AKUSTI-selvitys Sote-tietojärjestelmät pilvipalveluina - soveltamisohje

10.4.2022 **SOSIAALI- JA TERVEYDENHUOLLON ATK-PÄIVÄT 2022**

Perttu Pöyhtäri
Johtava konsultti

Nordic Healthcare Group

Sote-tietojärjestelmät pilvipalveluina –soveltamisohje

Kuntaliiton AKUSTI-foorumin projekti Q4/2021

Tavoitteena selkeyttää:

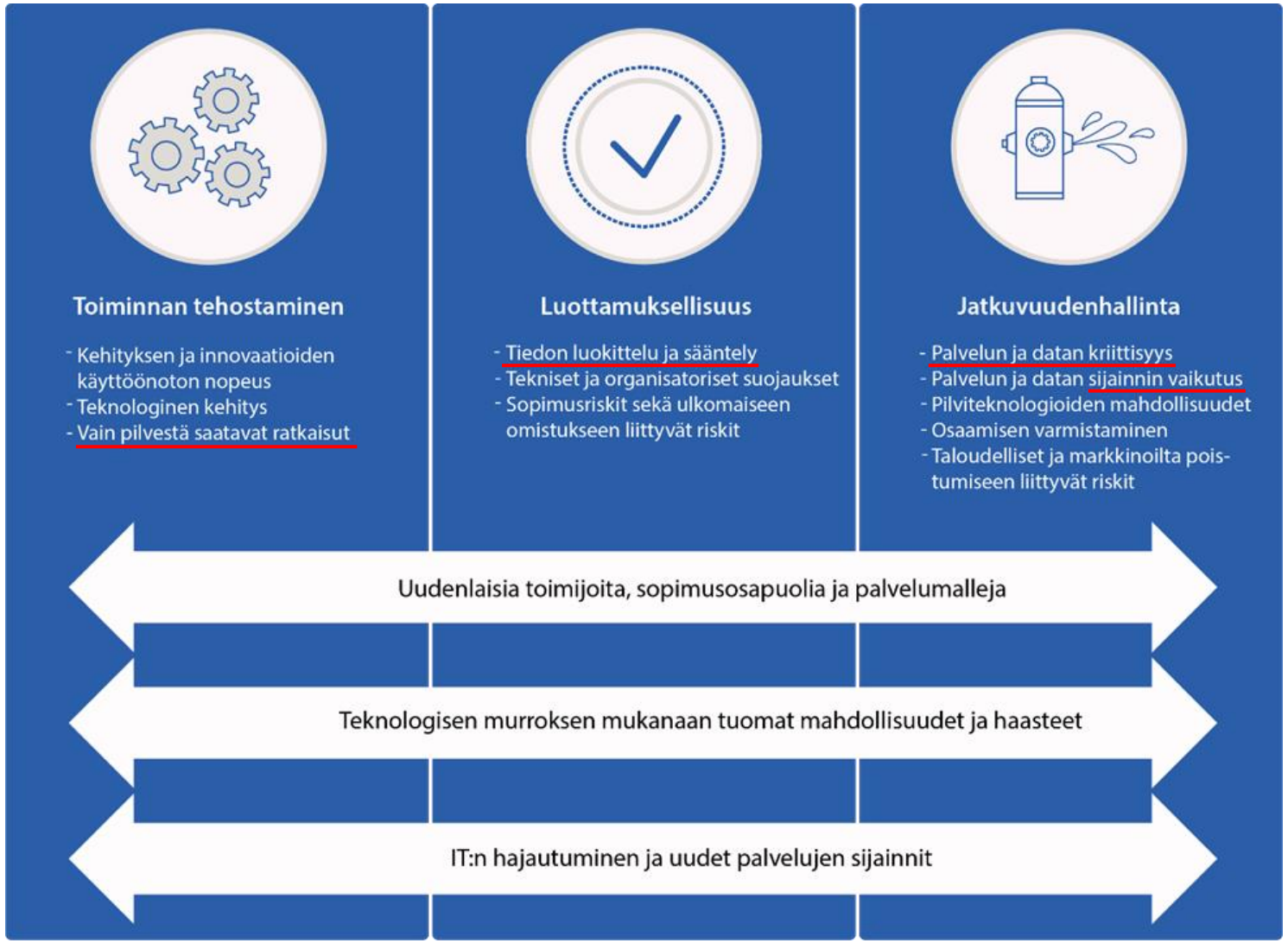
- Miten pilvisiirtymä vaikuttaa sote-toimialaan?
- Pilvipalveluiden sääntely nykytila?
- Miten asiakastietoja käsittelevien palveluiden toteuttaminen pilvipalveluna eroaa perinteisistä palvelu- ja tuotantomalleista?

Taustalla osittain epäselväksi ja tulkinnanvaraiseksi koettu kansallinen sääntely ja ohjeistus. Tämä on johtanut erilaisiin tulkintoihin eri organisaatioissa pilvipalveluiden käytön mahdollisuuksista ja rajoittanut osittain pilvisiirtymää.

Mukana merkittävä määrä sote-kentän, ministeriöiden ja muiden viranomaistahojen sekä teknologiantoimittajien asiantuntijoita

https://www.kuntaliitto.fi/julkaisut/2022/2158-sote-tietojarjestelmat-pilvipalveluina
(ISBN 978-952-293-835-0)

Sote-pilvisiirtymän keskeiset näkökulmat



Keskeiset näkökulmat

Muutosten hallinta vaatii monipuolista uutta osaamista

Yhtäaikaisia muutoksia

Ks. ohjeen luku 2.2

Nykytila

Nordic Healthcare Group

Sote pilvisiirtymä osana ICT trendejä

Merkittävä osa ICT-ratkaisuista siirtyvät palveluna ostettavaksi

Uusilla teknologioilla toteutettavia ICT-palveluja saa enää rajoitetusti oman lähikonesalien alustoille
Yhä useammin nämä ratkaisut on luokiteltavissa pilvipalveluksi.

Teknologiainvestoinnit kohdistuvat pilveen

Kansainvälisesti ICT-panostukset ovat keskittyneet jo noin 10 vuotta pilviteknologioihin.
Suomen sote ICT-kehityksen on olennaista hyödyntää näitä valtavia kehityspanoksia

ICT kansainvälistyy

Sote ratkaisut ovat entistä enemmän kansainvälisten markkinoiden vaatimusten mukaan toteutettuja pilvipalveluita
Kansallisten erityisvaatimusten huomioiminen on hyvin rajallista. EU sääntely paremmin tunnettua esim. MDR, GDPR.

