Tiedon eheys

OECD Series of Principles: Number 22

Advisory Document of the Working Party on Good Laboratory Practice on

GLP Data Integrity

2.12.2021

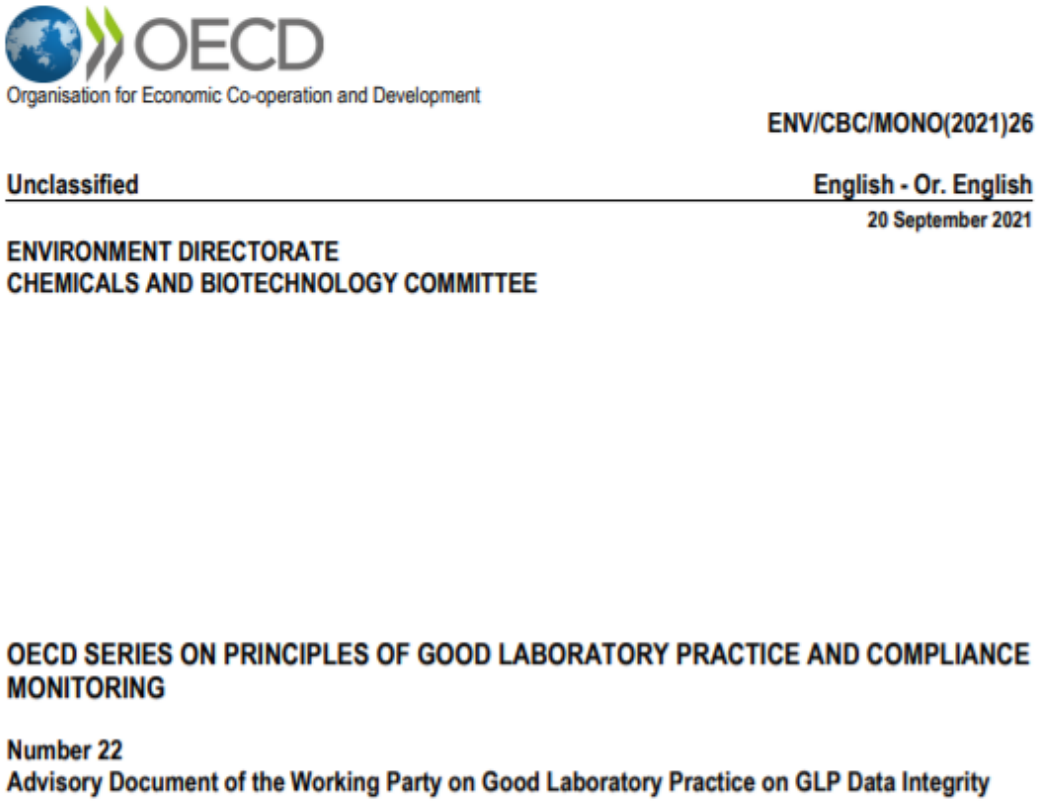
Lääkealan turvallisuus- ja kehittämiskeskus
Mirka Laavola
2.12.2021

Sisältö

- Tiedon eheys (Data integrity)
- OECD ohjeen No 22 sisältö
- Esimerkkejä tiedon eheyteen liittyvistä tarkastushavainnoista

Uusi ohje

- OECD julkaisi 20.9.2021 uuden ohjeen tiedon eheydestä
- Number 22: Advisory Document of the Working Party on Good Laboratory Practice on **GLP Data Integrity**
- **https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=env/cbc/mono(2021)26&doclanguage=en**



