antaman ohjeistuksen mukaisesti;
4) tietojärjestelmiä **ylläpidetään ja päivitetään** tietojärjestelmäpalvelun tuottajan ohjeistuksen mukaisesti;
5) tietojärjestelmän **käyttöympäristö** soveltuu tietojärjestelmien asianmukaiseen sekä tietoturvan ja tietosuojan varmistavaan käyttöön;
6) tietojärjestelmiin **liitetyt muut tietojärjestelmät** tai muut järjestelmät eivät vaaranna tietojärjestelmien suorituskykyä eivätkä niiden tietoturva- tai tietosuojaominaisuuksia;
7) tietojärjestelmiä **asentaa, ylläpitää ja päivittää** vain henkilö, jolla on siihen tarvittava ammattitaito ja asiantuntemus;
8) 29 §:ssä tarkoitetut tietojärjestelmät täyttävät käyttötarkoituksensa mukaiset 34 §:ssä säädetyt **olennaiset vaatimukset**; sekä
9) palvelunantajalla, välittäjällä ja Kansaneläkelaitoksella on suunnitelma siitä, miten **omavalvonta** järjestetään ja toteutetaan sen toiminnassa.

Tietoturvasuunnitelmaan liittyvät velvoitteet – jatkuu (AsTL 27 § ja 28 §)

- Ennen liittymistään valtakunnallisten tietojärjestelmäpalvelujen käyttäjäksi on palvelunantajan tietoturvasuunnitelmassa **selvitettävä**, miten tietosuoja ja valtakunnallisten palvelujen tietoturvallisen käytön edellyttämät **vaatimukset** on varmistettu. (AsTL 27 § 2 mom)

- Sosiaali- ja terveydenhuollon palvelunantajan **vastaavan johtajan** on huolehdittava, että 27 §:ssä tarkoitettu tietoturvasuunnitelma **laaditaan** ja sitä **noudatetaan**. Vastaavan johtajan on annettava kirjalliset **ohjeet asiakastietojen käsittelystä** ja **noudatettavista menettelytavoista** sekä huolehdittava **henkilökunnan riittävästä asiantuntemuksesta ja osaamisesta** asiakastietojen käsittelyssä. (AsTL 28 § 1 mom)

Olennaiset vaatimukset

Asiakastietolaki 34 § ja 29 §

- Asiakastietojen käsittelyssä käytettävän tietojärjestelmän tulee täyttää yhteentoimivuutta, tietoturvaa ja tietosuojaa sekä toiminnallisuutta koskevat **olennaiset vaatimukset**
- **Tietojärjestelmäpalvelun tuottajan** on laadittava kuvaus tietojärjestelmänsä ja hyvinvointisovelluksen valmistajan hyvinvointisovelluksensa käyttötarkoituksesta ja siitä, **kuinka se täyttää sitä koskevat olennaiset vaatimukset**
- Vaatimusten on täytyttävä käytettäessä tietojärjestelmää sekä **itsenäisesti** että **yhdessä muiden siihen liitettäviksi tarkoitettujen tietojärjestelmien kanssa**
- Terveyden ja hyvinvoinnin laitos antaa tarkempia **määräyksiä** olennaisten vaatimusten sisällöstä ja siitä, mitkä olennaiset vaatimukset on täytettävä eri palveluissa käytettävissä tietojärjestelmissä ja hyvinvointisovelluksissa
- **Palvelunantajan käyttämien tietojärjestelmien** on vastattava käyttötarkoitukseltaan palvelunantajan toimintaa ja täytettävä palvelunantajan toimintaan liittyvät olennaiset vaatimukset (Asiakastietolaki 34 §)

Sote-tietojärjestelmien olennaiset vaatimukset

Asiakastietolaki 29 § ja 34 §, THL Määräys 5/2021

- **I Toiminnalliset vaatimukset**
  - Kuvattava **käyttötarkoitus** ja **luokiteltava järjestelmä**
  - Tietojärjestelmäpalvelun tuottajan annettava **selvitys** toiminnallisten vaatimusten täyttymisestä (A- ja B-luokan järjestelmät)
  - Vaatimusten täyttyminen osoitetaan tietojärjestelmäpalvelun tuottajan antamalla selvityksellä
  - **Määräysten 4-5/2021 kautta selvitys annetaan vertailtavalla tavalla sertifiointia tai rekisteröintiä tukien**

- **II Yhteentoimivuuden vaatimukset**
  - **Todennetaan** luokan A2 ja A3 järjestelmille (Kanta-palveluihin liittyvät) **Kelan yhteistestauksen** kautta

- **III Tietoturvavaatimukset**
  - **Todennetaan** luokan A (A1, A2, A3) järjestelmille tietoturvallisuuden **arviointilaitoksen suorittamassa tietoturvallisuuden arvioinnissa**

- Yhteentoimivuuden ja tietoturvallisuuden vaatimukset nojautuvat toiminnallisiin vaatimuksiin
  - Käyttötarkoitus ja siitä annettu kuvaus, järjestelmää koskevat olennaiset vaatimukset

Olennaisten vaatimusten toteuttamisesta ja todentamisesta vastaa tietojärjestelmäpalvelun tuottaja tai valmistaja.
Palvelunantajan on varmistettava olennaisten vaatimusten toteutuminen käyttämissään tietojärjestelmissä.

Määräys 5/2021 sosiaali- ja terveydenhuollon tietojärjestelmien olennaisista toiminnallisista ja tietoturvavaatimuksista 1/2

1. Määräyksen tarkoitus
2. Määräyksen soveltamisala
3. Määräyksen keskeinen sisältö ja rajaukset
4. Suhde muihin määräyksiin, ohjeisiin ja määrityksiin
5. Olennaiset toiminnalliset vaatimukset
6. Olennaiset tietoturvavaatimukset
7. Vähimmäisvaatimusten profiilit
8. Olennaisten vaatimusten täyttäminen / tietojärjestelmäpalvelun tuottaja
9. Olennaisten vaatimusten täyttäminen / palvelunantaja

Määräys 5/2021 sosiaali- ja terveydenhuollon tietojärjestelmien olennaisista toiminnallisista ja tietoturvavaatimuksista 2/2

10. Olennaisten vaatimusten todentamisen tarkennuksia
    - 10.1 Vaatimusten täyttymisen arviointi järjestelmissä, jotka eivät liity Kanta-palveluihin
    - 10.2 Vaatimusten täyttymisen arviointi ja todentamistavat sertifioinnissa
    - 10.3 Vaatimusten ja määrittelyjen versionhallinta
    - 10.4 Poikkeamat vaatimustenmukaisuudesta
11. Ohjaus ja neuvonta
12. Voimaantulo ja siirtymäsäännökset

Liite 1 Olennaisten vaatimusten soveltamisohjeet

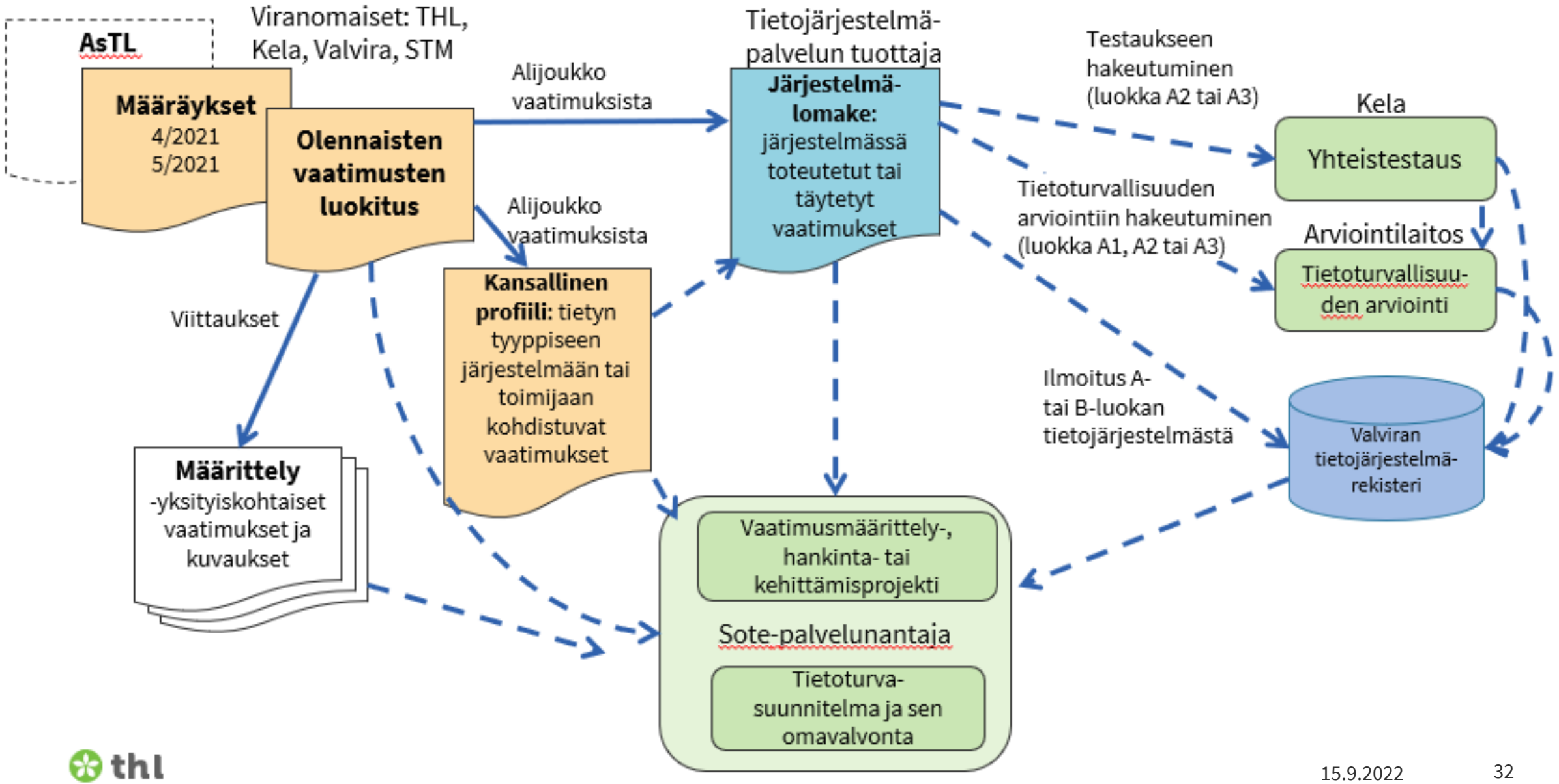
Liite 2 Olennaisten vaatimusten luokitus

Liite 3a-3g Vähimmäisvaatimusten profiilit

Liite 4 Järjestelmälomake

Olennaisten vaatimusten toteuttamisesta tietojärjestelmään ja todentamisesta vastaa valmistaja tai tietojärjestelmäpalvelun tuottaja. Palvelunantajan osaltaan huolehdittava että käytetyt tietojärjestelmät täyttävät olennaiset vaatimukset ja vastaavat palvelunantajan toimintaa.