Kokonaisarkkitehtuuri hajautuu

Erilaiset pilvipalvelut osa ICT-arkkitehtuurin hajautumista organisaation seinien ulkopuolelle. Uusia toimijoita, sopimisosapuolia ja palvelumalleja.
Hajautuvan kokonaisuuden hallinta vaatii erityisosaamista ja aktiivista panostusta.

Kehitys ja innovaatio; pilvipalveluiden käytön rajoittaminen aiheuttaa vaihtoehtokustannuksia

Moderneja ratkaisuja ja innovaatioita ei saada käyttöön. Joudutaan toteuttamaan kalliita erityisratkaisuja sote-tarpeisiin ja osaamisen varmistaminen vaikeutuu.
Tuloksena muita toimialoja hitaampi tehokkuuden kehittyminen, mikä näkyy palveluiden laadussa ja vaikuttavuudessa.

Ohjeen luku 2.1

Pilvipalveluita käytetään laajasti ja kasvavissa määrin

- Hyvin erilaisia pilviratkaisuja, teknologioita ja ympäristöjä
- Organisaatioiden pilvikyvykkyydet sekä pilvisiirtymän tilanne vaihtelevat huomattavasti
- **Ei ole kaiken kattavaa ”tee näin”-ohjetta, joka kattaa aukottomasti kaikki erilaiset tarpeet, ympäristöt ja ratkaisut**
- Pilvipalvelut keskittyvät merkittävästi muutaman toimittajan hyperskaalautuville pilvipalvelualustoille.
  - Näiden osalta kansallisten/EU linjausten terävöittäminen on erityisen tärkeää.
  - EU:lla ei ole omaa hyperskaalautuvaa pilveä ja pilvisuvereniteetti onkin aktiivinen teema.

Esimerkkejä sote-pilvipalveluista:

- Sähköposti, kalenteri ja tiimityön ratkaisut (Office 365)
- Data-alustat: Tietoallas, tutkijantyötilat, tietovarastot, raportointi
- Konesalipalvelut (IaaS/PaaS)
- Organisaation toiminnanohjaus, logistiikka ja HR-järjestelmiä (ERP)
- Lomakepalvelut
- Erilaisia erikoisalakohtaisia järjestelmiä
- Hyvinvointialue tasoinen tuotannonohjaus
- Leikkaus- ja anestesiajärjestelmien ei-kriittisiä osia
- Kansalaisille suunnatut palvelut
- Kotiin toimitettavien palveluiden palvelualustat, hyvinvointilaitealustat
- Kliininen päätöksenteontuki
- Laaturekisterit
- Laboratorion tutkimusohjekirja
- Terveysportti
- Koulutus- ja perehdytysalustat
- Puheentunnistus
- Asiakastiedon hakukone, aluekatseluratkaisut
- www-sivut
- Taloautomaatiojärjestelmät (IoT)
- Yksityisen sektorin asiakas- ja potilastietojärjestelmät
- Kansallisia palveluita
- …

Pilvipalveluiden sääntely ja luottamuksellisuus

Nordic Healthcare Group

Lainsäädäntö, ohjeet ja suositukset

Lainsäädäntöä:

- Asiakastietolaki
- THL määräykset (erit. 04/2021 ja 05/2021)
- Toisiolaki ja Findata määräykset
- GDPR ja tietosuojalaki
- Terveydenhuoltolaki
- Sosiaalihuoltolaki
- Potilaslaki
- Julkisuuslaki
- Tiedonhallintalaki
- MDR
- Arviointilaki
- Päivystysasetus
- Ensihoitoasetus
- Laki julkisen hallinnon turvallisuusverkkotoiminnasta
- Valmiuslaki

Ohjeet, suositukset ja standardit

- VM:n ohjeistukset: Tuottavuutta pilvipalveluilla (2020), laajempi Pilvipalveluiden soveltamisohje (2020) sekä Julkisen hallinnon pilvipalvelulinjaukset (2019)
- Pitukri: Pilviturvallisuuden kriteeristö
- Katakri: Kansallisen turvallisuuden kriteeristö sekä
- (Julkri: Julkisen hallinnon digitaalisen turvallisuuden arviointikriteeristö, valmistelussa)
- VAHTI hyvät käytännöt –tukimateriaalit
- Tiedonhallintalakiin liittyvät suositukset
  - Suositus turvaluokiteltavien asiakirjojen käsittelystä pilvipalvelussa
  - (Suositus salassa pidettävän tiedon käsittelystä pilvipalvelussa, valmistelussa)
- Tietosuoja-asetuksen 40 artiklan mukaiset käytännesäännöt (SCOPE ja CISPE)
- ISO standardeista 27000, 27017, 27018, 27701 ja 9001
- Pilvipalvelualustojen toimittajien koulutusmateriaalit, compliance-dokumentaatiot ja parhaat käytännöt.

