Tietoturvasuunnitelman koulutus 4.6.2024 – Q & A

Koulutuksen aikana esille nousseet kysymykset ja niihin vastaukset

Sote-tiedonhallinnan ohjaus
sotetiedonhallinta@thl.fi

Terveyden ja hyvinvoinnin laitos
Institutet för hälsa och välfärd
Finnish Institute for Health and Welfare
PL / PB / P.O. Box 30
FI-00271 Helsinki, Finland
Puh/tel +358 29 524 6000
thl.fi

	Kysymys chatissä	Vastaus
1	K: Suunnitelman vaatimukset tuntuvat hyvin laajoilta monissa kohdissa yhden ihmisen toiminimiyrityksen näkökulmasta. Moni kohta myös vaikuttaa siltä, ettei ole ammatinharjoittajan suunnitelmassa oleellinen. On eri asia tehdä suunnitelma satojen henkilöiden kokoiselle yritykselle ja yhden ihmisen yritykselle. Olisi kiva saada selkosuomella ohjeistusta yksinyrittäjälle.	V: Kyllä, osa lain edellyttämistä kohdista on enemmän relevantteja monimutkaisemmissa tai laajemmissa ympäristöissä. Pienet palveluntuottajat ovat usein saaneet apua tietojärjestelmätoimittajaltaan tai tehneet toistensa kanssa yhteistyötä suunnitelmien tekemisessä. Apteekkariliitto on ainakin aiemmin tuottanut malleja ja pohjia apteekeille. Esimerkiksi suunnitelman mallipohjasta on järkevää tunnistaa ne kohdat, jotka ovat omassa toiminnassa tarpeen. Mallipohjaan on kuvattu asioita laajan organisaation näkökulmasta, mutta kukin palvelunantaja (pieni, keskikokoinen tai iso) täyttää juuri ne kohdat, jotka ovat relevantteja hänen omaa toimintaansa ajatellen.
2	K: Esim. MinduuPro:ssa pystyy valitsemaan, ostaako vain laskutuspalvelut vai liittyykö myös Kantaan. Pitääkö jatkossa aina liittyä Kantaan, ja kai tämä tulee näille sähköisten järjestelmien pitäjille velvollisuudeksi myös tiedottaa?	V: Kanta-liittymisvelvoite koskee yksityisiä toimijoita, jos käytössä on asiakastietolain tarkoittamien asiakastietojen käsittelyyn tarkoitettu järjestelmä. Järjestelmien valmistajien on sinällään itse tunnettava säädökset ja määriteltävä järjestelmänsä käyttötarkoitus ja otettava kantaa siihen onko järjestelmä sertifioitava tai rekisteröitävä, kannattaa ilman muuta varmistaa, että tietojärjestelmätoimittaja on asian huomioinut, jos käyttää jotain järjestelmää tai on hankkimassa sellaista. Asiakastietolaki 67 §: Yksityisen sosiaali- ja terveydenhuollon palvelunantajan on liityttävä valtakunnallisten tietojärjestelmäpalvelujen käyttäjäksi, **jos sillä on käytössään potilastietojen tai sosiaalihuollon asiakastietojen käsittelyyn tarkoitettu tietojärjestelmä**. Tietoturvasuunnitelma on oltava olemassa joka tapauksessa.