Olennaiset vaatimukset: kansallisesti sote-tietojärjestelmille asetettavat vähimmäisvaatimukset – Määräys 5/2021 liite 1 luku 2



Olennaisten vaatimusten profiilit 1/5 (liite 3a)

Seuraaviin keskeisiin järjestelmien käyttötarkoituksiin olennaisten vaatimusten koonti:

- **3a Sähköisen reseptin profiilit**
  - **Lääkemääräystä käsittelevä potilastietojärjestelmä (PTJ)**
  - **Apteekkijärjestelmä**

Tietojärjestelmäpalvelun tuottajan on kuvattava, minkä profiilien mukaiset vaatimukset järjestelmä täyttää
Palvelunantaja voi tarkistaa eri tietojärjestelmissä toteutetut profiilit mm. Valviran tietojärjestelmärekisteristä

Olennaisten vaatimusten profiilit 2/5 (liite 3b-3c)

Seuraaviin keskeisiin järjestelmien käyttötarkoituksiin olennaisten vaatimusten koonti:

- 3b Kanta-arkistoon liittyvien järjestelmien vähimmäisvaatimusprofiilit
  - Kanta-arkistointipalvelusta tietoja hakeva sovellus tai palvelu
  - Kanta-arkistointipalvelusta haettuja tietoja hyödyntävä sovellus
  - Kanta-arkistointipalveluun tietoja toimittava sovellus tai palvelu
  - Kanta-arkistointipalveluun toimitettavia tietoja tuottava sovellus

- 3c Potilastiedon arkiston profiilit
  - Potilaskertomusjärjestelmä (perusvaatimukset)
  - Suun terveydenhuollon järjestelmä
  - **UUSI:** Optisen toimialan järjestelmä

Tietojärjestelmäpalvelun tuottajan on kuvattava, minkä profiilien mukaiset vaatimukset järjestelmä täyttää
Palvelunantaja voi tarkistaa eri tietojärjestelmissä toteutetut profiilit mm. Valviran tietojärjestelmärekisteristä

Olennaisten vaatimusten profiilit 3/5 (liite 3d)

Seuraaviin keskeisiin järjestelmien käyttötarkoituksiin olennaisten vaatimusten koonti:

- **3d Sosiaalihuollon asiakastiedon arkiston profiilit**
  - **UUSI: Sosiaalihuollon rakenteisia asiakastietoja käsittelevä järjestelmä (liittymisvelvoitteen vaatimukset)**
  - **UUSI: Sosiaalihuollon asiakastiedon arkistoon toimitettavia rakenteisia tietoja tuottava ja käsittelevä sovellus**
  - **UUSI: Sosiaalihuollon asiakastiedon arkistoon tietoja toimittava sovellus tai palvelu**
  - **UUSI: Sosiaalihuollon asiakastiedon arkistosta tietoja hakeva sovellus tai palvelu**

Tietojärjestelmäpalvelun tuottajan on kuvattava, minkä profiilien mukaiset vaatimukset järjestelmä täyttää
Palvelunantaja voi tarkistaa eri tietojärjestelmissä toteutetut profiilit mm. Valviran tietojärjestelmärekisteristä

Olennaisten vaatimusten profiilit 4/5 (liite 3e)

Seuraaviin keskeisiin järjestelmien käyttötarkoituksiin olennaisten vaatimusten koonti:

- 3e Kuvantamisen profiilit
  - **UUSI:** Kuvantamiseen liittyvä potilashallinnon perusjärjestelmä (HIS)
  - **UUSI:** Kuvantamisen toiminnanohjausjärjestelmä (RIS), Kantaan liittynyt
  - **UUSI:** Kuvantamisen toiminnanohjausjärjestelmä (RIS), EI Kantaan liittynyt
  - **UUSI:** Kuvien tallennus- ja jakamisjärjestelmä (PACS)
  - **UUSI:** Kuvantamisen katselinohjelmisto

Tietojärjestelmäpalvelun tuottajan on kuvattava, minkä profiilien mukaiset vaatimukset järjestelmä täyttää
Palvelunantaja voi tarkistaa eri tietojärjestelmissä toteutetut profiilit mm. Valviran tietojärjestelmärekisteristä

Olennaisten vaatimusten profiilit 5/5 (liite 3f-3g)

Seuraaviin keskeisiin järjestelmien käyttötarkoituksiin olennaisten vaatimusten koonti:

- 3f Todistusten profiilit
  - Kanta-arkistosta todistuksia tai lausuntoja kyselevä palvelu
  - Kanta-arkistosta todistuksia tai lausuntoja vastaanottava palvelu
  - Kanta-arkistoon todistuksia tai lausuntoja tuottava palvelu

- **3g Asiakas- tai potilastietojen käsittelyyn tarkoitetun järjestelmän vähimmäisvaatimukset (sis. luokka B tai A1)**
  - **UUSI: Asiakas- tai potilastietojen käsittelyyn tarkoitetun järjestelmän vähimmäisvaatimukset (sis. luokka B tai A1)**

Tietojärjestelmäpalvelun tuottajan on kuvattava, minkä profiilien mukaiset vaatimukset järjestelmä täyttää
Palvelunantaja voi tarkistaa eri tietojärjestelmissä toteutetut profiilit mm. Valviran tietojärjestelmärekisteristä

Sote-tietojärjestelmien luokittelu: luokka A

Määräys 4/2021 luku 5 ja liite 1

Luokka A: sertifioitavat

- **Luokka A1**: ”Tietoturvallisuuden arvioinnin suorittavat”
  - tietoturvallisuuden arviointia vaativat järjestelmät, joilta ei edellytetä yhteistestausta
  - tekniset Kanta-välityspalvelut
  - luokkaan voi kuulua sekä suppeampia että laajempia järjestelmiä
  - luokkaan voi kuulua laajasti asiakastietoja käsitteleviä / korkean riskitason järjestelmiä, jotka eivät liity Kanta-palveluihin
- **Luokka A2**: ”Kanta-palveluihin liittyvät, suppeat”
  - yhteistestausta ja tietoturvallisuuden arviointia vaativat, Kanta-palveluihin liittyvät, rajattua tietosisältöä tai käyttötarkoitusta palvelevat järjestelmät
- **Luokka A3**: ”Kanta-palveluihin liittyvät, laajat”
  - yhteistestausta ja tietoturvallisuuden arviointia vaativat, Kanta-palveluihin liittyvät, sote-palveluja tuottavaan organisaatioon kohdistuvat vaatimukset kattavasti tai merkittävässä määrin täyttävät, laajasti hoidollisia tietoja käsittelevät tai erityisen arkaluonteista tai erityissuojattavaa tietoa sisältävät järjestelmät
  - erikseen ”kriittiset luokan A3 järjestelmät” joissa erityisiä varautumisvaatimuksia

Luokittelusta vastaa tietojärjestelmäpalvelun tuottaja tai valmistaja. Palvelunantajan on käytettävä luokkaan A (A2, A3) kuuluvaa järjestelmää liittyessään Kanta-palveluihin

Sote-tietojärjestelmien luokittelu: luokka B

Määräys 4/2021 luku 5 ja liite 1

Luokka B: ei-sertifioitavat

- asiakas- tai potilastietojen käsittelyyn tarkoitetut järjestelmät
- voi sisältää mm. erikoistuneita järjestelmiä, lääkinnällisiä laitteita
- voi sisältää järjestelmiä, joissa tietoturvallisuus varmistetaan pääosin palvelunantajan suojatoimenpiteiden kautta
- voi sisältää järjestelmiä jotka tuottavat tai käyttävät joitakin tietoja (muiden järjestelmien kautta) Kanta-palveluihin

Lisäksi: luokittelemattomat

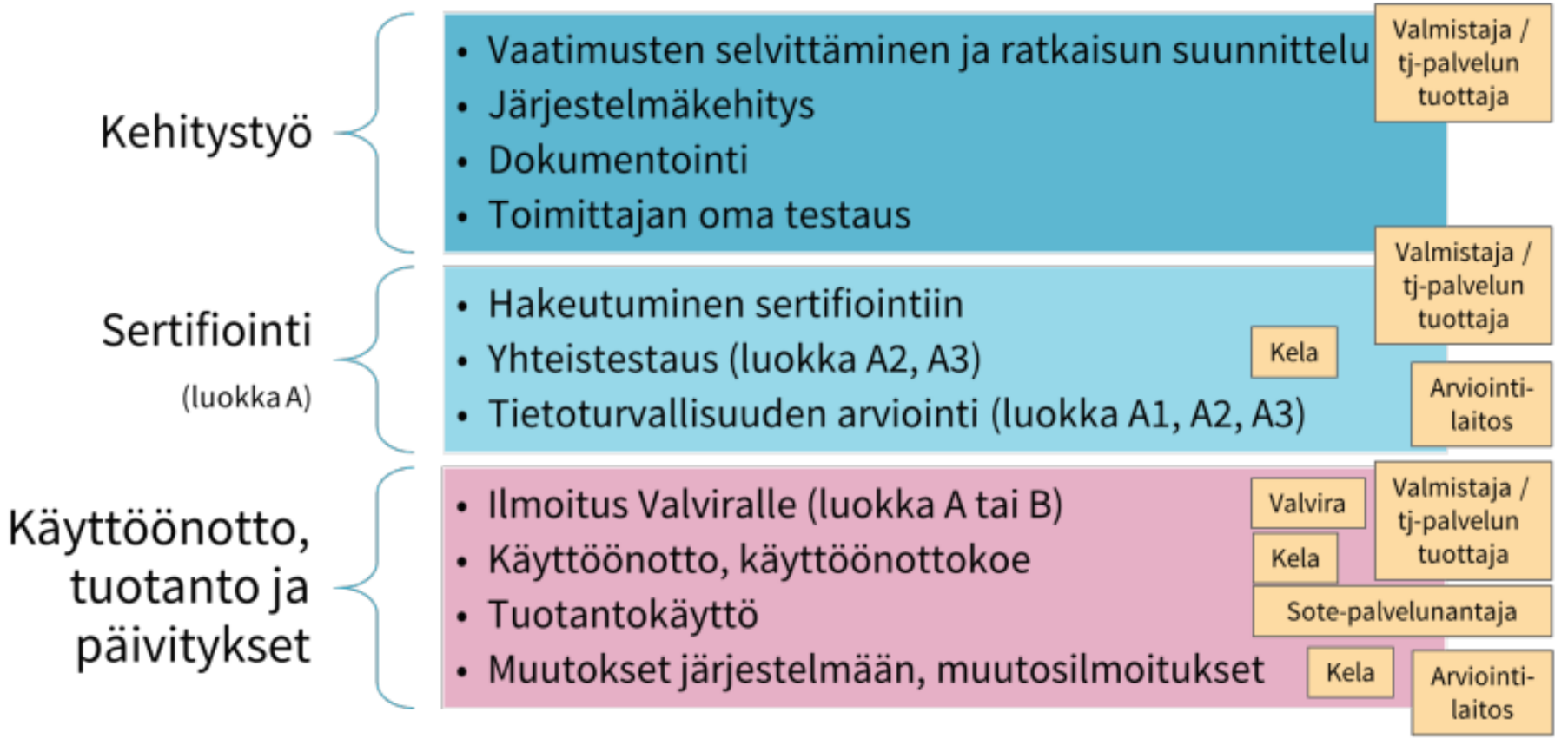
- ei asiakastietojen käsittelyyn suunniteltu tietojärjestelmä

Esimerkkejä järjestelmien luokittelusta: **Määräys 4/2021 Liite 1**

Luokittelusta vastaa tietojärjestelmäpalvelun tuottaja tai valmistaja. Palvelunantajan on käytettävä luokkaan A (A2, A3) kuuluvaa järjestelmää liittyessään Kanta-palveluihin

Sote-tietojärjestelmien sertifiointi

Määräys 5/2021 Liite 1



Sertifioinnista vastaa tietojärjestelmäpalvelun tuottaja tai valmistaja. Palvelunantajan on varmistettava, että käyttöön otettavan tietojärjestelmän tiedot löytyvät Valviran rekisteristä ja sen luokkaan A kuuluva tietojärjestelmä on sertifioitu.

Määräys 4/2021 sosiaali- ja terveydenhuollon tietojärjestelmien luokittelusta ja sertifioinnista luvut 1-7

1 Määräyksen tarkoitus

2 Määräyksen soveltamisala

3 **Määritelmät**

4 Määräyksen **rajaukset** ja suhde muihin määräyksiin ja dokumentteihin

5 Tietojärjestelmien **luokittelu**

6 Tietojärjestelmän **käyttötarkoituksen** kuvaaminen ja **selvitys** olennaisten vaatimusten täyttämisestä

7 **Sertifiointiprosessi**

- 7.1 Sertifiointiprosessiin liittyvät velvoitteet
- 7.2 Yhteistestauksen sisältö ja tulokset
- 7.3 Tietoturvallisuuden arvioinnin sisältö ja tulokset

HUOM. Tietojärjestelmän luokittelusta ja sertifioinnista vastaa tietojärjestelmäpalvelun tuottaja.
Määräys 4/2021 kohdistuu tietojärjestelmäpalvelujen tuottajiin.

Määräys 4/2021 sosiaali- ja terveydenhuollon tietojärjestelmien luokittelusta ja sertifioinnista luvut 8-12 ja liitteet

8 Tietojärjestelmän **rekisteröinti**

9 Tietojärjestelmän **käyttöönotto**

10 Vaatimustenmukaisuuden **uudistaminen**

11 Ohjaus ja neuvonta

12 Voimaantulo ja **siirtymäsäännökset**

Liite 1 Esimerkkejä järjestelmien **luokittelusta**

Liite 2 Luokkaan A kuuluvien sosiaali- ja terveydenhuollon tietojärjestelmien **muutosten** ilmoittaminen

HUOM. Tietojärjestelmän luokittelusta ja sertifioinnista vastaa tietojärjestelmäpalvelun tuottaja!
Määräys 4/2021 kohdistuu tietojärjestelmäpalvelujen tuottajiin.