Ohjeen luvut 4.2 ja 4.3

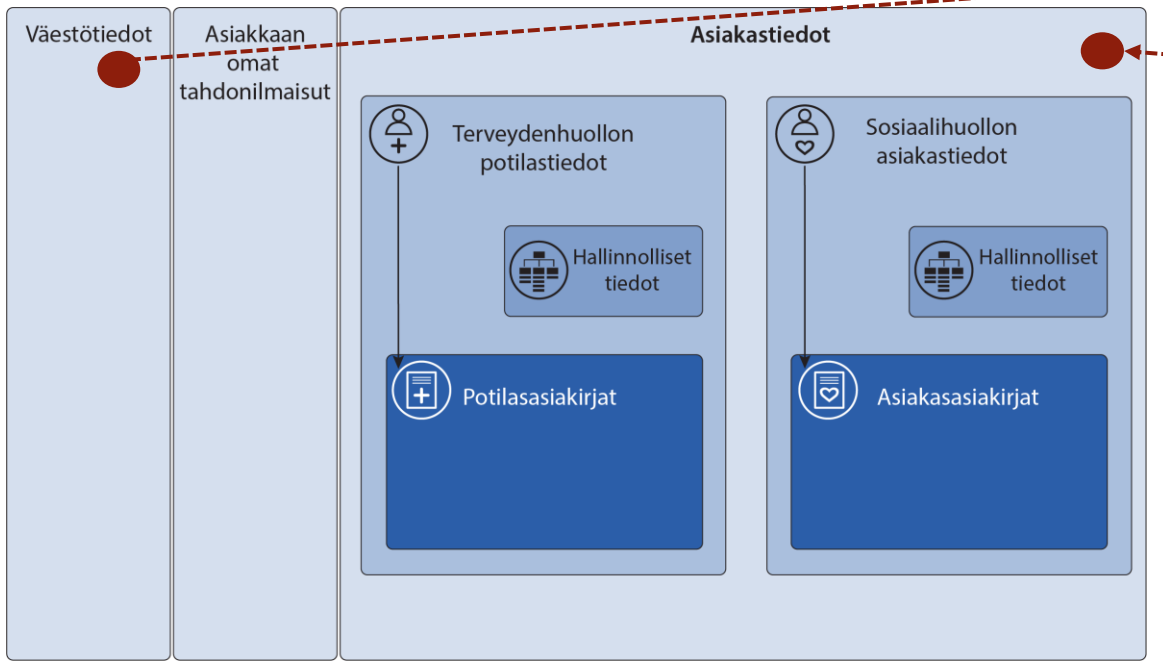
Sote-tiedon julkisuusluokat

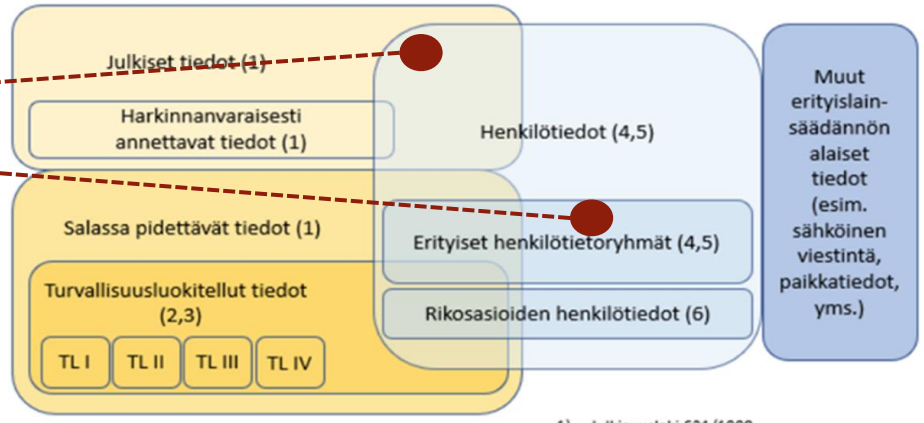
Pilvipalveluiden kannalta tärkeimmät tiedon julkisuusluokat:

1) Henkilötieto (asiakkaat, henkilökunta, väestö), GDPR ja tietosuojalain mukainen käsittely.
2) Sosiaali- ja terveydenhuollon salassa pidettävä asiakastieto on suojattava kaikilta ulkopuolisilta.

Asiakastiedot <u>eivät ole</u> turvaluokiteltavia asiakirjoja, joita koskee erityisiä rajoitteita tietojen käsittelyssä.

Sote-organisaatiolla on kuitenkin käytössään turvaluokiteltavia asiakirjoja, esim. varautumiseen liittyen.





Kuvan lähde: DVV "Suositus salassa pidettävän tiedon käsittelystä" (luonnos)

1) Julkisuuslaki 621/1999
2) Tiedonhallintalaki 906/2019
3) Turvallisuusluokitteluasetus 1011/2019
4) EU:n yleinen tietosuoja-asetus (EU) 2016/679
5) Tietosuojalaki 1050/2018
6) Laki henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä 1054/2018

Ohjeen luku 4.4

Sääntelyn LINJAUKSET

1. Valtionvarainministeriön pilvilinjaukset **suosittelevat pilvipalveluiden käyttöä julkishallinnossa aina ensisijaisesti**, kun ne ovat paras ratkaisu tarpeeseen (2019)

2. Sääntely on teknologianeutraalia; **pilvipalveluiden käytölle sote-asiakastietoa käsitteleville järjestelmissä ei ole kategorista estettä**

3. Toisaalta **pilvipalveluiden on täytettävä samat vaatimukset**, kuin perinteisemmillä palvelu- ja tuotantomalleilla toteutettujen palveluiden

Palvelun ja tiedon SIJAINTI?

1. **Sääntely ei lähtökohtaisesti eroa sen suhteen talletetaanko ja käsitelläänkö sote asiakastietoja Suomessa vai muualla EU/ETA-alueella**
    - GDPR takaa henkilötiedon vapaan liikkuvuuden; käsittely EU/ETA-alueella samoin perustein kuin Suomessa.

2. Asiakastietojen käsittely ja tallentaminen on mahdollista myös EU/ETA-alueen ulkopuolella, kun GDPR:n vaatimukset (siirtoperuste, TIA riskiarviot, ..) henkilötietojen siirrolle huomioidaan
    - Kuitenkin mm. sopimusriskien hallittavuuden vuoksi suositellaan rajaamaan käsittely EU/ETA-alueelle aina kun mahdollista.

Erityisiä varautumisen vaatimuksia

Säännön vahvistava ”poikkeus”

THL määräyksissä 04/2021 ja 05/2021 asetetaan jatkuvuuden varmistamiselle asetetaan erityisiä varautumisen vaatimuksia julkisen terveydenhuollon ensihoidon ja päivystyksen toteuttamiseen tarvittavien kriittisten järjestelmien osalta (ns. A3-kriittiset):

- ”Kriittisiä luokan A3 järjestelmiä ovat **ne luokan A3 tietojärjestelmät**, joita käytetään erikoissairaanhoidossa tai kuntien tai hyvinvointialueiden sairaaloissa tai julkisen perusterveydenhuollon avosairaanhoidossa **päivystysvastuun toteuttamisessa ja ensihoidossa** taudinmääritykseen, sairauksien tutkimukseen ja hoitoon ja näihin liittyvien asiakastietojen hallintaan. Kriittisten järjestelmien joukkoa on mahdollista laajentaa myöhemmin.”
- ”Luokan A3 kriittisissä järjestelmissä järjestelmän **jatkuva toimivuus tai viiveetön palauttaminen toimivaksi on oltava mahdollista nopeasti** sellaisen poikkeavan tilanteen vallitessa, jossa **yhteiskunnan verkkoyhteydet on rajoitettu Suomen maantieteellisten rajojen sisäpuolelle**.” (liite 3g, vaatimus AKYM16).