	Kysymys chatissä	Vastaus
3	K: Tiedonhallinta sote-toimialalla ei ole kovin yksinkertainen kokonaisuus, riippumatta palveluntuottajan kokoluokasta. Kanta-palveluiden myötä yksittäisen palveluntuottajan vastuu tietosuojasta korostuu ehkä jopa enemmän kuin isommissa organisaatioissa.	V: Kyllä, tiedonhallinta ja sen säädökset ovat laaja kokonaisuus. Tietosuojan perusasioiden miettiminen ja suunnittelu (myös tietoturvasuunnitelmassa) oman toiminnan ja siinä tapahtuvan tietojen käsittelyn näkökulmasta antaa hyvät lähtökohdat. Saatavilla on myös kaupallisia palveluita auttamaan tietoturva- ja tietosuoja-asioissa, sekä tietojärjestelmätoimittajilta että muilta palvelujen tarjoajilta.
4	K: Tuleeko tietoturvasuunnitelma laatia tapauksessa, jossa yksityisenä toimivalla terveydenhuollon palvelunantajalla ei ole käytössään sähköistä potilastietojärjestelmää?	V: Tietoturvasuunnitelma on lain mukaan laadittava myös, vaikka ei olisi sähköistä potilastietojärjestelmää. **Kanta-liittyminen on velvoittavaa**, jos käytössä on asiakastietolain tarkoittama asiakas- ja potilastietojen suunnitteluun tarkoitettu tietojärjestelmä. Tietoturvasuunnitelman tarkoitus on tunnistaa *ennalta* mahdolliset uhat ja riskit ja varautua niihin. Tämän vuoksi suunnitelman laatiminen on tärkeää palvelunantajan koosta riippumatta tai siitä, minkälainen järjestelmä on tai onko sitä käytössä laisinkaan.
5	K: Mitkä ovat THL:n määräyksen 3/2021 ja 3/2024 keskeiset muutokset?	V: Suurin osa sisällöstä on samaa kuin aiemminkin. Uuden lain kautta täsmentyneitä asioita olivat mm. se, että tietoturvasuunnitelman laatimisvelvoite koskee entistä selvemmin myös ei-sähköistä asiakastietojen käsittelyä (myös lain nimestä lähti pois sana ”sähköinen”). Lisäksi lain 77 § tuli tarkennus siitä että, järjestelmiä asentavien ja ylläpitävien henkilöiden luotettavuus on varmistettava, jos henkilö pääsee käsittelemään asiakastietoja. Muilta osin monet muutokset ovat lähinnä selkeytyksiä ja täydennyksiä aiempien lakien mukaisiin sisältöihin.

	Kysymys chatissä	Vastaus
6	K: Muistutus: Ei sähköinen = kynällä ja paperilla, ei wordilla, excelillä jne toteutettu. K: Jossain koulutuksessa sanottiin, että word ei ole sähköinen järjestelmä K: tietokoneella = sähköinen järjestelmä, ja aika usein sellainen vaihtoehto joka nostaa meidän tietoturvaihmisten niskakarvat pystyyn potentiaalisten ja usein reaalisten riskien vuoksi. K: Ymmärtääkseni koska word ym ei ole virallinen potilastietojen käyttöön oleva järjestelmä, tämän tyyppiset tiedostomuodot esim suojatulla ulkoisella muistilähteellä luokitellaan manuaaliseksi tiedoksi. Ainakin joskus on ollut tällainen ohjeistus. Oikaiskaa jos olen aivan väärässä? K: Ja jos siis kirjoittaa esim. tiedoston wordilla ja tulostaa sen heti paperiversioksi poistaen tiedoston myös välittömästi = manuaalinen järjestelmä.	V: Tietoturvasuunnitelmassa on huomioitava myös ei-sähköinen asiakastietojen käsittely ja yleisten ohjelmistojen käyttö. Kanta-liittyminen on eri asia, ks. yllä olevat vastaukset, kuten kohta 2. Esimerkiksi Word ei ole asiakastietojen käsittelyyn suunniteltu eikä siis Word-järjestelmää esimerkiksi sertifioida tai rekisteröidä Valviralle (ei ole asiakastietolain tarkoittama asiakastietojen käsittelyyn suunniteltu järjestelmä). Näiden yleiskäyttöisten ohjelmistojen (tekstinkäsittely ym.) kautta tapahtuvan asiakastietojen käytön ja niihin liittyvän tietosuojan suunnittelu on erityisen tärkeää tietoturvasuunnitelmassa, koska niihin järjestelmiin ei kohdistu asiakastietolain mukaista sertifiointia. Sertifioitu on turvallisempi!