Miten varmistan palvelunantajana, että käyttämäni tietojärjestelmä täyttää siihen kohdistuvat olennaiset vaatimukset?

- Yhteistyössä tietojärjestelmäpalvelun tuottajan kanssa
- Hankinta- ja kehittämisprojekteissa, järjestelmiin liittyviä sopimuksia uusittaessa ja tietoturvasuunnitelman mukaan säännöllisesti osana omavalvontaa
  - Tarkistan järjestelmän tiedot Valviran tietojärjestelmärekisteristä
    - Esim. järjestelmän luokittelu, tietoturvallisuuden arvioinnin voimassaolo, Kanta-palveluihin liittyvälle järjestelmälle suoritetut yhteistestaukset
  - Varmistan, että järjestelmässä on toteutettu ne profiilit (vähimmäisvaatimukset), jotka ovat omassa toiminnassani tarvittavia
  - Pyydän tarvittaessa tietojärjestelmäpalvelun tuottajalta THL määräyksen 5/2021 mukaisen *järjestelmälomakkeen*, jossa kuvattu yksityiskohtaisemmin, mitä kansallisia vaatimuksia järjestelmä täyttää
    - Tietojärjestelmäpalvelun tuottajan on toimitettava järjestelmälomake, jos sitä pyydetään tarjouspyynnössä tarjouksen liitteeksi tai muussa hankintaprosessiin kuuluvassa menettelyssä
  - Seuraan poikkeamia ja ilmoitan niistä tarvittaessa (Asiakastietolaki 41 §)

Palvelunantajan velvollisuudet asiakastietolaista, määräyksistä ja suhde muihin säädöksiin

Palvelunantajan velvoitteita asiakastietolaista ja määräyksistä – kooste 1/4

[osin Valviran materiaalia]

Asiakastietolaissa mainittuja palvelunantajan velvoitteita ovat muun muassa

- **liittyä Kanta-palvelujen käyttäjäksi** säädöksissä kerrottujen määräaikojen mukaisesti, jos palvelunantajalla on käytössään asiakas- ja potilastietojen käsittelyyn tarkoitettu tietojärjestelmä
- vastata Kanta-palveluihin tallennettavien tietojen **oikeellisuudesta**
- ottaa käyttöön säädösten edellyttämät uudet toiminnot määräaikojen mukaisesti
- käyttää olennaiset vaatimukset täyttävää **tietojärjestelmää**, joka vastaa **käyttötarkoitukseltaan** palvelunantajan toimintaa ja jonka tiedot löytyvät Valviran tietojärjestelmärekisteristä
    - ilmoittaa tietojärjestelmäpalvelun tuottajalle ja Valviralle, jos olennaisten vaatimusten täyttymisessä on merkittävä poikkeama

Palvelunantajan velvoitteita asiakastietolaista ja määräyksistä – kooste 2/4

[osin Valviran materiaalia]

Asiakastietolaissa mainittuja palvelunantajan velvoitteita ovat muun muassa

- huomioida, että se ei saa **ottaa käyttöön** tietojärjestelmää, jonka tietoja ei löydy Valviran tietojärjestelmärekisteristä tai jonka tietoturvallisuustodistus (luokan A järjestelmät) on vanhentunut
- nimittää **tietosuojavastaavan** (tietosuoja-asetus 37-39 artikla)
- **ilmoittaa** tietosuojavaltuutetulle, jos tietojärjestelmän olennaisten vaatimusten täyttymisessä on tietosuojapoikkeama
- **ilmoittaa** merkittävä poikkeama tietojärjestelmän olennaisten vaatimusten täyttymisessä
  - tietojärjestelmäpalvelun tuottajalle
  - Valviralle jos poikkeama voi aiheuttaa merkittävän riskin asiakasturvallisuudelle tai tietoturvalle

Palvelunantajan velvoitteita asiakastietolaista ja määräyksistä – kooste 3/4

[osin Valviran materiaalia]

Asiakastietolaissa mainittuja palvelunantajan velvoitteita ovat muun muassa

- määritellä **oikeudet asiakastietojen käyttöön** ammattihenkilölle ja muille asiakastietoja käsitteleville henkilöille
- huolehtia siitä että asiakastietojen sähköisessä käsittelyssä eri toimijat **tunnistetaan luotettavasti**
- kerätä **lokitiedot** rekisterikohtaisesti kaikesta asiakas- ja potilastietojen **käytöstä ja luovutuksesta** seurantaa ja valvontaa varten
- vastata asiakkaiden **tietopyyntöihin** siitä, kuka on käyttänyt tai kenelle luovutettu asiakasta koskevia tietoja

Palvelunantajan velvoitteita asiakastietolaista ja määräyksistä – kooste 4/4

[osin Valviran materiaalia]

Asiakastietolaissa mainittuja palvelunantajan velvoitteita ovat muun muassa

- antaa asiakkaalle tiedot asiakkaan oikeuksista ja Kanta-palveluista (**informointi**)
- huolehtia asiakastietojen luovuttamista koskevan **luovutusluvan, suostumuksen ja kiellon** vastaanottamisesta ja tallentamisesta.

- Laatia ja ylläpitää tietoturvaan ja tietosuojaan sekä tietojärjestelmien käyttöön liittyvää **tietoturvasuunnitelmaa**
  - **käytännössä suunnitelmassa kuvataan ja kannattaa kuvata, kuinka monet myös muista edellä näkyneistä velvoitteista täytetään.**

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)

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

Tietosuoja-asetuksen (GDPR) toteuttamisen välineitä 1

- Tietosuoja-asetuksen mukainen **vaikutustenarviointi** ja sen dokumentointi
- Tarkoituksena auttaa tunnistamaan, arvioimaan ja hallitsemaan henkilötietojen käsittelyyn sisältyviä riskejä.
  - arvioida käsittelytoimien tarpeellisuutta, oikeasuhtaisuutta
  - arvioida henkilöiden oikeuksiin ja vapauksiin kohdistuvia riskejä ja niiden hallintaa
  - parannetaan vaatimusten noudattamista ja osoitetaan niiden noudattaminen
- Laadittava, kun suunniteltu käsittely todennäköisesti aiheuttaa korkean riskin ihmisten oikeuksille ja vapauksille, erityisesti kun
  - henkilötietojen käsittelyssä käytetään uutta teknologiaa
  - käsitellään laajamittaisesti erityisiä henkilötietoryhmiä (kuten terveystietoja)
  - henkilön henkilökohtaisia ominaisuuksia arvioidaan automaattisen käsittelyn avulla järjestelmällisesti ja kattavasti ja arvio johtaa päätöksiin, joilla on oikeusvaikutuksia tai jotka muuten vaikuttavat henkilöön merkittävästi
  - yleisölle avointa aluetta valvotaan järjestelmällisesti ja laajamittaisesti.
- Milloin tehdään:
  - ennen henkilötietojen käsittelyn aloittamista
  - kun käsittelytoimien sisältämä riski muuttuu
- Organisaation sisäinen asiakirja - ei tarvitse julkaista
- Malli ja lisätietoja tietosuojavaltuutetun toimiston sivuilla

Vaikutustenarviointi ennen tietoturvasuunnitelman laatimista tai päivittämistä auttaa tunnistamaan seikkoja, joita erityisen tärkeää huomioida suunnitelmassa. Suunnitelma myös auttaa uusien vaikutusarviointien tekemisessä.

Tietosuoja-asetuksen (GDPR) toteuttamisen välineitä 2

- **Seloste käsittelytoimista**: kirjallinen kuvaus organisaation tekemästä henkilötietojen käsittelystä
- pakollinen jos organisaatiossa on yli 250 työntekijää TAI työntekijöiden määrästä riippumatta, kun
  - henkilötietojen käsittely aiheuttaa todennäköisesti riskin rekisteröidyn oikeuksille ja vapauksille tai
  - henkilötietojen käsittely ei ole satunnaista tai
  - käsiteltävät henkilötiedot sisältävät **erityisiä tietoryhmiä (kuten terveystiedot)** tai rikostuomioihin ja rikkomuksiin liittyviä henkilötietoja.
- Lisätietoja tietosuojavaltuutetun sivuilla
- Esimerkki sisällöstä (rekisterinpitäjän pohja / Tietosuojavaltuutetun toimisto)
  - Organisaation, tietosuojavastaavan ja edustajan tiedot
  - Tehtävä, johon tietoja käsitellään
  - Käsittelyn tarkoitus
  - (Tarvittaessa) yhteisrekisterinpitäjä ja tämän yhteystiedot
  - Rekisteröityjen ryhmät
  - Henkilötietojen ryhmät
  - Vastaanottajaryhmät
  - Viittaus (mahdolliseen) henkilötietojen käsittelijän kanssa solmittuun henkilötietojen käsittelyä koskevaan sopimukseen
  - Kolmannet maat ja kansainväliset järjestöt, joihin tietoja siirretään tai tieto siitä, ettei henkilötietoja siirretä kolmansiin maihin tai kansainvälisiin järjestöihin
  - Asianmukaisia suojatoimia koskeva dokumentaatio, jos henkilötietoja siirretään kolmansiin maihin tai kansainvälisiin järjestöihin
  - Tietojen säilytysajat, tai sen määrittämisen kriteerit
  - Kuvaus tietosuoja-asetuksen 32 artiklan 1 kohdan mukaisista teknisistä ja organisatorisista turvatoimista

Seloste kokoaa tietosuojanäkökulmasta keskeisiä tietoja – seloste ja tietoturvasuunnitelma ovat toisiaan täydentäviä dokumentteja

Tietosuoja-asetuksen (GDPR) toteuttamisen välineitä 3

- **Tietotilinpäätös:** tilannekuva organisaation henkilötietojen käsittelyn nykytilasta, sekä arvio tietosuojan toteutumisesta
- Voidaan hyödyntää keskeisenä välineenä osoitusvelvollisuuden täyttämiseen
- Tietotilinpäätökseen sisällytettäviä tietoja esimerkiksi (VAHTI-raportti 2016 tietosuojan kannalta tärkeimpiä osa-alueita)
  - jatkuvuus ja riskienhallinta
  - riskianalyysi
  - turva-arkkitehtuuri
  - **tietojärjestelmien hankinta**
  - **tietojärjestelmien kehitys ja ylläpito**
  - **pääsynhallinta**
  - omaisuuden ja tiedon hallinta
  - **päivitysten ja muutosten hallinta**
  - fyysinen turvallisuus
  - henkilöstöturvallisuus
  - **toimittajien ja sopimusten hallinta**
  - **toiminnan jatkuvuuden hallinta**
  - **tietojen käsittelyn valvonta ja seuranta**
  - **tietoturvallisuuden hallinta**
  - **laatustandardit ja auditoinnit**
  - **sidosryhmien kanssa tehdyt sopimukset**
  - **tietoturvapoikkeamien käsittely, niiden määrät ja merkitys**
  - **tietoturvapoikkeaminen ilmoitusvelvollisuus, ilmoitukset**
  - henkilötietojen käsittelytoimien vaikutusarvioinnit ja ennakkokuulemiset

Tietotilinpäätöstä voi ja kannattaa hyödyntää myös tietoturvasuunnitelman toteuttamisen ja seurannan välineenä!

NIS-direktiivin raportointivelvollisuus

- Euroopan verkko- ja tietoturvadirektiivi (NIS-direktiivi) velvoittaa tiettyjä toimijoita raportoimaan merkittävistä tietoturvahäiriöistä ja -poikkeamista sektoria valvovalle viranomaiselle
- Terveydenhuollossa sektorikohtainen viranomainen on Valvira:
  - Sosiaali- ja terveyspalvelujen antajat
  - Lääkinnällisten laitteiden valmistajat
  - Sote-tietojärjestelmien valmistajat
- Uhkista ja loukkauksista ilmoittaminen mahdollistaa kohteena olevan organisaation auttamisen ja auttaa varautumaan ajankohtaisiin uhkiin
  - Lisätietoja tietoturvauhkien ja -loukkausten ilmoittamisesta (Valviralle ja Traficomin Kyberturvallisuuskeskukselle) Valviran sivuilla

Väliyhteenveto 1/2

Säädöksissä on **velvoitteita sekä palvelunantajille että tietojärjestelmäpalvelujen tuottajille**

- Jotta tietoturvallisuus ja tietosuoja suunnitellaan ja toteutetaan riittävällä tasolla
- Jotta asiakastiedot ja niiden käsittelyssä käytetyt järjestelmät toimivat asianmukaisesti
- Jotta tiedot saadaan talteen sekä hyödynnettäväksi myös yli organisaatio- ja järjestelmärajojen.