Huomioi:

- Nämäkään vaatimukset eivät ole pilvispesifisiä tai kategorisesta rajaa EU/ETA-alueen pilvipalveluiden käyttöä pois keinovalikoimasta.
- Julkisen terveydenhuollon päivystysvelvollisten organisaatioiden *jatkuvuuden kannalta kriittiset järjestelmät* on nykyisin toteutettu valtaosin Suomessa sijaitsevista konesaleista

Vaatimuksenmukaisuuden varmistaminen

1. Pilvipalveluiden tietoturva on yleensä paremmalla tasolla kuin lähikonesalista tuotetun palvelun, mutta sen toteuttaminen vaatii erilaista osaamista

2. Vaatimustenmukaisuuden ja luottamuksellisuuden todentamisessa pilvipalveluissa korostuu **dokumentaatio ja yhteistyö** (hallintamalli)
    - Sopimusten, riskiarvioiden, käytännesääntöjen, sertifiointien, tietoturvakuvausten, ratkaisu- / palvelukuvausten sekä hallintamallin rooli on iso

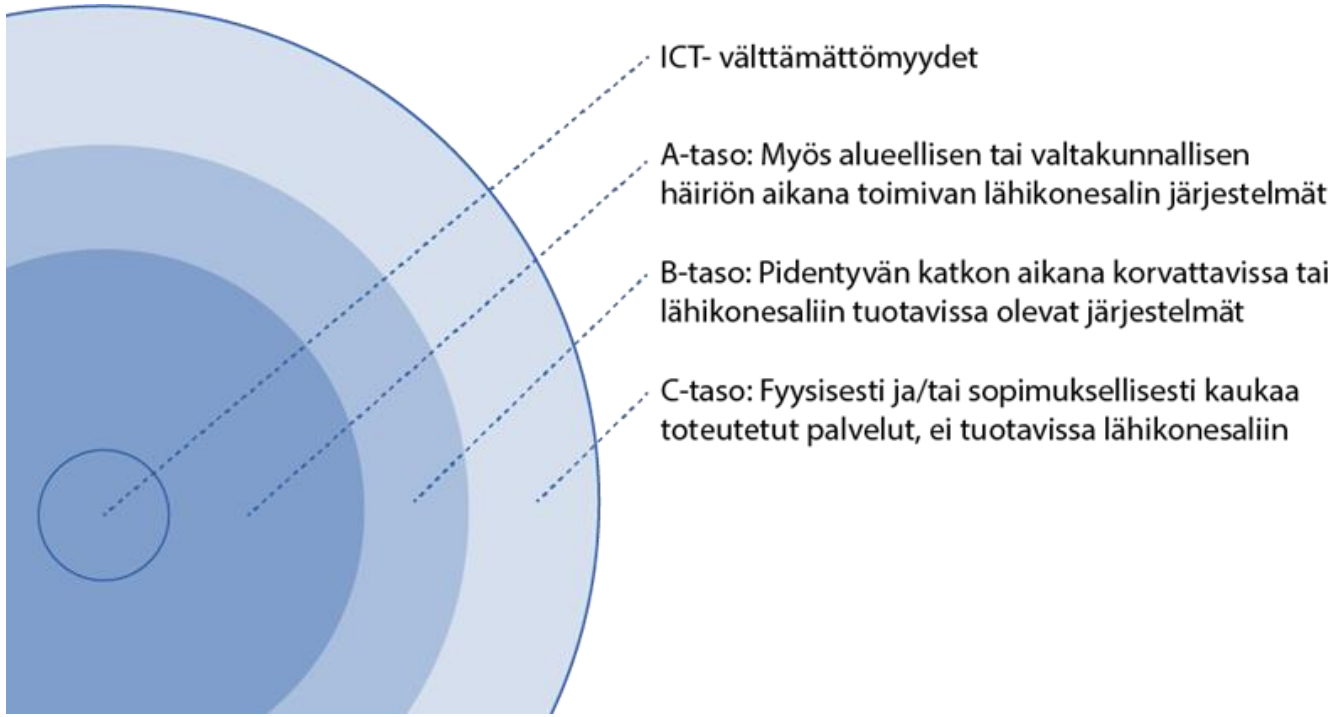
3. Ratkaisukohtaiset **sopimusriskien hallinnan** sekä **teknisten- ja organisatoristen suojausten arvioinnin** pilviosaamista on kehitettävä systemaattisesti

Pilvipalvelut ja jatkuvuudenhallinta

Nordic Healthcare Group

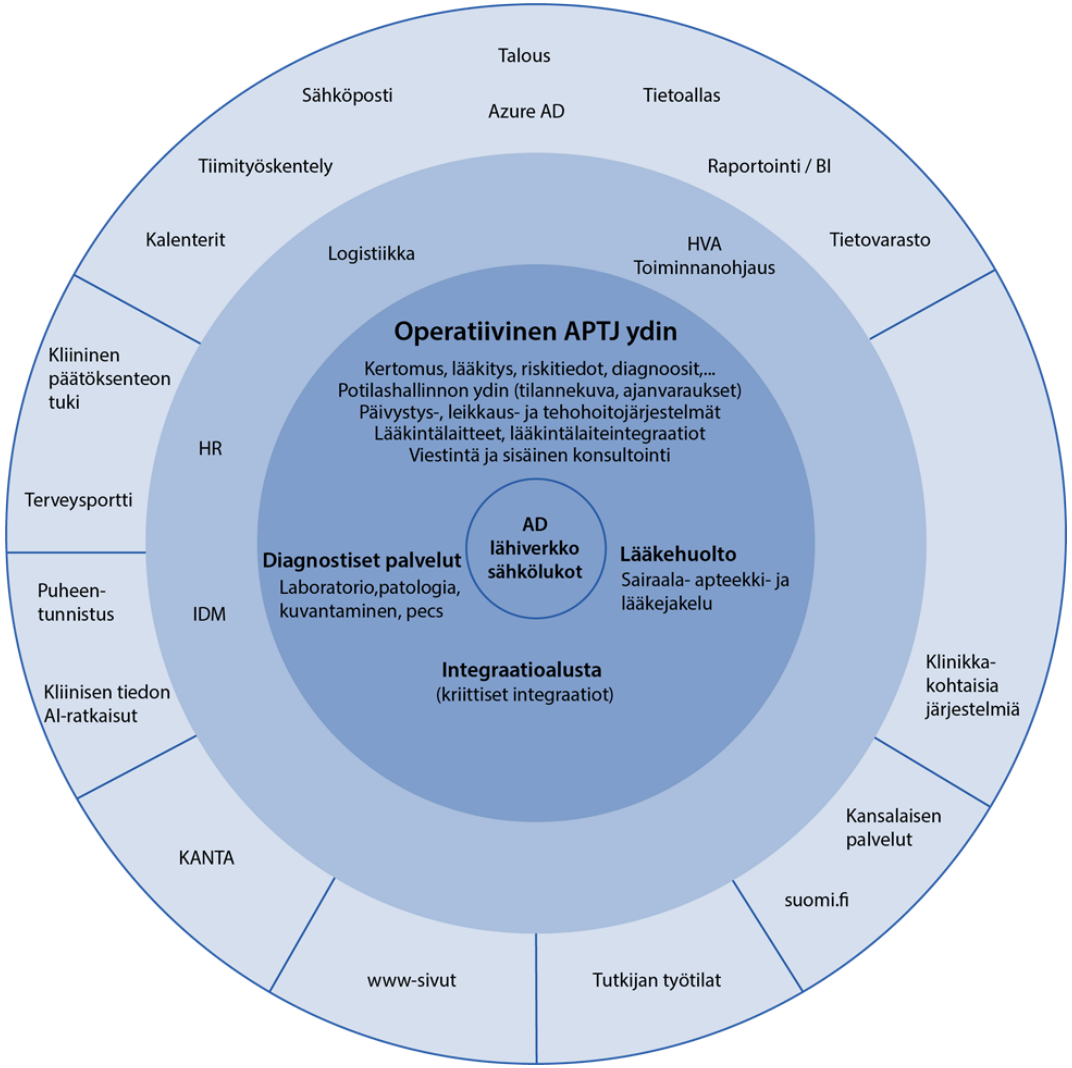
Pilvipalvelut huomioiva jatkuvuuden riskiskenaarioanalyysi

