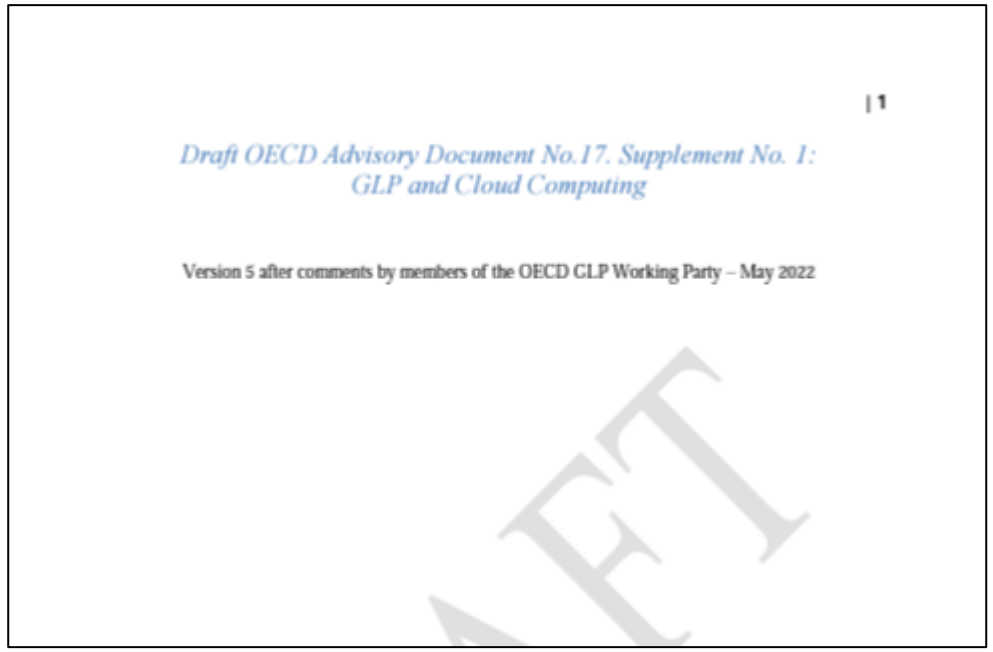
Draft OECD Advisory Document No.17. Supplement No. 1: **GLP and Cloud Computing**

30.3.2023

Lääkealan turvallisuus- ja kehittämiskeskus
Mirka Laavola
30.3.2023

Esityksen sisältö

- Pilvipalveluiden käyttöä GLP:ssä koskevan ohjeistuksen tilanne
- OECD ohjeluonnoksen No 17 Supplement 1 sisältö tässä vaiheessa
- Havaittuja puutteita pilvijärjestelmien hallinnassa



Ohjeen tilanne

https://www.oecd.org/env/ehs/testing/draft-advisory-doc-17-%20supplement-1-glp-cloud-computing.pdf

- Ohje täydentää ohjetta No. 17 ja tulisi soveltaa yhdessä sen kanssa
- Luonnos oli OECD:n sivuilla julkisilla kommenteilla elokuuhun 2022 asti
  - Vastaanotettiin yli 500 kommenttia toimijoiden puolelta
- Tämä versio on saatavilla oheisesta linkistä
- Korjattu luonnos oli viranomaisilla kommenteilla helmikuuhun 2023 asti
- Korjattu luonnos on hyväksytty julkaistavaksi OECD:n vuosikokouksessa maaliskuussa 2023
- Lopullinen versio voisi olla julkaistavissa kesällä 2023

Ohjeen rakenne

- Yleiskatsaus pilvipalveluista
- Pilvipalvelut GLP-ympäristössä
  - Vastuut
  - Vaatimukset
  - Pilviratkaisun toteutus
- Valvontaviranomaisten odotukset pilvipohjaisten ratkaisujen GLP-vaatimustenmukaisuudesta tarkastuksessa
  - Pilviratkaisun käyttöönotto
  - Pilvipalvelusovelluksen elinkaari
  - Elektroniset arkistot pilviratkaisussa

Pilvipalvelu tarkoittaa tietoteknisten palveluiden toimittamista tarvittaessa tyypillisesti internetin välityksellä. Ydinkäsite tarkoittaa tietoteknisen infrastruktuurin tai datakeskuksien omistamisen sijaan vuokraamista pilvipalvelun tarjoajalta.