OECD
Organisation for Economic Co-operation and Development

ENV/CBC/MONO(2021)26

Unclassified

English - Or. English

20 September 2021

ENVIRONMENT DIRECTORATE
CHEMICALS AND BIOTECHNOLOGY COMMITTEE

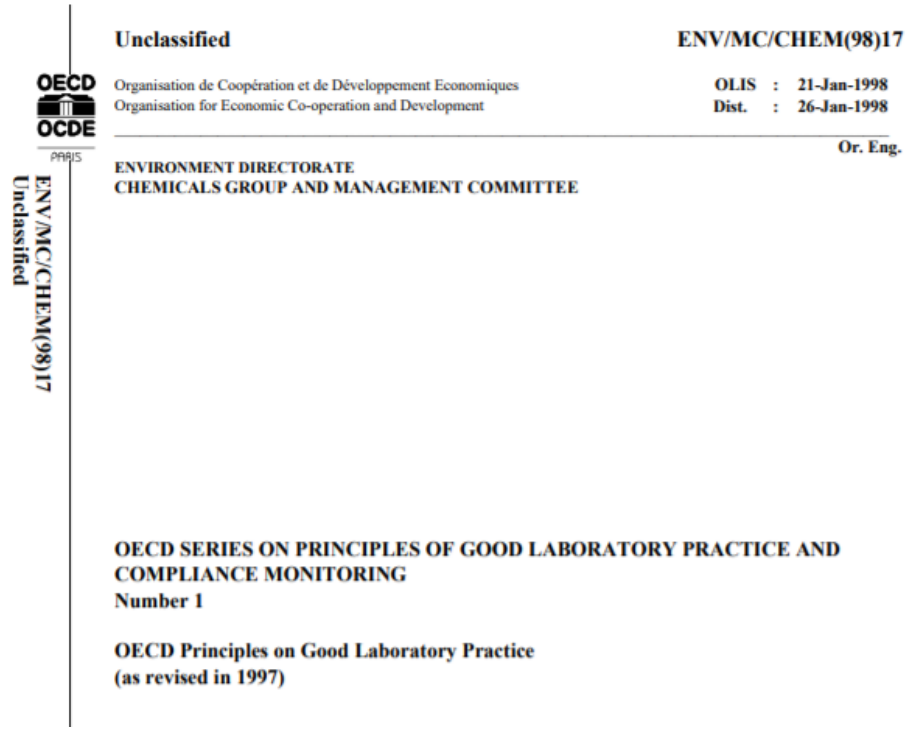
OECD SERIES ON PRINCIPLES OF GOOD LABORATORY PRACTICE AND COMPLIANCE MONITORING

Number 22
Advisory Document of the Working Party on Good Laboratory Practice on GLP Data Integrity

Tiedon eheys

Uusi ohje viittaa GLP Principles dokumentin seuraaviin kohtiin tiedon eheyteen liittyen:

Section II: 1.1.2.b-e, 1.1.2.l, 1.1.2.q, 1.2.2.f, 1.2.2.g, 1.2.2.i, 1.4.3, 2.1.1.c, 3.4, 7.1, 7.4.3, 8.2.6, 8.3.3, 8.3.4, 8.3.5, 10.1



Unclassified ENV/MC/CHEM(98)17

OECD OCDE PARIS

Organisation de Coopération et de Développement Economiques
Organisation for Economic Co-operation and Development

OLIS : 21-Jan-1998
Dist. : 26-Jan-1998

Or. Eng.

ENVIRONMENT DIRECTORATE
CHEMICALS GROUP AND MANAGEMENT COMMITTEE

Unclassified ENV/MC/CHEM(98)17

OECD SERIES ON PRINCIPLES OF GOOD LABORATORY PRACTICE AND COMPLIANCE MONITORING
Number 1

OECD Principles on Good Laboratory Practice
(as revised in 1997)

Tiedon eheyden vaatimukset (ALCOA)

- **A**ttributable “jonkun syyksi/ansioksi luettava”(tiedon tulee olla jäljitettävissä tekijään)
- **L**egible “luettava” (tiedon pitää olla luettavissa)
- **C**ontemporaneous “samanaikainen”
- **O**riginal “alkuperäinen” (tieto on alkuperäisessä muodossa missä se luotiin tai verifioituna kopiona, jossa kaikki alkuperäinen tieto on olemassa)
- **A**ccurate “täsmällinen” (tieto on todellista ja vastaa tehtyä mittausta tai toimintoa)

ALCOA+ periaatteet (CCEA)