- **Visualisoidaan** pilvipalveluiden vaikutus jatkuvuudenhallintaan osana järjestelmäkokonaisuutta
- Skenaarioanalyysejä pohjautuen mm. **kansallisiin- ja alueellisiin riskiskenaarioihin**
- Sipulin kerrokset kuvaavat eri **tuotantosegmenttiä** (konesalit, pilvisijainnit)
- **Yksinkertaistettu** näkymä helpottaa kommunikointia ja työstämistä sidosryhmien kanssa

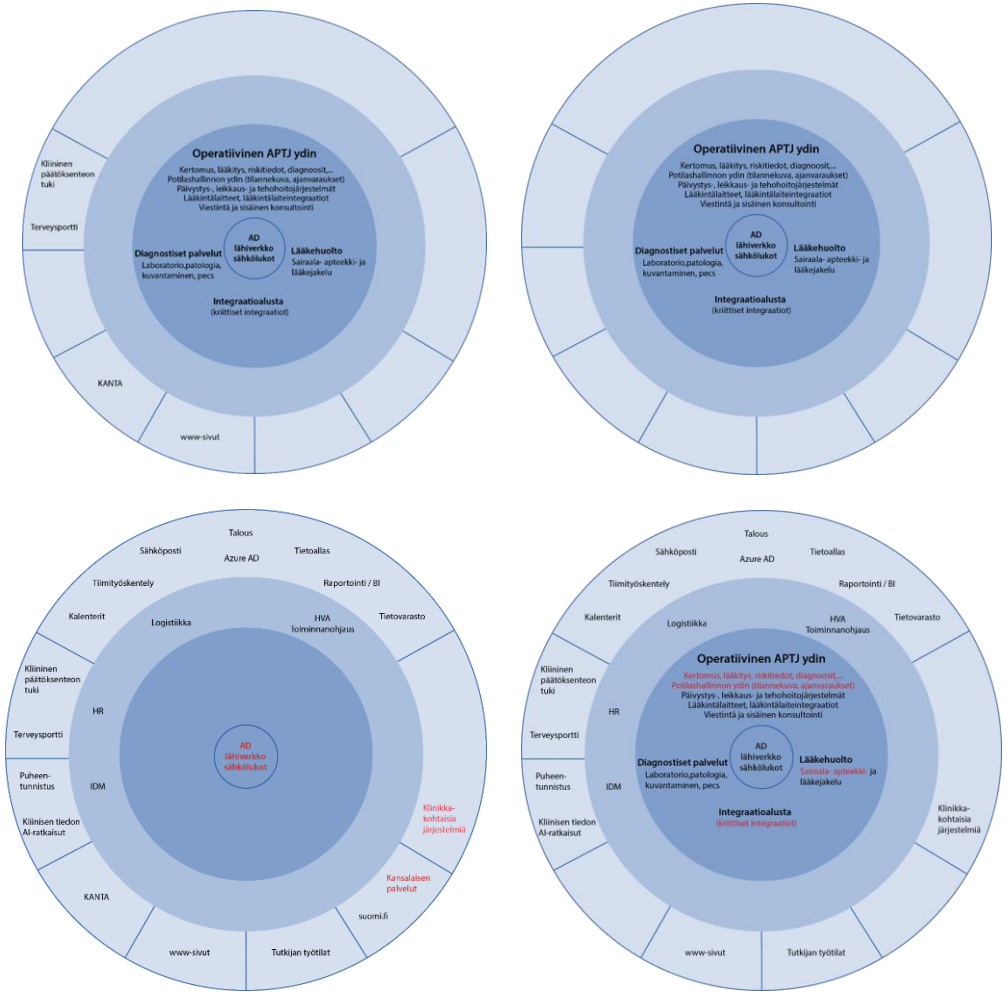


Sipulimallin käyttö

1. Organisaation palveluiden sijoittelu sipulimalliin



2. Skenaarioanalyysejä pohjautuen mm. kansallisiin- ja alueellisiin riskiskenaarioihin:



Ohjeen luku 6.3

Esimerkki

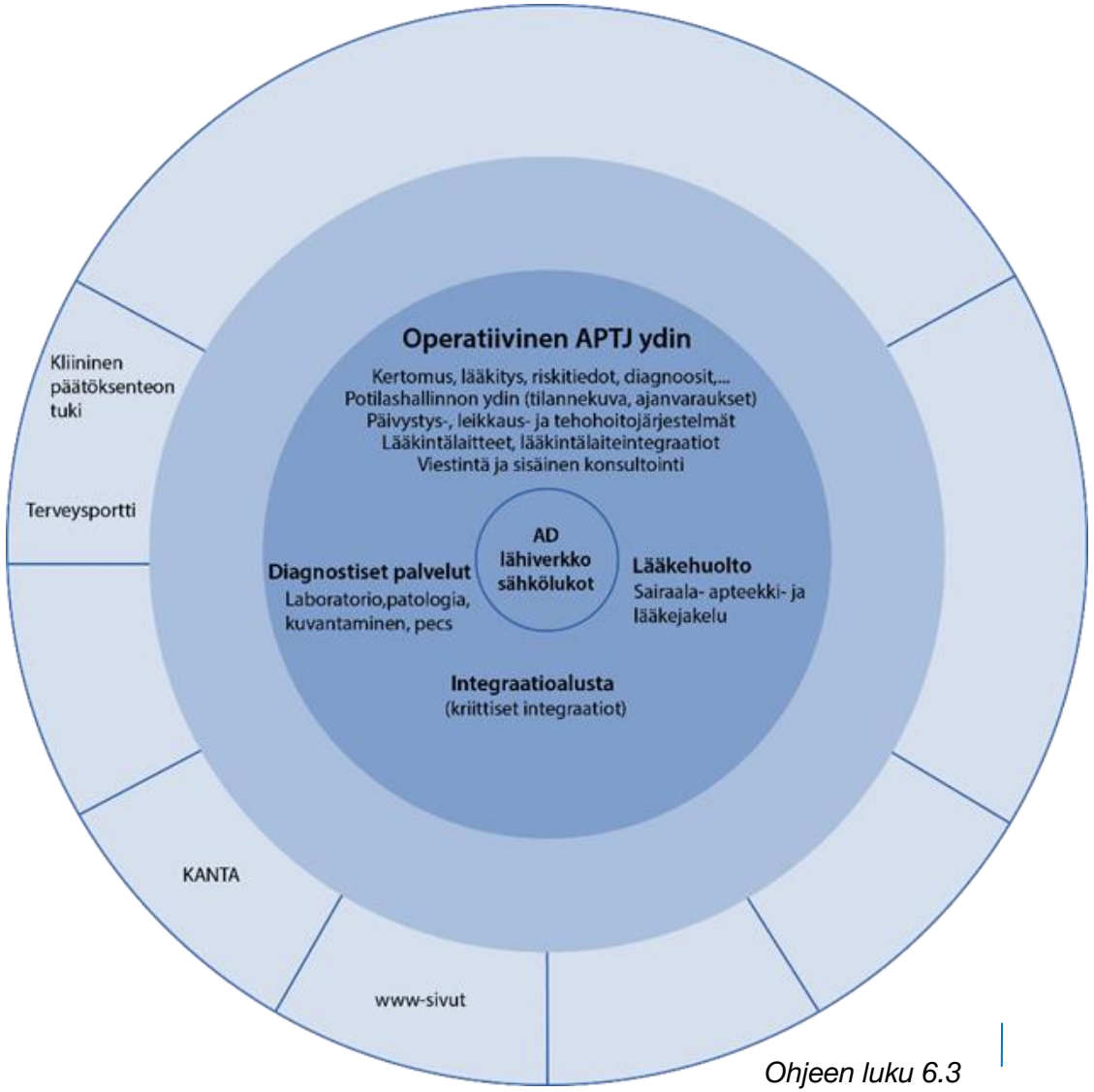
Skenaario 1: Verkkoyhteydet Suomeen ovat poikki

Skenaario

- Verkkoyhteydet Suomesta muualle Eurooppaan ovat katkenneet esim. terrori-iskun, kyberhyökkäyksen, teknisen häiriön tai vastaavan vuoksi.