	Kysymys chatissä	Vastaus
7	K: THL mallipohja on erinomainen työkalu ennen kaikkea pienille toimijoille.	V: Mallipohja on pyritty tekemään sellaiseksi, että siinä on kaikki asiat, joita voidaan tarvita ja että samoja asioita ei tarvitse toistaa. Tietoturvasuunnitelmassa olevat asiat voi jäsentää myös muulla tavalla. Suurilla toimijoilla yleensä suunnitelma pikemminkin kokoaa erillisissä dokumenteissa erikseen koottuja asioita. Kaikkien asioiden ei välttämättä tarvitse olla yhdessä suunnitelmadokumentissa, vaan esimerkiksi tietojärjestelmiin tai käyttäjien ohjeisiin liittyvät asiat voivat olla myös erillisissä dokumenteissa, joihin suunnitelmassa viitataan.
8	K: Haaste ehkä on, että asiat on käytännön tasolla hyvällä mallilla mutta huonosti dokumentoitu	V: Dokumentointi on tärkeää, jotta tiedetään, miten toimitaan yleisesti ja myös esimerkiksi, jos tulee poikkeamatilanne, ja että pystytään tarvittaessa myös osoittamaan, että tarvittavat seikat on suunniteltu, esimerkiksi jos valvontaviranomainen tarkastaa asioita. On tärkeää myös seurata ja dokumentoida suunnitelman toteuttamista. Tietoturvasuunnitelman laatiminen ja sen dokumentointi voi tuoda esille asioita, joita ei välttämättä ole huomioitu aiemmin.
9	K: Tarkoitatteko, että wordilla saa kirjoittaa esimerkiksi lausunnon potilaalle mukaan annettavaksi vain sellaisella koneella, joka ei ole verkossa ja joka ei tallenna väliaikaistiedostoja?	V: Tällaista yksityiskohtaista kansallista vaatimusta ei ole tiedossa, vaikuttaa kovin erikoiselta. Olennaista on huolehtia, että tiedot eivät päädy sivullisille.
10	K: Onko THL:lla suositusta millä tasolla tai kuka Tietoturvasuunnitelman hyväksyy? Tällä hetkellä meillä on määritettynä aluehallitus	V: Mainio kysymys! Hyvä käytäntö on käyttää samoja hyväksymismenettelyjä, joita käytetään muihin tärkeisiin dokumentteihin ja toimintaohjeisiin. Aluehallitus lienee hyvinkin sopiva käytäntö.

	Kysymys chatissä	Vastaus
11	K: Onko OneDrive tai GoogleDrive pilvipalvelut kiellettyjä käyttää sote-aloilla? K: Voiko kirjanpidon tositteita säilyttää pilvipalvelussa (esim. google drive)? Laskuissa näkyy asiakkaiden nimet ja osoitteet. K: Onko myös android-puhelimessa siis salattujen tiedostojen avaaminen turvattu toiminto, ja ne eivät tallennu puhelimeen? K: Miten lähteä liikkeelle, kun selvittää mikä on sopiva ohjelmisto tms. aineiston käsittelyyn ja tallentamiseen? esim. Teams, mistä näkee onko sopiva vai ei. K: Onko tietoturvan kannalta eroa, jos käytössä on maksullinen microsoftin 365 tilaus tai jos käyttää ilmaista officea - vai ovatko molemmat täysin kiellettyjä sotealalla?	V: THL:llä ei ole valtuuksia eikä erityisosaamista arvioida yksittäisiä palveluja, järjestelmiä eikä alustoja. Kategorista kieltoa ei ole tullut vastaan, mutta esimerkiksi pilvipalvelujen käytössä on tärkeää pystyä varmistamaan, että tiedot eivät päädy sivullisille. Alusta- ja verkkopalveluihin liittyvät asiat ovat kuvattuina myös Tietoturvasuunnitelman mallipohjassa luku 7.3. ja määräys 3:ssa luku 6.11. Mobiililaitteiden suojaaminen, kuten lukitukset ja muut turvalliset käyttötavat kuten haitallisten ohjelmien asentamisen estäminen ovat tärkeä osa tietoturvasuunnitelmaa, jos niitä käytetään asiakastietojen käsittelyyn. ”Salattujen tiedostojen avaaminen” riippuu käytettävistä laitteista ja sovelluksista, mutta on hyvä varmistaa, että puhelimeen ei myöskään tallennu tarpeettomasti arkaluonteista asiakastietoa. Yleiskäyttöisten ohjelmistojen käyttö ei ole kiellettyä, mutta tiedossamme ei ole julkaistuja arviointeja siitä, miten esimerkiksi yleiskäyttöisten toimisto-ohjelmistojen tietoturvallisuutta olisi varmistettu arkaluonteisten henkilötietojen käsittelyssä. Asiakastietojen käsittelyssä on suositeltavaa käyttää sertifioituja tai asiakastietojen käsittelyyn tarkoitettuja järjestelmiä, joiden tiedot löytyvät Valviran tietojärjestelmärekisteristä, ks. kysymys 12.