Lääkealan turvallisuus- ja kehittämiskeskus
Mirka Laavola
30.3.2023

Termiä pilvipalveluiden tarjoaja voidaan dokumentissa käyttää sisäisestä tai ulkoisesta IT palveluntarjoajasta sekä isännöidystä palveluntarjoajasta tai toimittajasta

Lääkealan turvallisuus- ja kehittämiskeskus
Mirka Laavola
30.3.2023

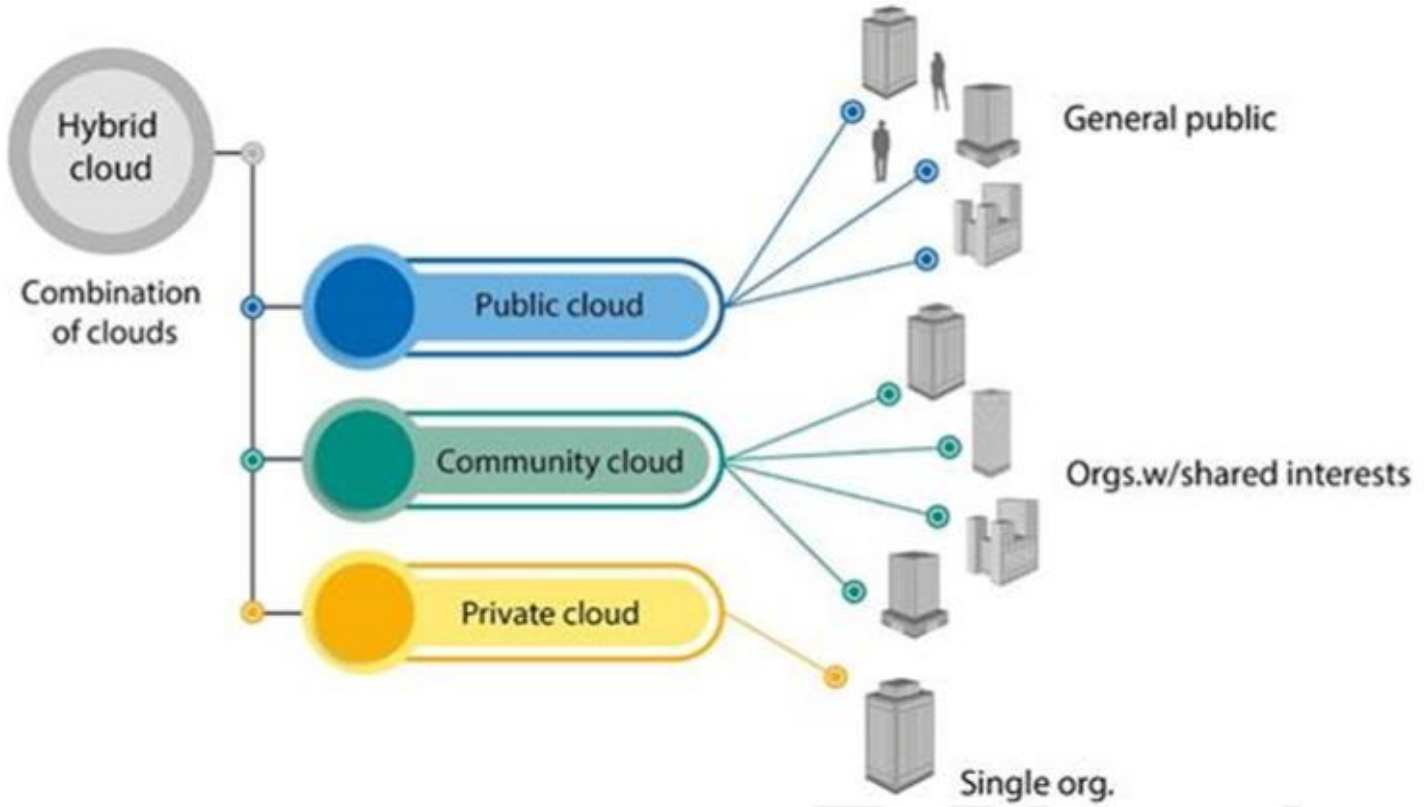
Käyttöönotto- ja palvelumallit

Figure 1. Cloud computing characteristics, deployment and service models

Source: FSI Insights on policy implementation No. 13, Regulating and supervising the clouds: emerging prudential approaches for insurance companies (Crisanto et al., 2018[5])

Käyttöönottomallit

Figure 2. Cloud computing characteristics, deployment and service models



Source: FSI Insights on policy implementation No. 13, Regulating and supervising the clouds: emerging prudential approaches for insurance companies (Crisanto et al., 2018[5]).