- Otettava huomioon myös THL:n määräysten asettamien vaatimustenkin vuoksi.

Variaatio / työpöytätestaa

- Onko kriittisimmistä tiedoista ja/tai koko järjestelmästä mahdollista säilyttää kopiota Suomessa?
- Palvelutuotannon riippuvuus muiden organisaatioiden ulkomailla tuotetuista pilvipalveluista?
- Henkilökunnan siirto ulkomaille käyttämään järjestelmiä?



Ohjeen luku 6.3

Esimerkki

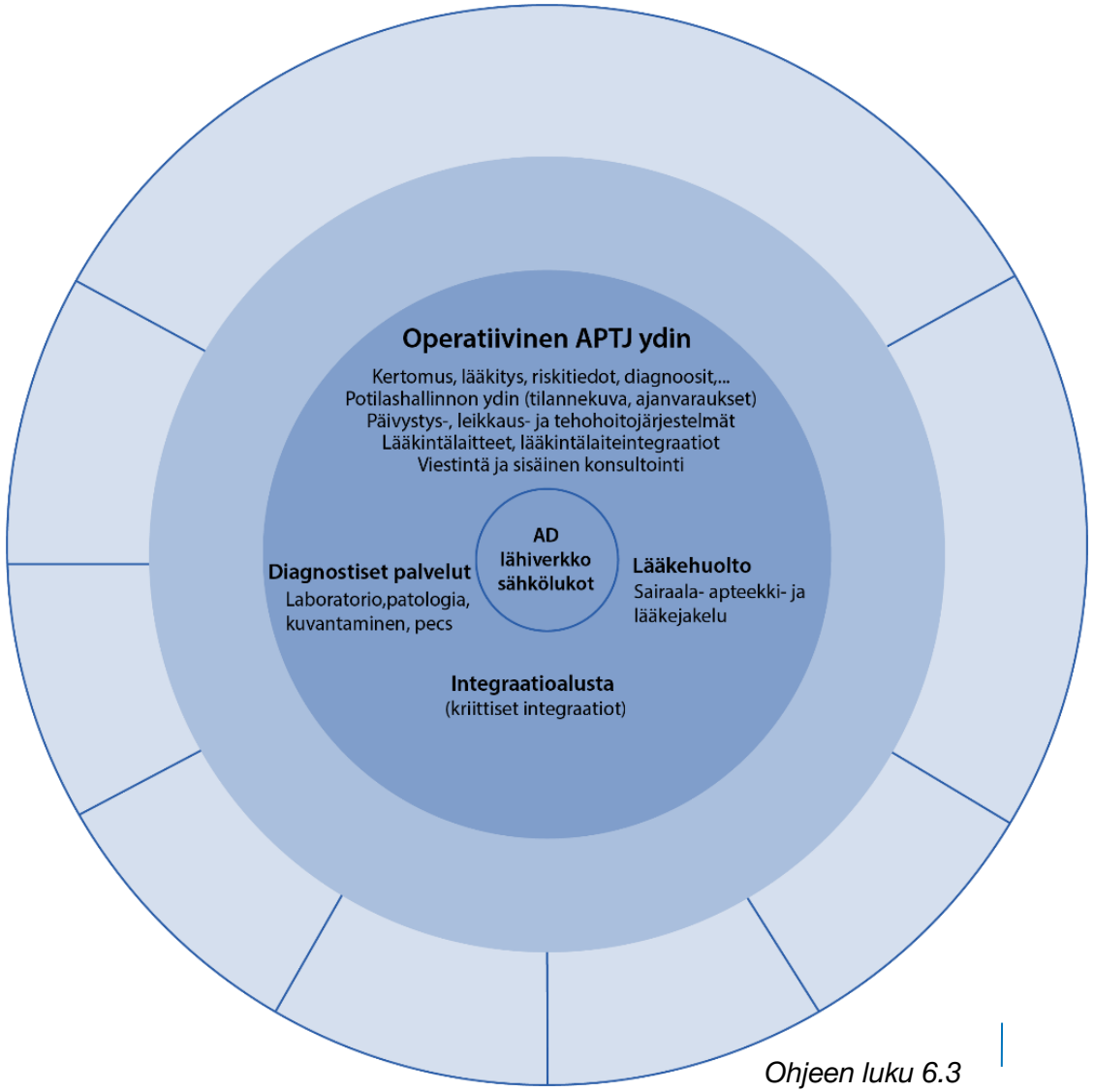
Skenaario 2: Sairaalan tietoliikenne on kokonaan poikki

Skenaario

- Sairaalan tietoliikenneyhteydet ulkomaailmaan ovat teknisen häiriö, kyberhyökkäyksen, terrori-iskun tai alueellinen sähkökatko vuoksi poikki.
- Teknisessä häiriössä esim. pääyhteys katkeaa samaan aikaan kun varayhteyttä huolletaan.