- **C**omplete ”täydellinen” (tieto sisältää kaiken kriittisen tiedon, jotta tapahtuma voidaan luoda uudelleen, elektroninen data sisältää myös metadatan)
- **C**onsistent ”jatkuva, yhtenäinen” (hyvät dokumentaatiotavat kattavat koko prosessin, kaikki muutokset on tallennettava)
- **E**nduring ”pysyvä” (tallenteet/dokumentit säilytetään vahingoittumattomana ja saatavilla koko säilytysajan)
- **A**vailable ”saatavilla” (tallenteiden/dokumenttien tulee olla saatavilla luettavassa muodossa katselmointia varten koko säilytysajan)

GLP vastuut tiedon luonnista arkistointiin asti

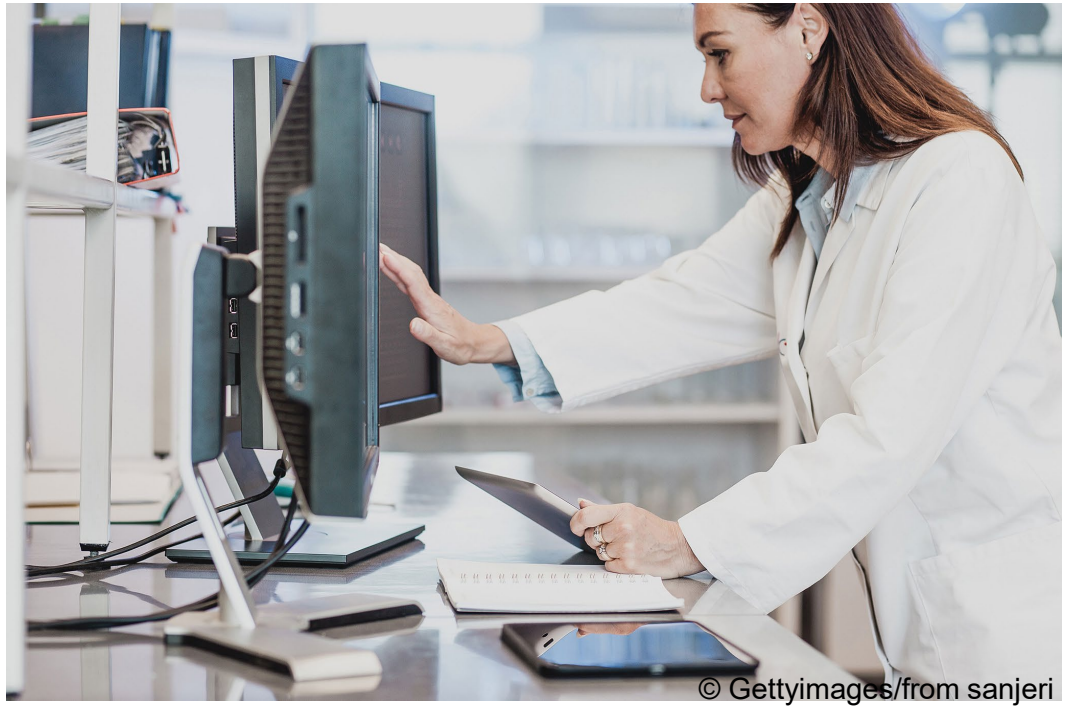
- Study Personnel:
  - Tiedon kirjaaminen/tallentaminen viipymättä ja tarkasti
- Study Director:
  - Kaikki raakadata on dokumentoitu
  - Tutkimuksessa käytetyt tietojärjestelmät on validoitu huomioiden tiedon eheyden vaatimukset
  - Tutkimuksen päättyessä tutkimussuunnitelma, loppuraportti, raakadata, tutkimusta tukevat materiaalit on arkistoitu niin, että tutkimus voidaan rekonstruoida tarvittaessa

GLP vastuut tiedon luonnista arkistointiin asti

- Archivist:
  - vastaa arkistoinnin hallinnasta, toiminnasta ja menettelytavoista (sähköinen ja fyysinen säilytys)
- Test Facility Management:
  - varmistaa resurssit tietojen hallinnan varmistamiseksi
  - huolehtii henkilökunnan pätevyydestä ja koulutuksesta (mukaanlukien tietojen eheys)
  - varmistaa, että saatavilla on voimassa olevat toimintaohjeet ja niitä noudatetaan
  - varmistaa, että on osoitettu arkistonhoitajat sekä paperi että sähköisen tiedon arkistoinnille
  - luo menettelyt, joilla varmistetaan tietojärjestelmien soveltuvuus käyttötarkoitukseensa, validointi ja ylläpito tiedon eheydestä huolehtien
  - käyttöönotetut tietojärjestelmät vastaavat viranomaisvaatimuksia
  - varmistaa, että tietojen eheyteen liittyvät jäännösriskit tunnistetaan ja niitä vähennetään