Olennaiset vaatimukset ja tietoturvasuunnitelmat ovat keskeisiä keinoja, joiden avulla **varmistetaan sekä asiakastietojen käsittelyssä että tietojärjestelmissä vähimmäisvaatimusten täyttäminen**.

Väliyhteenveto 2/2

Olennaisten **vaatimusten toteuttamisesta tietojärjestelmiin** ja **sertifioinnista vastaa tietojärjestelmäpalvelujen tuottaja**, mutta **palvelunantajan on varmistettava,** että **käytettävät järjestelmät täyttävät olennaiset vaatimukset**.

Tietoturvasuunnitelmat ja tietojärjestelmien tietoturvavaatimukset ovat tärkeitä keinoja riskien hallinnassa ja eri säädösten velvoitteiden täyttämisessä

- Muodostavat jatkumon teknisistä ratkaisuista päivittäisessä toiminnassa tapahtuvaan tietojen käsittelyyn
- Antavat **pohjan asioille**, ”joista ainakin **on huolehdittava**”.

TAUKO – jatketaan klo 10.15

Tietoturvasuunnitelman koulutustilaisuuden ohjelma 15.9.2022

Klo 9:00-9:05	Tilaisuuden avaus, tavoitteet ja kulku
Klo 9:05-9:25	Yleiskuva voimassa olevasta asiakastietolaista ja THL:n määräyksistä
Klo 9:25-9:45	Palvelunantajan velvollisuudet asiakastietolaista, määräyksistä ja suhde muihin säädöksiin
Klo 9:45-10:05	Yleiskuva tietoturvasuunnitelmasta ja sen suhteesta tietojärjestelmien olennaisiin vaatimuksiin
Klo 10:05-10:15	**Tauko**
Klo 10:15-11:15	**Tietoturvasuunnitelman laatiminen: läpikäynti uuden mallipohjan kautta sekä koulutustilaisuuden yhteenveto**
Klo 11:15-11:30	**Kysymyksiä ja keskustelua**
Klo 11.30	**Tilaisuuden päätös**

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

Tietoturvasuunnitelman laatiminen: läpikäynti [uuden mallipohjan, .docx] kautta

Tietoturvasuunnitelma – keille ja mitä? 1/2

- "Määräys tietoturvasuunnitelmaan sisällytettävistä selvityksistä ja vaatimuksista **koskee niitä**, jotka **asiakastietolain mukaan ovat velvollisia laatimaan tietoturvasuunnitelman**: sosiaali- ja terveydenhuollon palvelunantajia, apteekkeja, välittäjiä sekä Kansaneläkelaitosta. Näiden tahojen on laadittava tietoturvaan, tietosuojaan ja tietojärjestelmien käyttöön liittyvä tietoturvasuunnitelma."

- "Tietoturvan toteutumisen varmistaminen, tietosuojasääntelyn noudattaminen ja asiakastietojen käsittelyn asianmukaisuuden varmistaminen ovat **kaikkien sosiaali- ja terveydenhuollon palveluiden tuottamiseen ja tietojärjestelmäratkaisujen toteutukseen** osallistuvien osapuolten tehtäviä."

- "Tietoturvasuunnitelmien avulla vahvistetaan sosiaali- ja terveydenhuollon toimijoiden tietoturvallisuuskäytäntöjä. Palvelunantajien, apteekkien, välittäjien ja Kansaneläkelaitoksen laatimissa tietoturvasuunnitelmissa on **oltava selvitykset siitä, miten sosiaalihuollon asiakastietojen ja potilastietojen käsittelyyn ja tietojärjestelmiin liittyvät vaatimukset varmistetaan** asiakastietolain 27 §:n 1 momentin kohtien 1-9 mukaisesti. Vaatimus koskee kaikkia asiakastietojen käsittelyyn osallistuvia palvelunantajia, apteekkeja, välittäjiä ja Kansaneläkelaitosta."

Tietoturvasuunnitelma – keille ja mitä? 2/2

- "Omavalvonnan kohteen **velvollisuutena on toimia tietoturvasuunnitelman mukaisesti** sekä **seurata aktiivisesti** suunnitelman toteutumista. Kyse on **jatkuvasta ja säännöllisestä riittävän tietoturvan ja asiakastietojen hallinnan asianmukaisten käytäntöjen varmistamisesta sekä toteuttamisesta**."

- "**Ennen liittymistään Kelan valtakunnallisten tietojärjestelmäpalvelujen (Kanta-palvelut) käyttäjäksi** on omavalvonnan kohteen tietoturvasuunnitelmassa selvitettävä, miten tietosuoja ja Kanta-palvelujen tietoturvallisen käytön edellyttämät vaatimukset on varmistettu."

Tietoturvasuunnitelma – miksi?

- Parantaa ja yhdenmukaistaa sosiaali- ja terveydenhuollon tietosuoja- ja tietoturvakäytäntöjä arkityössä
- Varmistaa, että henkilöstö tietää tietosuojaan ja tietoturvaan liittyvät menettelyt ja noudattaa niitä asiakas- ja potilastietojen käsittelyssä
- Ottaa huomioon arkaluonteisen tiedon salassapidon merkityksen
- Helpottaa ymmärtämään väärinkäytöksien seuraamukset
- Ohjaa ja tukee toimimaan tietoturvallisten käytäntöjen mukaisesti
- Auttaa seuraamaan toimintaa käytännössä – tietoturva, tietosuojan ja myös kyberturvallisuuden tilannekuva
- Auttaa varmistamaan myös muiden palvelun tuottamiseen osallistuvien tahojen tietoturvallisen toiminnan
- Selkeyttää roolit ja vastuut.

Tietoturvasuunnitelman sisällys avattuna 1/2

1. Tietoturvasuunnitelman käyttötarkoitus

2. Tietoturvasuunnitelman kohde ja päivityskäytännöt

3. Yleiset tietoturvakäytännöt

4. Menettelyt virhe- ja ongelmatilanteissa sekä jatkuvuudenhallinta

5. Henkilöstön koulutus ja osaaminen sekä tietojärjestelmien käyttöohjeet ja tietoturvallinen käyttäminen

- 5.1. Henkilöstön koulutus sekä osaamisen ylläpito ja kehittäminen
- 5.2. Tietojärjestelmien käyttöohjeet ja ohjeiden mukainen käyttö

6. Tietojärjestelmien tietoturvakäytännöt

- 6.1. Tietojärjestelmien perustiedot, kuvaukset ja olennaisten vaatimusten täyttyminen
  - 6.1.1. Kanta-palveluihin liittyvät tietojärjestelmät (luokat A2 tai A3)
  - 6.1.2. Muusta syystä tietoturva-auditoidut tietojärjestelmät (luokka A1)
  - 6.1.3. Muut asiakastietoja käsittelevät järjestelmät (luokka B)
  - 6.1.4. Muut tietojärjestelmät, jotka on otettava huomioon arkaluonteisten asiakastietojen suojaamisen kannalta
  - 6.1.5. Tietojärjestelmien olennaisten vaatimusten täyttyminen
- 6.2. Tietojärjestelmien asennus, ylläpito ja päivitys
- 6.3. Käyttövaltuuksien hallinnan ja tunnistautumisen käytännöt
- 6.4. Asiakas- ja potilastietojärjestelmien pääsynhallinnan ja käytön seurannan käytännöt

Tietoturvasuunnitelman sisällys avattuna 2/2

7. Tietojärjestelmien käyttöympäristön tietoturvakäytännöt

- 7.1. Fyysinen turvallisuus osana tietojärjestelmien käyttöympäristön turvallisuutta
- 7.2. Työasemien, mobiililaitteiden ja käyttöympäristön tukipalveluiden hallinta
- 7.3. Alusta- ja verkkopalvelujen tietoturvallinen käyttö tietosuojan ja varautumisen kannalta

8. Kanta-palvelujen liittymisen ja käytön tietoturvakäytännöt

9. Tietojärjestelmäkohtaiset tarkemmat kuvakset, ohjeet ja suunnitelmat

- 9.1. Järjestelmät X (luokkiin A2 ja A3 kuuluvat)
- 9.2. Järjestelmät X (luokkaan A1 kuuluvat)
- 9.3. Järjestelmät Y (luokkaan B kuuluvat)
- 9.4. Järjestelmät Z (muut järjestelmät, jotka eivät kuulu luokkiin A tai B)

Tietoturvasuunnitelman laatiminen on sitä yksinkertaisempaa, mitä enemmän pohjatyötä on jo tehty 1/2

- Tietoturvasuunnitelmassa
    - viitataan aina kuin mahdollista, olemassa oleviin, erikseen ylläpidettäviin ohjeisiin ja dokumentteihin (esimerkiksi linkkien avulla)
    - olennaista on, että suunnitelmasta selviää, mistä tiedot / dokumentaatio on löydettävissä tai miten vaatimuksen täyttyminen on todennettavissa
- Mikäli valmista dokumentaatiota ei ole, tietoturvasuunnitelmaan kuvataan vaadittavat asiakokonaisuudet ja toimintatavat (tai tehdään erillisiä dokumentteja, joihin viitataan tietoturvasuunnitelmasta)
- Tietoturvasuunnitelma on aina sovellettava OMAAN TOIMINTAAN. Valmis mallipohja on vain esimerkkimalli, jonka pohjalta tehdään (voidaan tehdä) tietoturvallisuuden omavalvonnan kohteen tietoturvasuunnitelma. **Määräys 3/2021 velvoittaa**, mallipohja auttaa velvoitteen täyttämisessä
- Kuvataan tietoturvasuunnitelman toteuttamisessa ja päivittämisessä noudatettavat käytännöt – mm. vastuut ja hyväksymiskäytännöt
- Merkittävä tietoturvasuunnitelmaan, mikäli joistakin suunnitelman asioista vastataan esim. sopimusten tai hankintojen kautta, myös nämä on oltava tarvittaessa todennettavissa

Tietoturvasuunnitelman laatiminen on sitä yksinkertaisempaa, mitä enemmän pohjatyötä on jo tehty 2/2

HYÖDYNNÄ MUUN MUASSA:

- Vanhan asiakastietolain mukainen omavalvontasuunnitelma
- Tietoturvapolitiikka, tietosuojapolitiikka, digitaalisen turvallisuuden politiikka tai vastaavat asiakirjat
- Riskienhallintapolitiikka, riskienhallintaan liittyvät suunnitelmat
- Selosteet henkilötietojen käsittelytoimista
- Kokonaisarkkitehtuurikuvaukset, Laatukäsikirja
- Listat sopimuksista, sopimuskumppaneista
- Omat tietoturvallisuusohjeet, etä- ja hybridityöohjeistukset, luettelot noudattavista ohjeista
- Tietojärjestelmäpalvelujen tuottajien tietoturvallisuusohjeet
- …

Tietoturvasuunnitelma – Luku 4, kalvo 1/2

Menettelyt virhe- ja ongelmatilanteissa sekä jatkuvuudenhallinta

Poikkeustilanteisiin varautumisessa ja jatkuvuuden suunnittelussa noudatetaan seuraavia toimintatapoja:

[Jatkuvuussuunnittelun ja varautumisen järjestäminen, esimerkiksi:

- aihepiiriin kuuluvat erilaiset suunnitelmat (jatkuvuus, toipuminen, varautuminen)
- käytännön harjoittelu, valmiustoiminta, ohjeistukset, ohjeiden saatavuus
- normaalista poikkeavat olosuhteet, lyhyt- ja pitkäkestoiset häiriöt, poikkeusolosuhteet
- varautuminen toimintaan poikkeustilanteissa ilman tietojärjestelmiä ja/tai alusta- ja verkkopalveluita
- …]

Virhe- ja ongelmatilanteissa noudatetaan seuraavia toimintatapoja…:

[Kuvaus siitä, miten menetellään virhe- ja ongelmatilanteiden selvittämisessä, vastuut virhe- ja poikkeustilanteissa, tarvittaessa erityyppiset virhe- ja ongelmatilanteet erikseen, esimerkiksi:

- verkko- tai tietoliikenneongelmat (menettelyt ja yhteystiedot verkkopalvelujen tuottajille, mahdolliset tuottajien ohjeet)
- tietojärjestelmien käyttöön liittyvät ongelmat (menettelyt, jos järjestelmä ei toimi, ei käynnisty tai toimii virheellisesti, eri järjestelmätoimittajien yhteystiedot ja tukipalvelut)
- tietojärjestelmien, niiden osajärjestelmien ja komponenttien hallintatoimenpiteet
  - valvonta-, huolto- ja päivitystoimet
  - …