Variaatio / työpöytätestaa

1. Miten pärjätään ilman Kanta-yhteyttä? Tiedottamisen hoitaminen?
2. Voidaanko tietoliikennettä reitittää väliaikaisesti mobiiliverkon kautta? Voidaanko sitä kautta ohjata käyttäjät pilvessä olevan pilvipalveluiden käyttöön?
3. Osa esim. diagnostisista integraatioista / palveluista ei käytössä?
4. IDM, saadaanko keikkatyöntekijöille tunnuksia järjestelmään?
5. Variaatiossa vain osa verkkoyhteyksistä, esim. Internetin kautta tuotettavat SaaS-palvelut eivät toimi, mutta dedikoitu yhteydet pilvipalvelualustoihin toimivat.



Ohjeen luku 6.3

Esimerkki

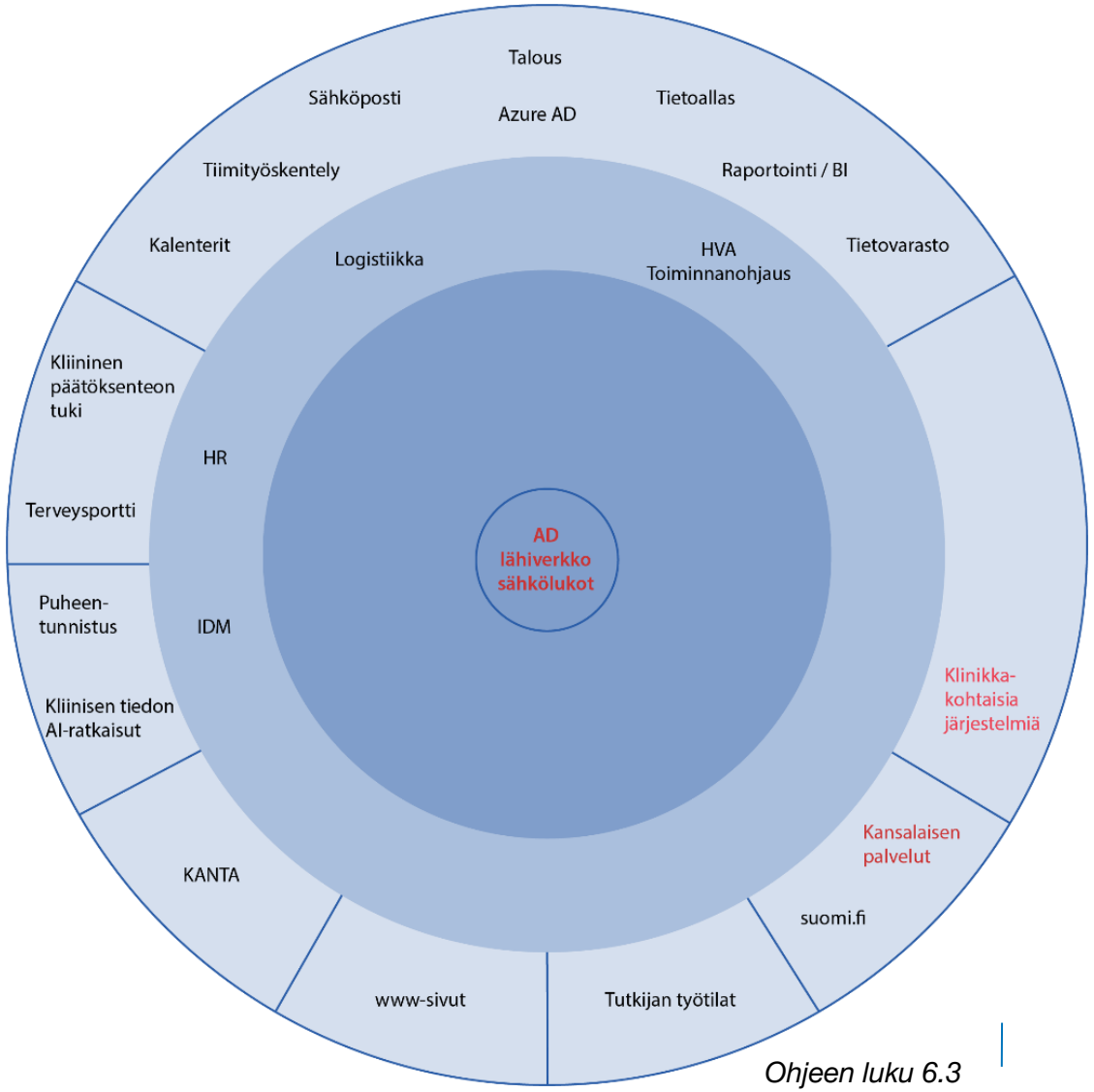
Skenaario 3: Lähikonesali ei käytettävissä

Skenaario

- Lähikonesalin laitteissa, ohjelmistoissa, virransyötössä tai verkkoyhteyksissä on tekninen vika tai on tapahtunut kyberhyökkäys, terrori-isku tai muu katastrofaalinen paikallinen ongelma.
- Havaitaan että pilvipalveluiden tuo hajautuminen myötä hyödyllistä vikasietoisuutta.

Variaatio / työpöytätestaa

1. Onko syytä varautua pilvipalveluiden käyttöön kännykkäliittymien avulla?
2. Voiko lähikonesalin järjestelmien vikasietoisuutta lisätä pilvikopiolla?
3. Onko sähköinen kulunhallinta tai sen ylläpito riippuvainen lähiverkosta?
4. Onko kansalaisen palvelut riippuvaisia lähikonesalin tiedoista?
5. Tukeutuuko pilvipalveluiden potilasvalinta lähikonesalin järjestelmiin?
6. Onko variaatioita, joissa osa lähikonesalin palveluista on käytössä?