GLP vastuut tiedon luonnista arkistointiin asti

- QA:
  - suorittaa tarkastuksia määrittääkseen, että kaikki tutkimukset suoritetaan GLP:n periaatteiden mukaisesti
  - sisältää tiedonkeruun, tiedonkeruujärjestelmät, toteutetut tiedonhallintatoimenpiteet ja niihin liittyvät SOP:t



Tiedon hallinta

- Tietojen hallinnan tulee olla suunnitelmallista toimintaa koko tiedon elinkaaren ajan
- Sen tulee sisältää valvontaa, prosesseja/järjestelmiä tietojen eheysvaatimusten noudattamiseksi sekä muutosten hallintaa
- Tietohallintojärjestelmien tulisi varmistaa, että tiedot ovat helposti saatavilla
- Sähköisen tiedon tulee olla saatavilla ihmisen luettavassa muodossa
- Testauslaitosten tulee olla tietoisia siitä, että asianmukainen tietojen eheyden valvonta on tarpeen tietokoneistettuihin järjestelmiin sekä paperipohjaisiin manuaalisiin järjestelmiin, vaikka valvonnan keinot eivät välttämättä ole samat

Tiedon hallinta

- Työympäristön tulisi olla tiedon hallinnan osalta mahdollisimman läpinäkyvä ja kannustaa aktiivisesti raportoimaan virheistä, puutteista ja poikkeavista tuloksista
- Tulee käyttää riskiperusteista lähestymistapaa. Tunnistettava riskit tiedon eheydelle ja minimoitava jäännösriskit.
- Tietoihin liittyviä riskejä voi arvioida sen perusteella kuinka helppo ne on poistaa tai muuttaa tarkoituksellisesti tai tahattomasti. Kuinka helposti poistaminen tai muuttaminen on havaittavissa.
  - Mikä on tietojen muuttumisen tai poistamisen vaikutus tutkimusdataan?

Riskiarviointi

- Monialainen asiantuntijaryhmä (tutkimus, IT, laadunvarmistus) laatii tiedon eheyden riskiarvioinnin
  - Huomioitavia asioita järjestelmiä arvioitaessa ovat toiminnot, prosessit, rajapinnat muihin järjestelmiin, vaatimukset, ihmisen puuttuminen, koulutus ja laatujärjestelmät
  - Automatisointi tai validoidun järjestelmän käyttäminen voi pienentää riskiä, mutta ei poista sitä. Valvontaa tulee olla, ei voi luottaa vain validoituun järjestelmään mikäli käyttäjä vastaa esim. tiedon tallentamisesta.
- Tunnistetut riskit tulee priorisoida huomioiden vaikutukset tutkimusdatalle ja riskiarviointi katselmoida säännöllisesti

Manuaalinen tietojen syöttö

- Manuaalinen tieto syötetään samanaikaisesti työn tekemisen kanssa
- Kriittisen tiedon valvontakeinoja voivat olla, samanaikainen toisen henkilön tietojen syöttämisen varmentaminen tai asiaan liittyvien tietojen ristiintarkistus lähteistä (esimerkiksi laitepäiväkirjat, testijärjestelmän tiedot jne.) tai tietojen tarkastus jälkikäteen
- Kirjoittajan käyttö tekijän henkilön puolesta voi olla perusteltua joissakin tilanteissa esim. tutkimushenkilön työskennellessä aseptisissa olosuhteissa (kirjaaminen kontaminaatioriski). Tällöin molempien tekijän ja kirjaajan tiedot tulee kirjata tutkimusdokumentaatioon.