Tietoturvasuunnitelma – Luku 4, kalvo 2/2

Menettelyt virhe- ja ongelmatilanteissa sekä jatkuvuudenhallinta

…**Virhe- ja ongelmatilanteissa** noudatetaan seuraavia toimintatapoja:

- epäiltyjen, havaittujen tai toteutuneiden tietoturva- tai tietosuojauhkien tai ongelmien hallinta
  - toimenpiteet, jos sosiaalihuollon asiakastietoja tai potilastietoja tai muita suojattavia tietoja on vuotanut sivullisille
  - toimenpiteet, jos havaintaan virus- tai haittaohjelma
  - toimenpiteet, jos työntekijän tunnukset ovat vuotaneet ulkopuolisille
  - toimenpiteet, jos havaitaan tietojen kalastelua

- toimenpiteet, jos sosiaalihuollon asiakastietoja tai potilastietoja käsittelevät tietojärjestelmät toimivat selvästi väärin suhteessa niille asetettuihin kansallisiin vaatimuksiin, kuinka asiasta ilmoitetaan tietojärjestelmäpalvelun tuottajalle tai valvontaviranomaisille
  - eli luokan A tai luokan B järjestelmien olennaisten vaatimusten täyttymisessä havaittujen merkittävien poikkeamien ilmoittaminen tietojärjestelmäpalvelun tuottajalle

- toimenpiteet, jos sosiaalihuollon asiakastietoja tai potilastietoja käsittelevät tietojärjestelmät aiheuttavat riskin potilasturvallisuudelle
  - eli luokan A tai luokan B järjestelmien merkittävien poikkeamien ilmoittaminen Valviralle, jos poikkeama aiheuttaa merkittävän riskin potilasturvallisuudelle tai tietoturvalle
  - esimerkiksi tilanteessa, jossa sosiaalihuollon asiakastiedot ja/tai potilastiedot ja/tai reseptitiedot ovat menneet väärälle asiakkaalle/potilaalle järjestelmävirheen vuoksi

- toimenpiteet tietosuojapoikkeamissa, ilmoittaminen tietosuojavaltuutetulle ja rekisteröidyille …]

Tietoturvasuunnitelma – Luku 7.1

Fyysinen turvallisuus osana tietojärjestelmien käyttöympäristön turvallisuutta

Fyysisestä turvallisuudesta osana tietoturvallisuuden varmistamista huolehditaan asiakastietojen ja tietojärjestelmien käyttöympäristössä seuraavasti:

[Kuvaukset ainakin seuraavista:

- miten huolehditaan toimitilojen lukitseminen ulkopuolisilta, kulunvalvonnan järjestelyt yms.
- näyttöpäätteiden sijoittuminen ja suojauskäytännöt, jottei sivullisilla ole näköyhteyttä ruuduille, esim. päätteiden sijoittelu, näytönsuojakalvot, käyttämättömän päätteen lukittumisaika ja salasanat
- kuinka ja millaisilla aikarajoilla määritellään istunnon aikakatkaisu tai käyttöliittymän lukittumisen aikaraja järjestelmissä, joissa käyttöliittymän käyttö on estettävä/lukittava
- kenellä on oikeus asentaa ohjelmistoja ja sovelluksia organisaation laitteille, kuinka huolehditaan siitä, että vain nämä henkilöt pääsevät tekemään asennuksia
- sallitaanko ulkoisten kovalevyjen ja muistitikkujen käyttö ja mitkä ovat niiden suojauskäytännöt, esim. vain yrityksen itse hankkimat tallennusvälineet, suojaus salasanalla, kuinka estetään se, että ulkopuoliset toimijat eivät voi tuoda muistivälineitä työasemille tai sisäverkkoon (liittyy mm. haittaohjelmilta suojautumiseen)
- tulostimien sijaintipaikat ja, kuinka estetään ulkopuolisten pääsy tulostimille, mahdolliset turvatulostusratkaisut
- arkistotoimeen liittyen sosiaalihuollon asiakastietoja tai potilastietoja sisältävien paperitulosteiden säilyttäminen paloturvallisesti lukittuna ja suojassa sivullisilta sekä niiden hävittäminen siten, etteivät sivulliset pääse tietoihin
- paperitulosteiden hävittämisen käytännön ratkaisut, esim. lukittavat säilytysastiat ja paperisilppurit, tulostajan ja tulosteiden käyttäjän vastuut tulosteiden turvallisuudesta
- tietoteknisten turvakäytäntöjen mahdollinen hyödyntäminen kulunvalvonnassa (liittyy mallipohjan kohtaan 6.4)]

Tietoturvasuunnitelma – Luku 7.3, kalvo 1/5

Alusta- ja verkkopalvelujen tietoturvallinen käyttö tietosuojan ja varautumisen kannalta

Alusta- ja verkkopalveluiden tietoturvallisuudesta huolehditaan seuraavasti…:

[Kuvaukset esimerkiksi (jos tällaisia palveluita on omavalvonnan kohteella käytössä) seuraavista:

Yleistä,

- Luettelot käytössä olevista alusta- ja verkkopalveluista sekä niiden hallinnan vastuukysymykset: palvelunantaja, tietojärjestelmäpalvelujen tuottaja(t), kolmannet osapuolet (alihankkijat)
- Tietosuojasäädösten lainmukaisuuden osoittaminen omassa toiminnassa käytettäessä ulkoisten palveluntuottajien alusta- ja verkkopalveluita (esimerkiksi mahdolliset viittaukset sopimuksiin ja tietoturvakäytänteisiin)
- Varautuminen toimintaan poikkeustilanteissa ilman tietojärjestelmiä (vrt. mallipohjan luku 4. Menettelyt virhe- ja ongelmatilanteissa sekä jatkuvuudenhallinta)

Palvelimet ja palvelinympäristöt,

- mitä palveluita ja mitä sovelluksia palvelimilla on ja kuka vastaa niiden asentamisesta ja ylläpidosta
- kuinka ne palvelimet, joilla tietojärjestelmät toimivat suojataan haittaohjelmilta, ja millainen on haittaohjelmien torjunnassa olevien ohjelmien päivityskäytäntö
- kuinka estetään se, ettei palvelinympäristössä ole aktiivisia oletustunnuksia tai muita oletuksena tulevia tietoturvallisuuden kannalta huonoja asetuksia

Tietoturvasuunnitelma – Luku 7.3, kalvo 2/5

Alusta- ja verkkopalvelujen tietoturvallinen käyttö tietosuojan ja varautumisen kannalta

- kuinka palvelinten tietoturvapäivitysten asentaminen on kuvattu ja järjestetty, miten päivitysten kriittisyys ja tarve arvioidaan, miten päivitykset testataan ja hyväksytään erillisessä testausympäristössä ennen tuotantoympäristöön asentamista
- …

Tietoverkkojen hallinta, verkkolaitteet, langattomat verkot ja reitittimet,

- kuinka on sovittu tietoliikenneoperaattoreista ja tietoliikenteen tietoturvaan liittyvistä vastuista, onko sopimuksissa mukana tietoturvallisuus- ja palvelun saatavuusasioita, mukaan lukien yhteydenotot ja menettelyt häiriötilanteissa
- miten käytössä olevien verkkojen tietoturvallisuuskäytänteet on järjestetty (esimerkiksi segmentoinnit, palomuurit, reititykset)
- salasanojen vaatiminen langattomissa verkoissa, salasanojen vaihtamiskäytäntö, yrityksen oman langattoman verkon suojaaminen ulkoisilta käyttäjiltä
- mikäli asiakkaille tarjotaan langaton verkko, sen erottaminen organisaation omasta verkosta
- reitittimien ja muiden verkkolaitteiden päivitysten ja suojausten huolehtimisen vastuut ja näihin mahdollisesti liittyvät sopimukset
- reitittimien, muiden verkkolaitteiden ja niiden komponenttien sekä laite- ja laiteohjelmistojen päivitykset
- …

Tietoturvasuunnitelma – Luku 7.3, kalvo 3/5

Alusta- ja verkkopalvelujen tietoturvallinen käyttö tietosuojan ja varautumisen kannalta

Etäyhteydet ja niiden tietoturva – tässä voidaan viitata organisaation mahdollisiin etätyöohjeistuksiin, jossa vastaavia tietoturvaan ja tietosuojaan liittyviä asioita on käsitelty,

- mitä palveluja tai järjestelmiä on sallittua käyttää etänä, miten huolehditaan muiden palvelujen etäkäytön estämisestä/kieltämisestä
- mitä tai minkälaisia palveluja Internetin kautta saa ja ei saa käyttää työasemilla
- millaisilla yhteyksillä ja tietoturvaratkaisuilla etänä käytettyjä palveluja voi ja saa käyttää (esim. VPN-yhteydet)
- laitteistojen ja ohjelmistojen huoltoyhteydet -ja käytännöt
- työntekijöille ja muille käyttäjille annettavat etäkäytön ohjeistukset esimerkiksi tietosuojaan ja tietoturvallisuuteen liittyen

- …

Pilvipalvelut, pilvipohjaiset ratkaisut, etähallintapalvelut, palvelinvuokraus, palvelinhallinta, varmistus- ja konesalipalvelut,

- henkilötietojen käsittelyyn liittyvien riskien arviointi (EU:n yleisen tietosuoja-asetuksen mukainen vaikutustenarviointi) kaikissa toiminnoissa ja niihin liittyvissä mahdollisissa alihankintaketjuissa

Tietoturvasuunnitelma – Luku 7.3, kalvo 4/5

Alusta- ja verkkopalvelujen tietoturvallinen käyttö tietosuojan ja varautumisen kannalta

- kuvaukset henkilötietojen kolmansiin maihin siirtojen riskitason arvioinnista niihin liittyvine tarkasteluineen tarvittavista organisatorisista, sopimuspohjaisista ja teknisistä suojatoimista tapaus- ja maakohtaisesti

- kuvaukset kaikista käytössä olevista pilvipalveluista (pilvipalveluiden erilaiset tyypit ja eroavaisuudet) liittyen käytössä oleviin tietojärjestelmiin; myös viittaukset näihin liittyviin sopimuksiin

- sopimusten ajantasaisuus vastaamaan voimassa olevia säädöksiä (mm. EU:n yleinen tietosuoja-asetus, tarvittaessa henkilötietojen siirtämisen perusteet ETA-alueen ulkopuolelle)

- kuvaukset käytössä olevien alusta- ja verkkopalveluiden (mukaan lukien pilvipalvelut) tilanteen jatkuvasta ja säännöllisestä seurannasta muun muassa toimivuuden, tietoturvallisuusriskien, häiriötilanteiden ja palveluiden käyttöehtojen näkökulmasta (sopimusten ja käytäntöjen päivittäminen muuttunutta tilannetta vastaavaksi)

- huolto- päivitys- ja uusimissuunnitelma tietojärjestelmien, osajärjestelmien, laitekomponenttien, verkkojen sekä huolto- ja päivitystoimenpiteiden osalta sekä toimintamalli huoltotoimenpiteisiin liittyvään päätöksentekoon

- varautumisen näkökulma, kun tietoon kohdistuu tarve olla käytettävissä myös normaalista poikkeavissa olosuhteissa; suunnitelmassa on kuvattava muun muassa, kuinka tiedon hallinnointi järjestetään mahdollisessa tilanteessa, jossa yhteiskunnan verkkoyhteydet on rajoitettu Suomen maantieteellisten rajojen sisäpuolelle.]