Ohjeen luku 6.3

Esimerkki

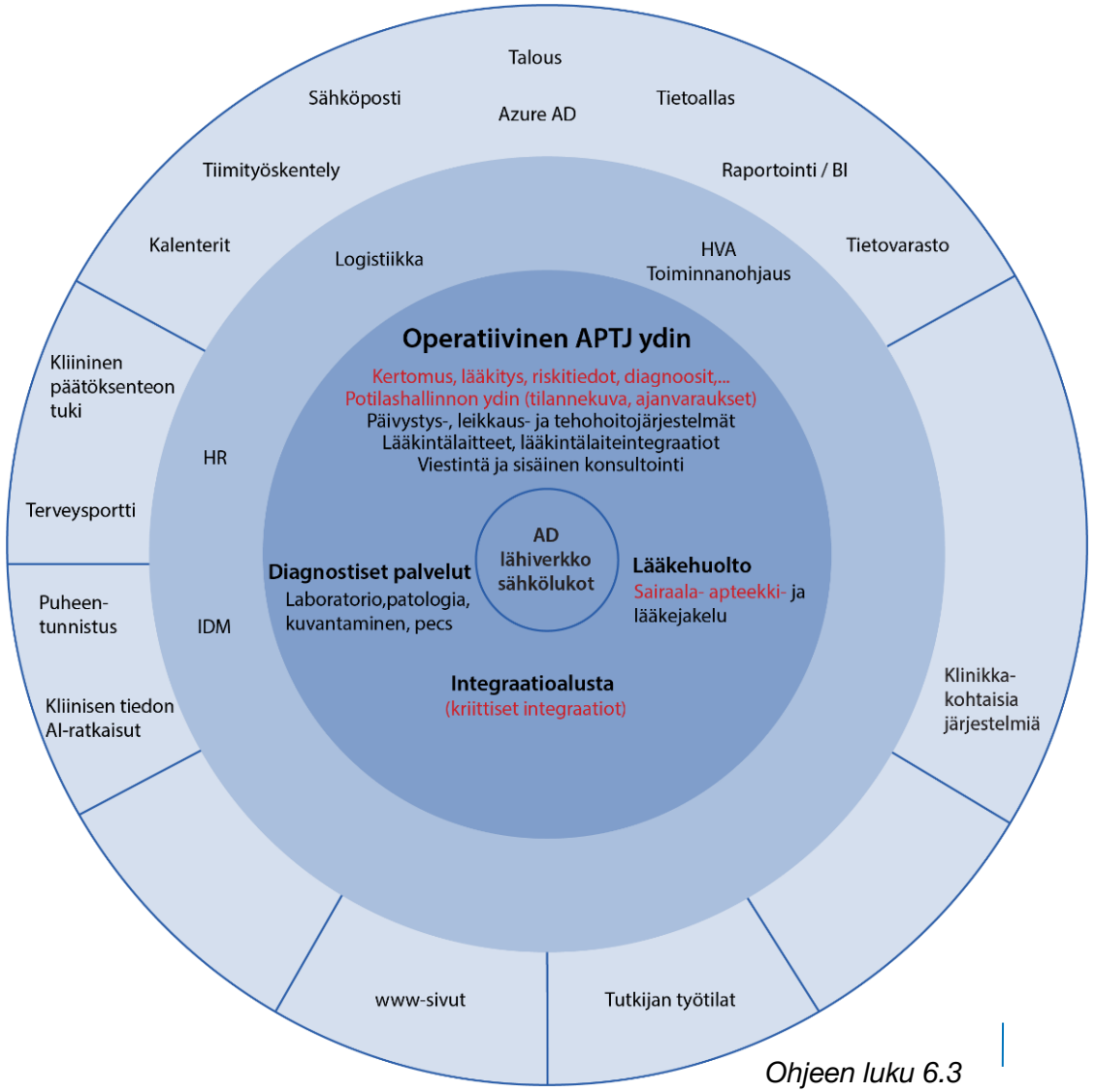
Skenaario 4: Kansalliset palvelut pois käytöstä

Skenaario

- Kansalliset palvelut kuten Kelan Kanta-palveluissa sekä Suomi.fi on käyttökatko esim. kyberhyökkäyksen, virransyötön ongelmien tai teknisten häiriöiden vuoksi. Tämä aiheuttaa kaikkiin Suomen APTJ järjestelmiin hitautta ja joihinkin käyttökatkoja, riippuen sovellusarkkitehtuurista.
- Suomi.fi palvelun käyttökatko vaikuttaa valtaosaan kansalaisten palveluista.

Variaatio / työpöytätestaa

1. Tunnistaako APTJ-järjestelmät Kantan ongelmatilanteet mukautuen tilanteeseen, vai hidasteleeko APTJ?
2. Tahdonilmaisut (luovutusluvat, luovutuskiellot ja hoitotahto) eivät ole käytettävissä
3. Riskitiedot eivät päivity Kannan kautta muilta palveluantajilta.
4. Jatkossa avolääkitys vain Kannassa? Voiko käydä niin että katkon aikana potilaiden ajantasaista lääkitystä ei ole kliinikoiden saatavilla?



Ohjeen luku 6.3

Soveltamisohjeessa esitetty järjestelmien kriittisyysluokittelu jatkuvuudenhallinnan kannalta

Hyödyntäminen:

1. Järjestelmien toiminnallisen kriittisyyden analysointi ja **tiedostaminen** organisaatiossa

2. Ei-toiminnalliset **vaatimusten asettaminen** järjestelmille kriittisyysluokittelun mukaisesti

Ohjeen luku 6.1 ja 6.2

Homma etenee

Kehitys kehittyy ja asiat selkenee

Tietoon perustuva eteneminen, arvolataukset tunnistaen

Ajankohtaiset haasteet ovat pääsääntöisesti sopimusteknisiä, ei teknisiä

Ajankohtaista

- Pilvikonesaleja pulpahtelee Suomeen
- Privacy shield 2.0 on toistaiseksi poliittinen päätös
- Parhaat käytännöt:
  - Valmiimmat yhteiset toimittajasopimusehdot julkishallinnolle, tietosuoja huomioiden
  - Kriteeristöjen, standardien ja käytännesääntöjen mukaisuus kehittyy
  - EU data boundary ja vastaavat, myös tukipalvelut
  - Varmenteiden hallinta puhuttaa yksittäisenä käytännön asiana
- ”Akuutista turvallisuusympäristön kehityksestä” opit?

Nordic Healthcare Group

perttu.poyhtari@salivirta.fi