Manuaalinen tietojen syöttö

- Raakatiedon syöttämiseen käytettyjen lomakkeiden tulisi olla saatavilla missä toiminta tapahtuu, jotta tieto voidaan tallentaa välittömästi
- Tyhjien paperilomakkeiden käyttöä raakadatan tallentamiseen olisi rajoitettava ja valvottava
- Lomaketulosteiden määrää tulee hallita tietojen eheysongelmien välttämiseksi, kuten tietueen uudelleen luomisen tai kopion havaitsemiseksi
- Kontrollointi on riskiperusteista ja tilanteet joissa kontrollia ei ole tulee olla perusteltuja
- Kontrollointina voi toimia esim. lomakkeiden saannon seuranta, etukäteisnumerointi, tulostusoikeuksien rajaaminen

Tiedon syöttö

- Suorana tietokonesyötteenä luodut tiedot olisi tunnistettava tietojen syöttöhetkellä (kuka, koska ja mitä)
- Käyttöoikeuksien tulee estää luvaton tietojen syöttäminen
- Järjestelmän pääkäyttäjien (system admin) määrä tulee olla rajattu
- Automaattista tietojen syöttöä voi hyödyntää kun järjestelmät ovat validoituja esim. ID-kortin lukija, viivakoodinlukija

Flat files

- "Flat file" sisältää vain siirrettävän datan sekä mahdolliset rivitarkenteet ja erotinmerkit. Aineiston rakenne on kuvattu erillisessä metatiedostossa, jonka perusteella vastaanottaja pilkkoo aineiston haluttuun rakenteeseen.
- Ongelmana, että tiedostot eivät mahdollista tallentavan henkilön jäljitettävyyttä eivätkä päivämäärä ja kellonaikatietoja. Joissakin flats-tiedostoissa voi olla perussisällönkuvaustietoja kuten tiedoston luonti ja viimeisimmän muutoksen päivämäärä, mutta ne eivät tarjoa riittävää tietojen jäljitettävyyttä (audit trail)
- Ei yleensä tulisi käyttää suoraan tiedonkeruuhun tai raakatietojen tallentamiseen
- Jos käyttö on välttämätöntä, tulee olla riskienhallintakeinot esim. tekninen tiedoston muuttamisen estäminen, salaus tms.

Elektroninen allekirjoitus

- Lisätty kuva allekirjoituksesta tai alaviite, joka osoittaa, että asiakirja on ollut sähköisesti allekirjoitettu ei riitä
- Sähköisen allekirjoituksen tulee olla yksilöitävissä ja yhdistettävissä mihin sitä käytetään
  - miten allekirjoitusasiakirja tallennetaan järjestelmään niin, ettei sitä voida muuttaa tai manipuloida mitätöimättä merkinnän allekirjoitusta tai tilaa
  - miten allekirjoituksen kellonaika ja päivämäärä kirjataan sekä omistajan nimi ja allekirjoituksen merkitys
  - miten allekirjoituksen turvallisuus varmistetaan, eli niin, että se voi olla vain allekirjoituksen omistaja
- Mikäli käytetään salasanan ja käyttäjätunnuksen sijaan biometrisiä tunnisteita, ne tulee validoida

Verifioitujen kopioiden luonti

- Todennettu/verifioitu kopio tiedoista on vahvistettava esim. dokumentoitu päivätyllä allekirjoituksella
- Verifioidun kopion on sisällettävä samat tiedot kuin alkuperäinen, tiedon eheys tulee säilyä
- Verifioidut kopioit voidaan säilyttää alkuperäisten sijaan, mutta alkuperäisen tiedon hävitys tulisi harkita tarkkaan (voi olla vaihtelua kansallisesti)

Audit trail

- Audit trail tulee olla GLP-järjestelmissä (kuka muutti, milloin ja mitä esim. alkuperäinen arvo ja uusi arvo, syyn kirjaus)
- Käyttäjillä joilla on suora intressi tutkimusaineistoon ei saisi olla oikeuksia ottaa audit trail toimintoa pois päältä (voi olla mahdollista esim. system admin tunnuksilla)
- Mikäli audit trailia ei ole tulee käyttää vaihtoehtoisia tapoja esim. manuaalinen käyttöpäiväkirja tms.
- Audit trailin katselmoinnin ei tarvitse sisältää kaikkia toimintoja. Määritellään riskiperusteisesti esim. kohdistuen GLP-kannalta kriittisiin toimintoihin (tiedon syöttö, muuttaminen, poistaminen)