Tietoturvasuunnitelma – Luku 7.3, kalvo 5/5

Alusta- ja verkkopalvelujen tietoturvallinen käyttö tietosuojan ja varautumisen kannalta

Hyödyllisiä lähteitä pilvipalveluaiheeseen:

- SOTE-tietojärjestelmät pilvipalveluina, soveltamisohje, AKUSTI
- Tietosuojavaltuutetun toimisto, Henkilötietojen siirrot Euroopan talousalueen ulkopuolelle
- Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri)

Tietoturvasuunnitelma – Luku 6.1, luku 6.1.1, kalvo 1/2

6.1. Tietojärjestelmien perustiedot, kuvaukset ja olennaisten vaatimusten täyttyminen

Kuvaukset käytössä olevista tietojärjestelmistä ja siitä, millaisia käytäntöjä asiakastietojen käsittelyn, tietosuojan ja tietoturvallisuuden toteuttamisessa ja seurannassa noudatetaan näitä tietojärjestelmiä käytettäessä:

[Tämän kohdan sisältö on usein tarkoituksenmukaista koota ensimmäisten asioiden joukossa]

[Tarkemmat kuvaukset tietojärjestelmistä: Vrt. mallipohjan luku 9. Tietojärjestelmäkohtaiset tarkemmat kuvakset, ohjeet ja suunnitelmat]

[Esimerkiksi viittaus erikseen ylläpidettävään ja ajantasaiseen tietojärjestelmien luetteloon, tietojärjestelmäsalkkuun tai tietojärjestelmäportfolioon, tai luettelo käytettävistä järjestelmistä. Tarvittaessa tehtävissä yhteistyössä tietojärjestelmä- tai ratkaisutoimittajan kanssa]

[Mukaan otetaan ainakin järjestelmät, joilla on vaikutusta sosiaalihuollon asiakastietojen tai potilastietojen käsittelyyn, tietoturvaan ja tietosuojaan]

6.1.1. Kanta-palveluihin liittyvät tietojärjestelmät (luokat A2 tai A3)

[Luettelo, jossa kustakin järjestelmästä järjestelmän perustiedot: nimi, versio (tai vastaava statustieto), toimittaja, yhteystiedot, tiedot tietoturvallisuuden arviointia koskevasta todistuksesta ja sen vastaavuus Valviran tietojärjestelmärekisterin tietoihin]

Tietoturvasuunnitelma – Luku 6.1, luku 6.1.5, kalvo 2/2

6.1. Tietojärjestelmien perustiedot, kuvaukset ja olennaisten vaatimusten täyttyminen

6.1.5. Tietojärjestelmien olennaisten vaatimusten täyttyminen

[Kuvattava omavalvonnan kohteen varmistavat toimenpiteet tietojärjestelmien olennaisten vaatimusten täyttymisessä, muun muassa:

- hankinnat, sopimukset ja niiden osana varmistukset siitä, että tietojärjestelmät täyttävät toiminnassa tarvittavien vähimmäisvaatimusten profiilien mukaiset vaatimukset
- käytettävien tai päivitettävien tietojärjestelmien tietojen ja vaatimustenmukaisuuden voimassaolon tarkistaminen Valviran tietojärjestelmärekisteristä
- tietojen ylläpitomenettelyt

…]

Tietoturvasuunnitelma – Luku 8, kalvo 1/2

[Seuraavat kohdat on mahdollista kuvata myös aiempien lukujen vastaavien kohtien yhteydessä tai järjestelmäkohtaisesti]

Kanta-palvelujen osalta noudatetaan seuraavia tietoturvakäytäntöjä ja asiakastietojen käsittelyn käytäntöjä:

[Ajantasaiset kuvaukset seuraavista tai viittaukset ajantasaisiin kuvauksiin:

- kuinka käyttäjät koulutetaan tai perehdytetään tuntemaan Kanta-palvelut ja varmistetaan niiden tietoturvallinen käyttö, esim. perehdytysmateriaali, verkkokoulut/kyselyt jne., ja kuinka varmistetaan, että perehdyttäminen on tehty, henkilöstön ohjeistukset (mm. tietojen lähettäminen viivytyksettä Kanta-palveluihin), asiakkaiden informointi
- toimintamalli Kanta-palvelujen käytön aktiivisesta seurannasta
- Kanta-palvelujen edellyttämien tunnistamis- ja todentamisratkaisujen toteuttaminen: Kanta-palveluja käyttävien järjestelmien kirjautumiskäytännöt

- Sote-organisaatiorekisteritietojen tai IAH-koodiston tietojen tarkastaminen:
  - organisaatio tarkastaa tiedot kansallisen koodistopalvelun Sote-organisaatiorekisteristä
  - itsenäinen ammatinharjoittaja tarkastaa tiedot IAH-koodistosta
  - virheellisten tietojen korjaukset ja lisäykset tehdään aina oman alueen AVI:in tai Valviraan
  - otettava huomioon myös muutostilanteissa tehtävät päivitykset
- Kanta-palvelujen edellyttämien varmenneratkaisujen toteuttaminen (erityyppiset Digi- ja väestötietovirastosta tilattavat henkilöiden toimikortit ja tietoteknisten palvelujen palvelinvarmenteet)
- Kanta-palvelujen edellyttämien käyttöoikeuksien/käyttövaltuuksien hallinta ja kytkentä työntekijöiden työrooleihin – tarvittaessa myös seuraaviin rooleihin liittyvät oikeudet ja tehtävät: pääkäyttäjä(t), arkistonhoitaja(t), tietosuojavastaava(t)

Tietoturvasuunnitelma – Luku 8, kalvo 2/2

- Kanta-palvelujen ja niihin liittyvien järjestelmien käytön seuranta, mukaan lukien sosiaalihuollon asiakastietojen ja potilastietojen käyttölokin ja luovutuslokin seuranta: kuka/ketkä seuraavat, millä tavoin, kuinka usein
- Kanta-palvelujen pääsynhallinnan toteuttaminen käytetyissä tietojärjestelmissä
- Kuinka on toteutettu sosiaalihuollon ja terveydenhuollon dokumenttien ja eri rekisterien erottaminen
- Miten ja kuinka usein varmistetaan, että Kanta-palveluihin liittyvillä tietojärjestelmillä (erityisesti A2 tai A3-luokan järjestelmät) ja muilla sertifiointia edellyttävillä tietojärjestelmillä ja välityspalveluilla (luokan A1 järjestelmät) on voimassa oleva todistus tietoturvallisuuden arvioinnista, ja tiedot Valviran tietojärjestelmärekisterissä (A1, A2 tai A3-luokan järjestelmä)
- Miten ja kuinka usein varmistetaan luokan A tietojärjestelmien vaatimustenmukaisuuden voimassaolo Valviran tietojärjestelmärekisteriä ja tietojärjestelmäpalvelun tuottajilta saatavia tietoja hyödyntäen (mm. tietoturvallisuustodistuksen voimassaolo, järjestelmään toteutetut olennaisten vaatimusten profiilit ja Kanta-palveluihin liittyneille järjestelmille tehtyjen yhteistestausten vastaavuus Kanta-palveluissa edellytettyihin määrittelyihin)

Tietoturvasuunnitelma – Luku 9.1, kalvo 1/2

[Perustiedot tietojärjestelmistä: Vrt. mallipohjan luku 6.1. Tietojärjestelmien perustiedot]

[Tässä tietoturvasuunnitelman luvussa 9 kuvataan tarvittaessa kaikki tai keskeisimmät tietojärjestelmät tarkemmin, mm. niihin liittyvät ohjeistukset ja suunnitelmat. Jos käytössä on vain yksi tietojärjestelmä, tietojärjestelmäkohtaisia osioita ei välttämättä tarvita. Täältä voidaan myös viitata erikseen ylläpidettäviin järjestelmäkohtaisiin kuvauksiin]

[Seuraavassa kuvattuihin eri kohtiin voidaan soveltuvin osin käyttää samantyyppisiä kuvauksia kuin tietoturvasuunnitelman aiempien lukujen vastaavissa osissa. Seuraavissa pohjissa on yksi esimerkkimalli luokan A2 ja A3 (Kanta-palveluihin liittyvät), luokan A1 (muusta syystä tietoturva-auditoidut tietojärjestelmät), luokan B (muut sosiaalihuollon asiakastietojen tai potilastietojen käsittelyyn tarkoitettu) ja muiden järjestelmien (joita voidaan tarvittaessa ottaa mukaan tietoturvasuunnitelmaan) kuvaamiseen]

- järjestelmä, versio, toimittaja, yhteystiedot: [löytyy osin myös Valviran tietojärjestelmärekisteristä, luokka A]
- käyttötarkoitus: [kuvaus löytyy myös Valviran tietojärjestelmärekisteristä, luokka A]
- käyttäjäryhmät:

[Seuraavat kohdat tarvittavin ja soveltuvin osin, mikäli poikkeavat tietoturvasuunnitelman muissa luvuissa kuvatuista käytännöistä]

- käyttöohjeet:
- ohjeiden päivittäminen ja jakelu:
- menettelyt virhe- ja ongelmatilanteissa:
- järjestelmäkohtaiset tukipalvelut:
- asennus- ja ylläpitovastuut ja -vaatimukset:
- menettelytavat ja vastuut virhe- ja poikkeustilanteissa:

Tietoturvasuunnitelma – Luku 9.1, kalvo 2/2

- käyttövaltuushallinta järjestelmässä:
- tunnistautuminen järjestelmässä:
- lokit:
- järjestelmän lukittuminen:
- Kantaan liittyvän järjestelmän tietoturvallisuuden arviointia koskevan todistuksen tietojen varmistaminen (luokka A):
- järjestelmän tiedot Kelan testaustulokset sivulla (luokka A):
- järjestelmän tiedot Valviran tietojärjestelmärekisterissä:
  - tietojärjestelmän tietojen tarkastusajankohta Valviran tietojärjestelmärekisteristä
  - tietojärjestelmän tietoturvallisuustodistuksen voimassaolon päättymispäivä
  - tietojärjestelmään toteutetut olennaisten vaatimusten profiilit
  - tietojärjestelmälle hyväksytysti suoritetut Kelan Kanta-palvelujen yhteistestaukset (Valviran tietojärjestelmärekisteristä ja/tai Kelan testaustulokset sivulta)
  - Valviran tietojärjestelmärekisteristä mahdollisesti löytyvät tietojärjestelmien käytössä tai käyttöönotossa huomioitavat asiat

Tietoturvasuunnitelman muu sisältö pikaisesti

Tarkempi sisältö tietoturvasuunnitelman mallipohjasta

Sisällys: kertaus luvut 1-4 – läpikäyty jo edellisillä kalvoilla:

1. Tietoturvasuunnitelman käyttötarkoitus
2. Tietoturvasuunnitelman kohde ja päivityskäytännöt
3. Yleiset tietoturvakäytännöt
4. Menettelyt virhe- ja ongelmatilanteissa sekä jatkuvuudenhallinta

Tietoturvasuunnitelman muu sisältö pikaisesti luvut 5-6

Tarkempi sisältö tietoturvasuunnitelman mallipohjasta

5. Henkilöstön koulutus ja osaaminen sekä tietojärjestelmien käyttöohjeet ja tietoturvallinen käyttäminen

- 5.1. Henkilöstön koulutus sekä osaamisen ylläpito ja kehittäminen
- 5.2. Tietojärjestelmien käyttöohjeet ja ohjeiden mukainen käyttö

6. Tietojärjestelmien tietoturvakäytännöt

- 6.1. Tietojärjestelmien perustiedot, kuvaukset ja olennaisten vaatimusten täyttyminen
  - 6.1.1. Kanta-palveluihin liittyvät tietojärjestelmät (luokat A2 tai A3) – **jo läpikäyty edellisillä kalvoilla**
  - 6.1.2. Muusta syystä tietoturva-auditoidut tietojärjestelmät (luokka A1)
  - 6.1.3. Muut asiakastietoja käsittelevät järjestelmät (luokka B)
  - 6.1.4. Muut tietojärjestelmät, jotka on otettava huomioon arkaluonteisten asiakastietojen suojaamisen kannalta
  - 6.1.5. Tietojärjestelmien olennaisten vaatimusten täyttyminen – **jo läpikäyty edellisillä kalvoilla**
- 6.2. Tietojärjestelmien asennus, ylläpito ja päivitys
- 6.3. Käyttövaltuuksien hallinnan ja tunnistautumisen käytännöt
- 6.4. Asiakas- ja potilastietojärjestelmien pääsynhallinnan ja käytön seurannan käytännöt

Tietoturvasuunnitelman muu sisältö pikaisesti – luvut 7.2 ja 9.2-9.4

Tarkempi sisältö tietoturvasuunnitelman mallipohjasta

7. Tietojärjestelmien käyttöympäristön tietoturvakäytännöt

7.1. Fyysinen turvallisuus osana tietojärjestelmien käyttöympäristön turvallisuutta – jo läpikäyty edellisillä kalvoilla

7.2. Työasemien, mobiililaitteiden ja käyttöympäristön tukipalveluiden hallinta

7.3. Alusta- ja verkkopalvelujen tietoturvallinen käyttö tietosuojan ja varautumisen kannalta – jo läpikäyty edellisillä kalvoilla

9. Tietojärjestelmäkohtaiset tarkemmat kuvakset, ohjeet ja suunnitelmat

9.1. Järjestelmät X (luokkiin A2 ja A3 kuuluvat) – jo läpikäyty edellisillä kalvoilla

9.2. Järjestelmät X (luokkaan A1 kuuluvat)

9.3. Järjestelmät Y (luokkaan B kuuluvat)

9.4. Järjestelmät Z (muut järjestelmät, jotka eivät kuulu luokkiin A tai B)

Yhteenveto tietoturvasuunnitelman laatimisesta

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

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

- Asiakastietolain toimeenpano ja määräykset luovat pohjaa esim. hyvinvointialueiden tarvitsemalle tiedonhallinnalle – tietoturva- ja tietosuojakäytäntöjen yhdenmukaistaminen ja parantaminen on keskeinen osa suunnittelua myös sote-uudistuksessa

- 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** (Asiakastietolaki 28 §)

Kysymykset

Kysymyksiä saa edelleen esittää Teams-chatin kautta tai lähettämällä kysymyksiä osoitteeseen sotetiedonhallinta@thl.fi .