	Kysymys chatissä	Vastaus
12	K: TYP:lle kirjoitan ohjauspäiväkirjan/raportit kuntouttavassa työtoiminnassa olevista raportin 3:n kk:n välein. TYP:stä sanottiin, että tulevaisuudessa kirjataan omakantaan. Kuka järjestelmät "toimittaa" pieneen yhdistykseen? K: Palvelun tilaaja määrittelee tarjoavatko he järjestelmän käyttöön vai pitääkö palveluntuottajan hankkia järjestelmä. Hankala tilanne pienelle toimijoille, kun järjestelmät ovat kohtuullisen arvokkaita. K: Tämä on järkyttävä viidakko myös erilaisten konsulttien ja yritysten osalta, jotka tarjoavat apua ko asioihin. Miten löytää hyvät ja luotettavat kumppanit tähän?	V: Kanta-palveluun liittyviä järjestelmiä löytyy Valviran tietojärjestelmärekisteristä: https://valvira.fi/sosiaali-ja-terveydenhuolto/tietojarjestelmarekisteri. Markkinoilla on myös palveluna tarjottavia järjestelmiä, jotka on suunnattu pienemmille toimijoille esim. kuukausimaksu-pohjaisesti. Asiantuntija- ja konsulttipalveluja on myös saatavilla. Tietoturvasuunnitelmaan ja sen mallipohjaan on koottu asioita, joiden avulla voi myös täsmentää sellaisia kohtia tai asioita, joihin tuntee tarvitsevansa tukea tai apua.

	Kysymys chatissä	Vastaus
13	K: Jos tekee ammatinharjoittajana yksityisvastaanottoa ja lisäksi alihankkijana tuottaa palvelua usealle eri isommalle talolle, kuten Terveystalo, Pihlajalinna, Mehiläinen, niin riittääkö että omassa tietoturvasuunnitelmassa on kuvattu yksityisvastaanottopuoli tarkasti ja sitten viitataan noiden isojen talojen omiin tietoturvasuunnitelmiin? K: Kiinnostaisi ohjeistus myös sellaiseen tilanteeseen, jossa on useampia itsenäisiä ammatinharjoittajia samassa osoitteessa _ilman_ kattoyritystä tilanteessa, jossa ei ainakaan vielä ole perustettu yhteispalveluyksikköä - voiko tietoturvasuunnitelma olla yhteinen	V: Tärkeää on kulloinkin selkeästi dokumentoida, mikä palvelunantajan omaan toimintaan liittyvä asia on kuvattu missäkin tietoturvasuunnitelmassa. Siis minkä tietoturvasuunnitelman mukaan kukin palvelunantaja eri asioissaan toimii eli minkä tietoturvasuunnitelman ja siitä viitatun dokumentin mukaan "mennään" missäkin asiassa. Jos laaditaan yhteisiä tietoturvasuunnitelmia, on tärkeää näkyä selvästi se, kenen kaikkien suunnitelmasta on kyse, ja myös varmistaa, että kunkin osalta tarvittavat seikat ovat mukana. Jokaisen on myös sitouduttava suunnitelmaan.
14	K: Jos yrityksessämme tapahtuu tietoturvaloukkaus, miten silloin toimitaan?	V: Ks. Tietosuojavaltuutetun toimiston sivut: https://tietosuoja.fi/tietoturvaloukkaukset ja https://tietosuoja.fi/ilmoitus-tietoturvaloukkauksesta Asiakastietolain mukaan merkittävistä tietojärjestelmissä olevista poikkeamista pitää ilmoittaa järjestelmän toimittajalle (tietojärjestelmäpalvelun tuottajalle). Jos poikkeama voi aiheuttaa merkittävän riskin asiakas- tai potilasturvallisuudelle tai tietoturvalle, pitää asiasta ilmoittaa myös Valviralle. Valviralle ilmoitettavia ovat myös esimerkiksi sellaiset merkittävät tietoverkkojen häiriöt, joiden seurauksena tietojärjestelmien käyttö ja sosiaali- ja terveyspalveluiden toteuttaminen voi merkittävästi vaarantua. Lyhyet käyttö- tai verkkokatkokset eivät kuitenkaan ole tällaisia häiriöitä.

	Kysymys chatissä	Vastaus
15	K: Yleisenä käytäntönä on pienten yksityisten toimijoiden kohdalla, että asiakkaat ottavat yhteyttä tavallisella sähköpostilla sote-yrittäjään ja sote-yrittäjä vastaa sähköpostilla. Mitä ajattelette tästä käytännöstä tietoturvan osalta?	V: Tavallinen sähköposti ei ole turvallinen kanava arkaluonteisen henkilötiedon (ts. asiakastiedon) käsittelyyn. Luottamuksellista tietoa ei palvelunantaja saa välittää salaamattomassa sähköpostissa riippumatta siitä, kuinka yhteydenottaja on toiminut. Luottamuksellista tietoa ei tule myöskään säilyttää sähköpostissa.