Vastuut TFM ja SD

- Test Facility Management (TFM) vastaa GLP:n noudattamisesta GLP-testauslaitoksessa ja toimintaa tukevissa järjestelmissä
- Jos IT-toiminnot siirretään paikallisesti ohjatuilta palvelimilta pilvipohjaiselle alustalle, on olennaista, että asianmukainen tieto, tietoisuus ja valvonta järjestelmistä ja käytännöistä säilyy testauslaitoksella ja asianmukaista valvontaa harjoitetaan
- Tutkimuksen johtajan tulee varmistaa, että tutkimuksissa käytetyt tietokonejärjestelmät (mukaan lukien virtualisoidut järjestelmät) on validoitu

Arkistonhoitajan vastuut

Jos GLP-arkistoja säilytetään pilvipohjaisessa ratkaisussa, arkistonhoitajan tulee varmistaa, että:

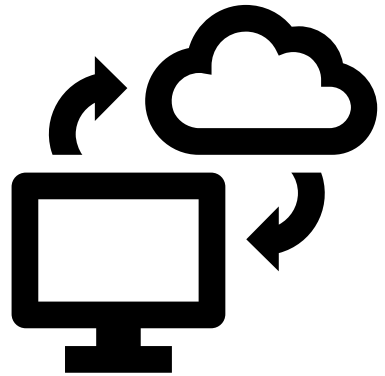
- arkistointiolosuhteet varmistavat arkistoitujen sähköisten asiakirjojen eheyden,
- pääsyä arkistoon valvotaan,
- indeksointijärjestelmä mahdollistaa asianmukaisen tallennuksen ja tietueiden hakemisen
- arkistoitujen sähköisten asiakirjojen liikkumista valvotaan ja dokumentoidaan asianmukaisesti,
- toteutetaan prosessi määräajoin luettavuuden tarkistuksia varten

Vaatimukset OECD Dokumenteissa No 1, No 15 ja No 17

	Traditional IT (*)	GLP Principles requirements	Cloud service models		
			IaaS	PaaS	SaaS
Computing resources					
Raw Data (including metadata)		1.2.2.f, 1.4.3, 8.3.5			
Data generation					
Data classification and accountability					
Protection					
User access management					
Encryption					
Metadata, audit trail generation and management					
Physical security measures		1.2.2.i			

- Vaalean harmaa = testauslaitoksen vastuulla
- Harmaa = jaettu vastuu testauslaitoksen ja alihankkijan kanssa (määriteltävä)
- Tumma harmaa = palvelun toimittajan vastuulla

	Traditional IT (*)	GLP Principles requirements	Cloud service models		
			IaaS	PaaS	SaaS
Computing resources					
Applications and software		1.1.2.b, 1.1.2.q, 1.2.2.g, 4.1			
Application level controls (access, rights)					
Physical security measures					
Runtime (data bases)		1.1.2.q			
Middleware (interface between applications)		1.1.2.q			
Operating systems (Windows, Linux,..)		1.1.2.b			
Virtualisation		1.1.2.b			
Servers (account, application and data servers)		1.1.2.b, 3.1.1			
Storage		1.1.2.b, 1.2.2.i, 3.1.1			



	Traditional IT (*)	GLP Principles requirements	Cloud service models		
			IaaS	PaaS	SaaS
Computing resources					
Archiving		1.1.2.l, 1.1.2.q, 3.4, 9.2.7, 10			
Host infrastructure					
Physical security measures					
Networking (web browser, web server)		1.1.2.b			
Network control					
IT Personnel		1.1.2.b,c,d, 1.4.1			
Computerised systems Validation		1.1.2.q, 1.2.2.g			
Quality Assurance (QA)		1.1.2.f, 2.1.1, 2.1.2			

- Kaikesta alihankinnasta on oltava kirjalliset sopimukset, jossa vastuut on kuvattu!