Kysymykset / 15.9. koulutus: yksityisten (sosiaalihuollon) palvelunantajien liittyminen Kanta-palveluihin

- K: Oliko niin, että yksityisten palvelunantajien, jotka tallentavat asiakastietoa ainoastaan omaan rekisteriinsä, on liityttävä viimeistään vuoden 2026 alusta Kanta-palveluihin?
- V: Asiakastietolaista:
  - *7 §: Palvelunantajan* on liityttävä 6 §:n 1 momentin 1, 6, 7 ja 8 kohdassa tarkoitettujen valtakunnallisten tietojärjestelmäpalvelujen käyttäjäksi. Yksityisen sosiaali- ja terveydenhuollon palvelunantajan on liityttävä valtakunnallisten tietojärjestelmäpalvelujen käyttäjäksi, jos sillä on käytössään asiakas- ja potilastietojen käsittelyyn tarkoitettu tietojärjestelmä.
  - *52 § Siirtymäsäännökset:* Julkisen sosiaalihuollon palvelunantajan on liityttävä 6 §:n 1 momentin 1 kohdassa mainittuun valtakunnalliseen asiakastietojen arkistointipalveluun viimeistään 1 päivänä syyskuuta 2024 ja yksityisen sosiaalihuollon palvelunantajan viimeistään 1 päivänä tammikuuta 2026.
- Voimassa olevan lain yleinen Kanta-liittymisvelvoite koskee kaikkia sote-palvelunantajia joilla on asiakas- ja potilastietojen käsittelyyn tarkoitettu tietojärjestelmä.Terveydenhuollon liittymisvelvoite on ollut voimassa jo joitakin vuosia. Sosiaalihuollon yksityisten palvelunantajien on oman toimintansa näkökulmasta (jos ei tuota palveluja julkisille) liityttävä viimeistään 1.1.2026.

Kysymykset / 15.9. koulutus: tilaajan järjestelmän käyttäminen / yksityinen palveluntuottaja

- K: Kun yksityinen palveluntuottaja tuottaa terveydenhuoltopalveluita jollekin soteorganisaatiolle esim. lääkäripalvelua ja ammattilainen käyttää palvelun tilaajan potilastietojärjestelmää, riittääkö että potilastietojärjestelmien osalta avataan, että toimitaan palvelun tilaajan tietoturvasuunnitelman mukaisesti näiltä osin ja heillä on vastuu järjestää potilastietojärjestelmään vaaditut dokumentoinnit. Toki palveluntuottaja vastaa omalta osaltaan tietoturvan toteutumisesta. Palveluntuottajalla ei ole missään vaiheessa omaa rekisteriä.
- V: Olennaista on tietää joka tilanteessa, minkä tietoturvasuunnitelman mukaisesti toimitaan. Tilaajan tulisi omassa suunnitelmassaan huomioida myös ostopalvelujen tuottajat ja tuottaja voi viitata tilaajan suunnitelman niihin kohtiin joiden mukaisesti toimii (esim. tietojärjestelmien osalta). Tuottajalla on syytä kuitenkin olla myös oma suunnitelma, jossa suunnitellaan tietosuojan ja tietoturvan toteuttaminen. Tuottaja voi myös tuottaa palvelua useille eri tilaajille. On tärkeää, että tilaajan ja tuottajan välisissä sopimuksissa kuvataan myös se, miten tietoturvasuunnitelman ja siihen liittyvän omavalvonnan vastuut jakautuvat.

Kysymykset / 15.9. koulutus: minimointiperiaate ja terveystietojen kirjaaminen sosiaalihuollon tietojärjestelmään

- K: Mistä löytyisi ohjeita/määräyksiä siitä, mitä tietoja asiakastietojärjestelmiin saa/ei saa tallentaa? Esim. terveystietojen kirjaaminen sosiaalihuollon tietojärjestelmään. Esim. "tietojen minimointi" on esitetty sen verran ympäripyöreästi, että tavallinen käyttäjä tarvitsisi konkreettisempia esimerkkejä.
- V: Minimointiperiaate ohjaa varsinkin järjestelmien ja ratkaisujen suunnittelua, mutta on tosiaankin lähinnä yleinen periaate. Pohjana toimivat mm. yleinen tietosuoja-asetus (GDPR) ja laki sosiaalihuollon asiakasasiakirjoista. Myös ammatillista harkintaa tarvitaan tietojen kirjaamisessa. Yksityiskohtaisempia ohjeita esimerkiksi sosiaalihuollossa kirjattavien potilastietojen osalta löytyy mm. seuraavista materiaaleista:
  - Aiheuutinen (2021): Sosiaali- ja terveydenhuollon monialaisen yhteistyön kirjaamisesta on julkaistu opas
  - Tietosuojavaltuutetun ohje Sosiaalihuollon asiakastietojen käsittelystä (2016)
  - Kanta-palvelujen käsikirja sosiaalihuollon toimijoille (2022) - Sosiaalihuollon asiakastiedon arkistoon tallennettavat ja sen ulkopuolelle jäävät tiedot (luku 9.1.3)
  - Lisäksi saatavilla on ollut aiempi ohje sosiaalihuollossa syntyvien potilastietojen erottamisesta terveydenhuollon potilasrekistereihin kuuluvista ja valtakunnalliseen potilastiedon arkistoon tallennettavista potilastiedoista

Kysymykset / 15.9. koulutus: muut kuin asiakastietojen käsittelyyn käytetyt järjestelmät, esim. laskutus ja HR

- K: Yhdistetäänkö tietoturvasuunnitelmaan myös organisaatiossa käytössä oleva laskutusjärjestelmä (asiakaslaskutus, sis. asiakkaiden henkilötietoja)? Entäpä työntekijöiden henkilötietojen näkökulmasta käytössä oleva HR-järjestelmä?
- V: Laki edellyttää tietoturvasuunnitelmaa nimenomaisesti asiakastietojen käsittelyyn liittyen, mutta monet suunnitelmassa käsiteltävät suojatoimenpiteet ja aiheet ovat sovellettavissa myös muuhun suojattavan tietoaineiston ja erityisesti henkilötietojen käsittelyyn. Laskutustiedot ja henkilöstön tiedot HR- tai käyttövaltuuksien hallintajärjestelmissä ovat hyviä esimerkkejä tästä. Tietoturvasuunnitelmassa ja siinä kuvattujen käytäntöjen piirissä saa ilman muuta olla mukana myös muita kuin asiakastietojen käsittelyn käytäntöjä ja asiakastietojen käsittelyyn tarkoitettuja tietojärjestelmiä.

Usein kysyttyjä kysymyksiä – vanhojen omavalvontasuunnitelmien päivittäminen + hyvinvointialueet

- K: Onko ohjausta siihen, missä aikataulussa organisaatioiden tulisi päivittää aiemmat omavalvontasuunnitelmat nykyisen Määräyksen mukaisiksi tietoturvasuunnitelmiksi? Voiko päivitys odottaa esim. vuotta 2023 ja Hyvinvointialueelle siirtymistä, jolloin suunnitelmat pitänee päivittää ko. organisaatiomallin mukaisiksi.
- V: Uusi laki ja määräys ovat jo astuneet voimaan. Suunnitelmien päivittämisessä nimenmuutoksen sijaan on kuitenkin **olennaista päivittää sisältö vastaamaan nykytilannetta**. Tämä ei edellytä välttämättä mittavia muutoksia tai lisäyksiä aiempaan tietosuojan ja tietoturvallisuuden omavalvontasuunnitelmaan.
- Hyvinvointialueen suunnittelussa ja sote-uudistuksessa on tärkeää ja järkevää tehdä suunnittelu suoraan vastaamaan tulevaa organisointia, jolloin on mahdollista erityisesti suunnitella kokonaisuus siten, että se palvelee hyvinvointialueen kokonaisuudessa riskien hallintaa ja myös muiden säädösten kuin asiakastietolain velvoitteiden täyttämistä.
  - Tietoturvasuunnitelmaa kannattaa käyttää välineenä esimerkiksi sote-uudistuksen alueellisen toimeenpanon tiekartan mukaisissa tietoturvallisuuteen ja tietosuojaan liittyvien asioiden suunnittelussa ja toimeenpanossa sekä sote-uudistuksen alueellisen toimeenpanon tiekartan osa-alueessa ”C. Toimialasidonnaiset järjestelmät” sekä kohdissa ”4 Riskienhallinnan ja valvonnan suunnittelu”, ”4.1 Tietoturva- ja tietosuojaohjeistuksen laatiminen”, ”4.3 Riskienhallintasuunnitelman laatiminen”, ”4.4 Sisäisen valvonnan suunnittelu”, ”1.6 tietoturvakysymykset osana tiedolla johtamisen kokonaisuutta”, jne.

Usein kysyttyjä kysymyksiä: pitääkö sosiaali- ja terveydenhuollolla olla oma tietosuojavastaavansa?

- Asiakastietolain (784/2021) 28 §:n 4 momentin mukaan tietosuojavastaavan nimittämisestä sekä tietosuojavastaavan asemasta ja tehtävistä säädetään tietosuoja-asetuksen 37-39 artiklassa.
- THL suosittelee vahvasti, että sote-organisaatioissa sote-palveluissa toimiville tietosuojavastaaville varmistetaan **sote-toimialan tuntemus**. THL pitää tärkeänä, että sinällään EU:n tietosuoja-asetuksen mukaan toimivat tietosuojavastaavat tuntevat myös ja erityisesti terveyden- ja sosiaalihuollon potilas- ja asiakastietojen erityissääntelyn.
- Asiakastietolain muutoksella ei ole tavoiteltu aiemman palvelunantajia koskevan tietosuojavastaavan nimittämisen poistamista vaan sitä, että tietosuojavastaava toimii myös sote-palveluissa tietosuoja-asetuksen mukaisesti.
- **Tietosuojavastaavan rooli ei liity sote-palveluissa ainoastaan Kanta-palveluihin**, vaan laajemmin sosiaali- ja terveydenhuollon asiakastietojen tietosuojaan.
- **Tietosuojavastaavalla tulisi olla selkeä ja dokumentoitu tehtäväkuva, jossa otetaan huomioon asiakas- ja potilastietojen käsittelyyn liittyvät velvoitteet**. Tietosuojavastaavalla tulisi olla **tehtävään soveltuva osaaminen** ja **riittävät resurssit hoitaa tehtävää** omavalvonnan kohteessa ottaen muun muassa huomioon rekisterinpitoon ja henkilötietojen käsittelyyn liittyvät vastuut ja velvoitteet, organisaation koko ja toiminnan laajuus.”
- Esimerkiksi tietoturvasuunnitelman ylläpito ja omavalvonta ovat luontevia sote-palveluissa toimivan tietosuojavastaavan tehtävänkuvaan kuuluvia tehtäviä

Usein kysyttyjä kysymyksiä – Tietosuojan vaikutusten arviointi (DPIA)

- K: Tietosuojan vaikutusten arviointi **(DPIA)** sisältää osin samoja asioita kuin tietoturvasuunnitelman sisällössä mainitaan. Näkökulma kuitenkin eri eli DPIA:ssa tietosuoja ja tietoturvasuunnitelmassa tietoturva. Ja eri lakiin perustuu velvoite tuottaa. Em. ajatuksesta huolimatta pohdituttaa myös nuo mahdolliset päällekkäisyydet.