Toteutus

Kun pilvipalveluita käytetään tarjoamaan, asentamaan, konfiguroimaan, integroimaan, ylläpitämään, muokkaamaan tai säilyttämään tietokoneistettua järjestelmää tai siihen liittyvää palvelua tai tietojenkäsittelyä, on GLP-vaatimusten mukaisuuden edellytyksenä:

- Yksityiskohtainen riskiarviointi (sisältäen pilviratkaisun määrittelyn)
- Pilvipohjaisen ratkaisun validointi
- Pilvipalveluntarjoajan perusteellinen arviointi
- Selkeästi määritellyt palvelusopimukset (SLA Service Level Agreement), määriteltynä toiminnot ja tarjottavat palvelut

Riskiarviointi

Arvioitaviin riskeihin kuuluvat esimerkiksi:

- Järjestelmän toiminnot (mukaan lukien järjestelmän rajoitukset)
- Laitteet ja sovellukset: käytössä oleva infrastruktuuri, verkko/alusta, sovellukset
- GLP kompliansi:
  - Uusi tiedon siirtoprosessi ja muutokset nykyisestä järjestelmästä, erityisesti tiedon siirron vaiheet tulee tunnistaa ja kuvata huolellisesti
  - Datan laatuun liittyvät riskit: datan keruu, luonti tai analysointi (datan luotettavuus, järjestelmän saatavuus, varmuuskopiointisuunnitelmat)

Riskiarviointi

GLP komplianssi:

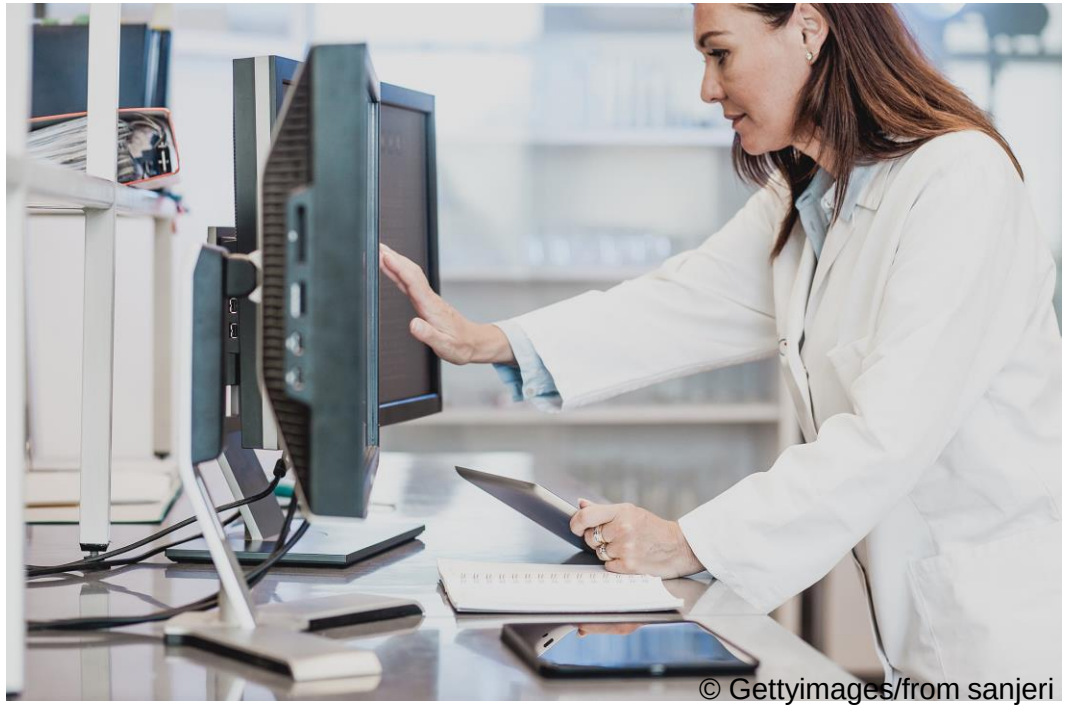
- Uudet riskit tietojen eheydelle (data integrity):
  - Etäkäytön turvallisuus
  - Tietojen suojauksen taso
  - Fyysinen turvallisuus (palvelinten sijainti ja turvallisuus)
  - Vaikutukset järjestelmän arkkitehtuuriin (testauslaitos ja palveluntuottaja), organisaatio ja valittu palvelumalli
  - Vaikutukset tiedon omistajuuteen
  - Vaikutukset testauslaitoksen henkilöstöön ja osaamiseen