- V: Ks. Esityksen kohta ”Tietosuoja-asetuksen (GDPR) toteuttamisen välineitä 1”. Tietoturvasuunnitelma ja esim. ISO-standardi 27701 sisältävät sekä tietoturvaan että tietosuojaan liittyviä asioita, ja niitä on mahdollista yhdistää. Vaikutustenarviointi ennen tietoturvasuunnitelman laatimista tai päivittämistä auttaa tunnistamaan seikkoja, joita erityisen tärkeää huomioida suunnitelmassa. **Valmis tai päivitettävä tietoturvasuunnitelma myös auttaa uusien vaikutusarviointien tekemisessä, jos niitä tarvitaan**.

Usein kysyttyjä kysymyksiä - työntekijät

- K: Millä tapaa työntekijöiden olisi hyvä osallistua suunnitelman laatimiseen vai "riittääkö", että heille suunnitelman sisältö jalkautetaan riittävän hyvin? Minkälainen/ mitä teemoja sisältävä tietoturvakoulutus henkilöstölle olisi järkevää järjestää vuosittain? GDPR toki asettaa omat vaateensa, mutta mitä tietoturvan näkökulmasta?
- K: Kuka/ketkä työpaikolla tietoturvasuunnitelman laativat/osallistuvat laatimiseen? (keiden olisi hyvä osallistua laadintaan)?

- V: Hyviä käytäntöjä:
  - palvelunantajan **vastaavan johtajan** huolehdittava suunnitelman laatimisesta ja noudattamisesta (laki)
  - **osallistaa tietosuojavastaavan ja työntekijät** suunnitelman tekemiseen
  - ottaa suunnitelmaan mukaan myös ne asiat, joihin kohdistuu **työntekijöiden tarpeita ja kysymyksiä**
  - tunnistaa osiot, joissa tai joihin on työntekijöiden päivittäistä toimintaa koskevia ohjeita ja varmistaa että ne ovat helposti hyödynnettävissä (esim. **erillinen ohjeistus / dokumentaatio**)
  - järjestää tietosuojasta ja tietoturvallisuudesta **”peruskoulutuksia”** toistuvasti mm. uusille työntekijöille ja tarjota myös kertausmahdollisuuksia
  - kouluttaa työntekijöitä erityisesti tilanteissa, joissa tietojen käsittelyyn, tietojärjestelmiin, tietoturvallisuuteen tai tietosuojajärjestelyihin tulee heidän **työhönsä vaikuttavia muutoksia**
  - **seurata systemaattisesti** ja pitää kirjaa koulutuksiin osallistumista (myös lain velvoite)
  - **seurata tietoturvauhkia** (esim. kalastelukampanjat) **ja tiedottaa** työntekijöille aktiivisesti tietosuojaan ja tietoturvallisuuteen liittyvistä asioista vastaavasti kuin tehdään muutakin sisäistä tiedottamista

Usein kysyttyjä kysymyksiä – Tietoturvasuunnitelman suhde omavalvontasuunnitelmiin

- K: Jäin vielä pohtimaan eri suunnitelmien suhdetta erityisesti pienten palveluntuottajien näkökulmasta, eli omavalvontasuunnitelma vs. tietoturvasuunnitelma. Voivatko nämä olla myös sama (julkinen) dokumentti, vai onko siitä jotain haittaa, jos omavalvontasuunnitelmaan sisällyttää tietoa hiukan laajemmin, jotta se vastaisi molempien dokumenttien vaatimuksiin? Oliko niin, että myös terveydenhuollon itsenäiseltä ammatinharjoittajalta vaaditaan sekä omavalvontasuunnitelma että tietoturvasuunnitelma?

- V: Ks. edellinen kysymys / tietoturvasuunnitelman salassapito. Asiakastietolain mukainen tietoturvasuunnitelma keskittyy erityisesti asiakas- ja potilastietojen käsittelyyn, tiedonhallintaan, tietojärjestelmien hallintaan sekä tietoturvaan ja tietosuojaan, kun taas esimerkiksi Valviraan tehtävä **sosiaalipalvelujen** tai **yksityisten terveyspalvelujen** omavalvontasuunnitelma ovat **erillisiä dokumentteja**, jotka ovat laajemmin **toiminnan sisällön** kannalta tehtäviä. Eri suunnitelmiin kohdistuvat tiedon saatavuustarpeet, tiedon julkaisemiseen liittyvät riskit ja sisällöt ovat niin erilaisia, että **suunnitelmia ei kannata yhdistää**. Palvelun laadun ja asiakasturvallisuuden varmistamiseen eri palveluissa tehdyissä julkaistavissa omavalvontasuunnitelmissa on voinut olla joitakin esimerkiksi henkilöstöön liittyviä kohtia, mutta monet tietoturvasuunnitelman yksityiskohdista eivät sovellu julkaistavaksi. Eri suunnitelmien välillä voi olla viittauksia ja linkityksiä toisiinsa. Osa Valviran määräyksissä ja mallipohjissa viitatuista säädöksistä ei enää ole voimassa.

Aiemmin kysyttyjä kysymyksiä – tietoturvasuunnitelman suhde standardeihin ja suosituksiin

- K: Millä tavalla tietoturvasuunnitelmassa on otettu huomioon ISO27001/27701, ITIL-suositukset, VAHTI ja Tiedonhallintalautakunnan suositukset?

- V: Määräys 3/2021, sivu 6/20, 3. kappale: "Tietoturvasuunnitelman laatimisessa suositellaan käytettäväksi tietoturvallisuuden suunnitteluun tarkoitettuja standardeja ja viitekehyksiä, kuten esimerkiksi ISO 27000-sarjan standardeja.”.
  - ISO 27000-sarja sisältää monia hyödyllisiä standardeja, joista erityisesti 27001 on keskeinen. 27701 lisää tietoturvallisuuden hallintanäkökulmaan myös tietosuoja- ja yksityisyysasioita, kuten tietoturvasuunnitelmassakin on mukana molempia näkökulmia. Lisäksi 27000-sarjassa on useita muita hyödyllisiä standardeja mm. tietoturvallisuuden hallintakeinojen menettelyihin (27002), hallintajärjestelmän toteuttamiseen (27003), tietoturvariskien hallintaan (27005), mittaamiseen (27004) ja henkilötietojen suojaamiseen pilvipalveluissa (27018).
  - Tietoturvasuunnitelman ja olennaisten vaatimusten pohjana ovat jo useita vuosia olleet useatkin eri VAHTI-suositukset, ja esimerkiksi tietojärjestelmien riskiarviointityökalussa (määräyksen 4/2021 tukimateriaalina) käytetään riskiarviointia, joka osin pohjautuu mm. VAHTI/Juhta-yhteishankkeiden sekä Tietosuojavaltuutetun toimiston materiaaleihin.
  - Tietojärjestelmien olennaisissa vaatimuksissa on viittauksia mm. Pitukri- ja Katakri-suosituksiin.
  - ITIL-suositukset IT-palvelunhallintaan eivät ole olleet erityisesti tietoturvasuunnitelman sisällön tai mallipohjan pohjana.
  - Tiedonhallintalakiin perustuvat Tiedonhallintalautakunnan suositukset ovat olleet yksi keskeinen lähdemateriaali myös määräysten uudistamisessa ja esimerkiksi lokitietojen käsittelyn lähtökohdat käyttö- ja luovutuslokin osalta ovat vastaavia kuin tiedonhallintalaissa ja lautakunnan suosituksissa.
  - Monet yleiskäyttöiset standardit ja suositukset ovat eri toimialoilla yleisesti hyödynnettyjä ja niitä kannattaa hyödyntää myös sote-palvelujen tietoturvallisuus- ja tietosuojatyössä, mutta Tietoturvasuunnitelma ja sen pohjana oleva määräys ja sote-tietojärjestelmien olennaiset vaatimukset on sovitettu nimenomaisesti **suomalaiseen sote-palvelujen tietosuoja- ja tietoturvallisuusympäristöön**.

Yhteenveto

Tietoturvallisuuden koulutustilaisuuden yhteenveto 1/2

- **Tietoturvallisuuden ja tietosuojan omavalvonta** sekä tietojärjestelmien olennaiset vaatimukset ovat keskeisiä keinoja riskien hallinnassa ja oikeusturvan toteuttamisessa!

- Tietojärjestelmien olennaisten vaatimusten sekä tietoturvan ja tietosuojan omavalvonnan kautta varmistetaan, että
  - järjestelmien toteutuksessa on riittävällä tavalla huomioitu käyttötarkoituksen edellyttämät yhteentoimivuus-, tietoturva- ja tietosuoja-asiat
  - **asiakas- ja potilastiedot suojataan asianmukaisilla tietoturva- ja tietosuojakäytännöillä palvelujen tuottajien toiminnassa**

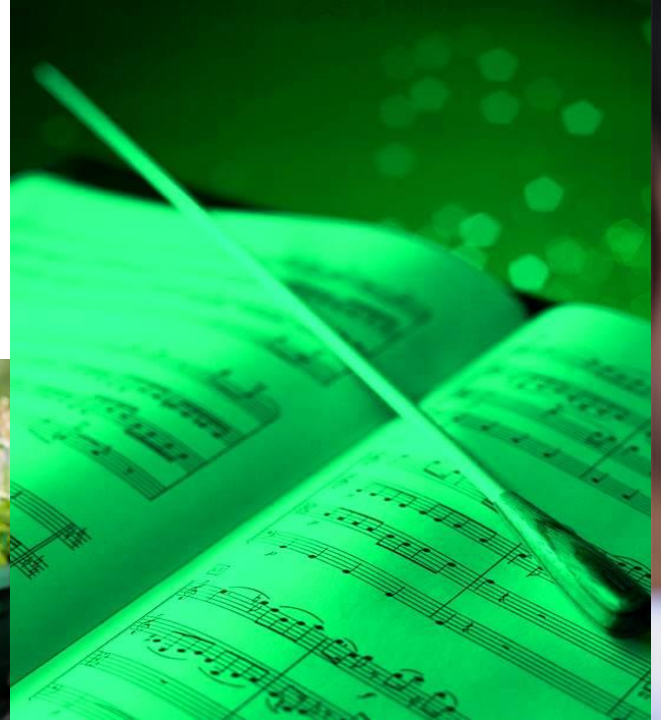
Tietoturvasuunnitelman koulutustilaisuuden yhteenveto 2/2

- **Tietoturvasuunnitelma** ja sen omavalvonta ovat **käytännön välineitä** myös yleisten tietosuoja- ja tietoturvallisuussäädöksien (mm. GDPR, Tietosuojalaki, Tiedonhallintalaki) toimeenpanoon
- Tietoturvasuunnitelman soveltaminen on **sovitettava palvelun tuottajan omien toimintatapojen** mukaiseksi
  - Esim. osa asioista mahdollista hoitaa sopimusten kautta, mutta vaatimukset pystyttävä todentamaan myös näissä tilanteissa
  - Tietoturvallisuuden ja tietosuojan toteuttaminen yksityisillä ja pienillä toimijoilla
- **Päivitä ja ylläpidä tietoturvasuunnitelma ja hyödynnä oman organisaatiosi palvelujen näkökulmasta riskien hallintaan ja säädösten mukaisten vaatimusten täyttämiseen!**

Materiaaleja ja lisätietoja

- Materiaalit tulevat saataville THL.fi tiedonhallinnan koulutusmateriaalisivulle
- THL Sote-tiedonhallinta / Tietoturvasuunnitelmat
- THL määräykset
  - Tämän tilaisuuden kannalta keskeisin Määräys 3/2021
  - THL:n määräyksen 3/2021 sivulla on myös Tietoturvasuunnitelman mallipohja
- Kysymyksiä voi lähettää osoitteeseen sotetiedonhallinta@thl.fi:
  viestin otsikkoon mukaan ”Kysymys 15.9.22 koulutuksesta”
- Tiedonhallinta sosiaali- ja terveysalalla: ajankohtaista ja uutiskirjeet /THL

- Kanta-sivut: Sertifiointi, olennaiset vaatimukset ja tietoturvasuunnitelma
- Kanta-aihepiirin koulutukset ja tilaisuudet /Kela
- Tietojärjestelmien ilmoittaminen ja valvonta, tietojärjestelmien rekisteri /Valvira
- Tietosuojavaltuutetun toimiston materiaalit:
  - Toimenpiteet ja dokumentit tietosuojan osoitusvelvollisuuden täyttämiseksi
  - Usein kysyttyä EU:n tietosuoja-asetuksesta



Kiitos – Tietoturvasuunnitelman koulutustilaisuus on päättynyt!

[Koulutuksen palautekysely]