Riskiarviointi

- Riskien vähentämistoimet (risk mitigation):
  - Riittävät kontrollit tiedon laadun ylläpitämiseksi (tiedon eheyden verifiointi tai datan katselmointi)
  - Audit trail
- Palvelun tuottajan valintakriteerit: vaaditut laatustandardit, jatkuvuussuunnitelmat, palautukset (disaster recovery)
- Suunnitelma tietojen siirtämiseksi palvelun päättyessä
- Arkistointi (jos tarpeen)

Käyttöönottosuunnitelma

- Riskiarvioinnin jälkeen kun tekninen ratkaisu on valittu, tulee laatia käyttöönottosuunnitelma
- Tarkempia tietoja suunnitelman sisällöstä on listattu ohjeessa


© Gettyimages/from sanjeri

Validointi

- Vain validoituja järjestelmiä tulee käyttää GLP-ympäristössä
- Kaikki järjestelmä validoinnin/kvalifioinnin vaatimukset tulee täyttyä
- Validointivastuu on testauslaitoksella
- Validoinnin laajuus tulee perustua järjestelmän riskiarviointiin
- Validointi tulisi tehdä testauslaitoksen toimesta, mutta siinä voi luottaa järjestelmän toimittajan kvalifiointeihin osittain
    - Käyttäjävaatimus tulee laatia, ymmärtää mitä pitää kvalifioida (sovellus) ja validoida (prosessi), kuka vastaa, että vaatimukset täyttyvät
    - Jos luotetaan toimittajan kvalifiointiin tulee dokumentaatio arvioida testauslaitoksen toimesta

Esimerkki SaaS validoinnista

- Asennuksen kvalifiointi (IQ) ja toiminnan kvalifiointi (OQ) sekä toimintaohjeet järjestelmän elinkaaren hallintaan voivat tulla toimittajalta, mutta testivaiheiden lopullinen hyväksyntä on testauslaitoksen vastuulla
- Suorituskyvyn(PQ) ja käyttäjien koulutus ja käyttöohjeiden laatiminen on testauslaitoksen vastuulla

Pilvipalveluiden toimittajan arviointi

- Toimittajan pätevyys ja luotettavuus ovat arvioinnin päätekijöitä
- Toimittajan auditointitarve on perustuttava dokumentoituun riskiarvioon, mutta on riskiperusteista
- Kun alihankitaan pilvipalveluita, on perimmäinen vastuu GLP-yhteensopivuuden osoittamisesta testauslaitoksella
- Arvioitava millainen laatujärjestelmä toimittajalla on
- Mahdolliset laatusertifikaatit voi ottaa huomioon arvioinnissa, arvioitava sopivatko mahdolliset laatusertifikaatit GLP-vaatimusten mukaisuuden tukemiseen
- Testauslaitos voi myös ulkoistaa pilvipalvelun arvioinnin ulkopuoliselle asiantuntijalle, mutta laadunvarmistuksen on arvioitava tämän asianmukaisuus

Pilvipalveluiden toimittajan arviointi

- Toimittajan vastuulla on, että henkilöstön osaamisesta on dokumentoitua näytöä
  - Toimenkuvat, CVt, täydennyskoulutusta IT-asioista
- GLP-tietoisuuskoulutus voi olla osa riskienhallintastrategiaa, jotta palvelun tarjoajat tietävät vaatimukset joille palvelua tuotetaan
- Arvioitavia kokonaisuuksia mm.
  - Dokumentaatio
  - Raakadatan määrittely
  - Tietojen eheyden ymmärtäminen ja politiikka.
  - Varmuuskopiointi ja palautus.
  - Sähköisten tietojen arkistointi.
  - Sähköisten tietojen omistus- ja käyttöoikeudet.

Palvelutasosopimus (SLA)

- Kirjalliset sopimukset tulee olla, joissa kuvataan kaikki yhteistyön näkökohdat
  - Vastuut ja mahdolliset kolmannet osapuolet tai alihankkijat tulee kuvata sopimuksissa
  - Sisältönä mm. vastuut ja velvollisuudet, turvallisuus, dokumentointi, arkistointi, koulutus, viestintä, raportointilinjat, auditoinnit, validointi, toiminta sopimuksen päättyessä

Johtopäätökset

- Pilvipohjaisen ratkaisun käyttöönotto ei saisi vaarantaa GLP-toimintojen noudattamista
- Laatu ja tiedon eheys tutkimuksen rekonstruoimiseen tulee olla edelleen mahdollista
- GLP-tarkastajat odottavat todisteita, jotka osoittavat, että testauslaitoksen johto pystyy osoittamaan vastuunsa siitä, että toteutettu pilvipalvelu on GLP-vaatimusten mukainen ja testauslaitoksella on riittävät keinot valvoa vaatimusten toteutumista

Odotukset GLP-tarkastuksilla

- Kriittisten GLP-järjestelmien tulee olla kvalifioituja ja validoituja ja niitä tulee käyttää tavalla, joka varmistaa GLP-tietojen tuloksen ja eheyden riippumatta siitä, onko ne asennettu paikallisesti tai pilvipalveluna
- Pilvipalveluiden käyttöönoton dokumentaatio
  - Toteutettujen järjestelmien tiedot
  - Dokumentoidut valintaperusteet
  - Tiedon laatua ja eheyttä kuvaava riskiarviointi
  - Dokumentoitu arviointi, että kvalifiointitoimet ovat olleet riittävät palveluntoimittajan osalta (voi perustua saatavilla olleeseen dokumentaatioon toimittajalta tai esim. auditointiin paikan päällä)
  - Dokumentaatio testauslaitoksen tekemistä riskiperusteisesti valituista lisävalidointitoimista
  - Sopimukset

Odotukset GLP-tarkastuksilla

- Järjestelmän elinkaaren aikana (validin tilan ylläpito)
  - Järjestelmän saatavuus, ylläpito, päivitykset, liiketoiminnan jatkuvuus (continuity plan), katastrofisuunnitelma (disaster plan) ja tietojen siirron suunnitelma (migraatio)
  - Varmuus tietojen eheydestä ja laadusta
  - Suunnitelma testauslaitoksen toteuttamista valvontatoimista
  - Dokumentaatio käyttäjätiedoista (pääsy ja todennus)

Odotukset GLP-tarkastuksilla

- Sähköinen arkistointi
  - Pilvipalveluntarjoajat voivat toimia sopimusarkistona
  - Kansallisesta lainsäädännön eroista johtuen GLP-arkistot voivat olla erillisia GLP-testauslaitoksia tai niitä tarkastetaan testauslaitoksen tarkastuksen yhteydessä
  - Palvelintilojen fyysinen turvallisuus
  - Arkiston valvonta: kulunvalvonta, inventaario, tietojen oltava indeksoitua säännöllistä tallennusta varten, tietueiden haettavuus, tallenteen eheys ja jäljitettävyys raakatiedoista loppuraporttiin

Pilvipalveluista muissa GxP-ohjeistoissa

- Guideline on computerised systems and electronic data in clinical trials
  - GCP puolella uusi ohje hyväksytty 7.3.2023, tulee voimaan 6 kk:n kuluttua hyväksymisestä
  - Kappale 6.7 Cloud solutions
- Concept Paper on the revision of Annex 11 of the guidelines on Good Manufacturing Practice for medicinal products – Computerised Systems
  - GMP puolella IT-ohje Annex 11 on päivityksessä, aiotuissa muutoksissa kuvataan myös pilvipalveluiden käytön ohjeistus
  - Ensimmäinen luonnos odotettavissa joulukuussa 2024

Esimerkkejä havaituista puutteista

- Yleisesti toimittaja-arviointien puuttuminen ja dokumenttien saatavuus
  - Siirretty esim. tutkimusdataa google cloudiin ilman minkäänlaista arviointia
- Ei ole sisäisiä/riippumattomia kontrolleja datalle
  - Pitäisi esim. tarkastaa, että arkistoitu data on säilynyt samana, eikä sitä ole modifioitu esim. ylläpitäjän toimesta
  - Tai voidaan rakentaa kontrolleja, esim. ilmoitus kun joku on muokannut tiedostoja tms.