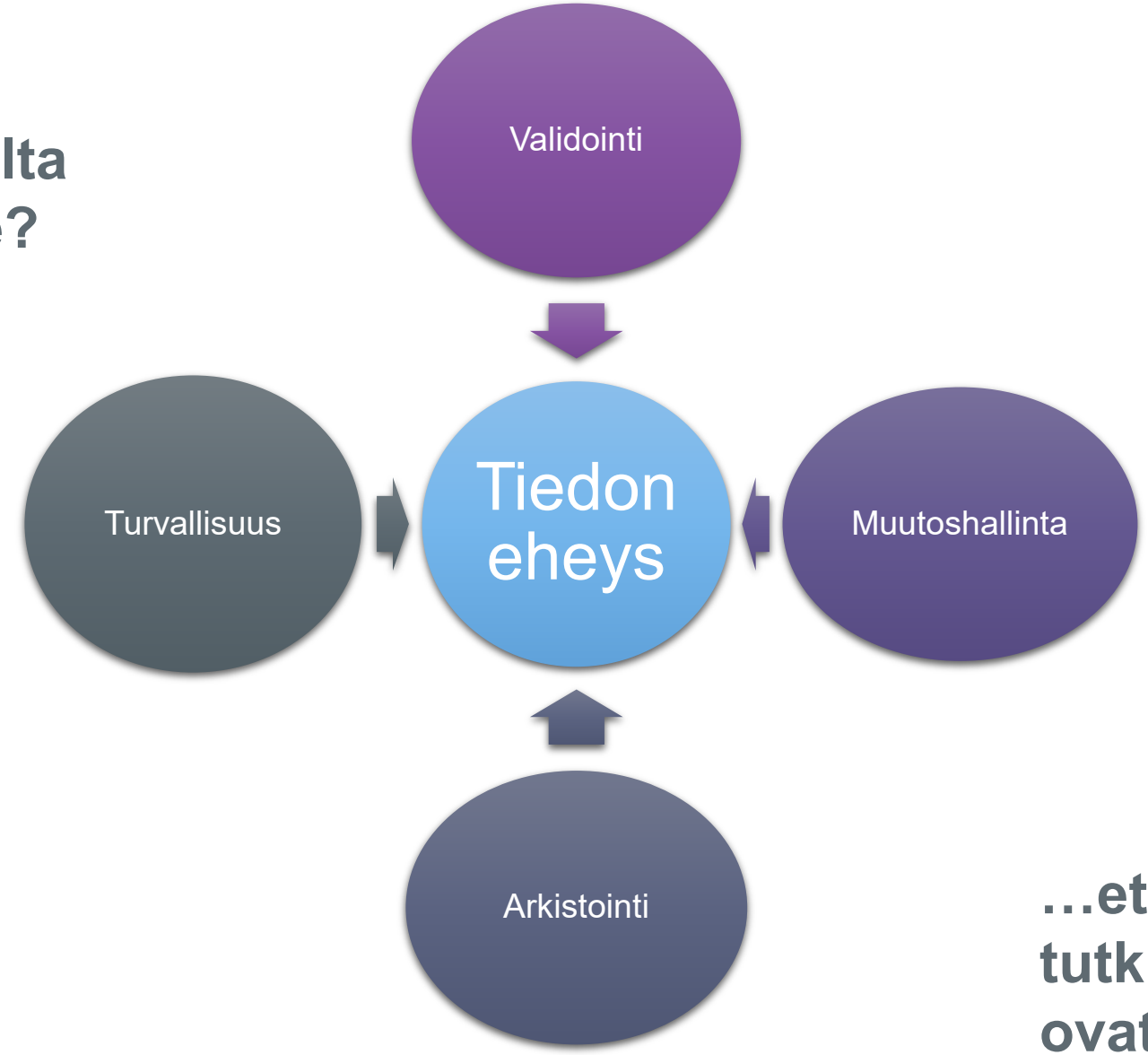
Tietojen säilytys ja arkistointi

- Kaikki tutkimukseen liittyvät tiedot tulee säilyttää, myös poissuljetut tai mitätöidyt
- Sähköiset tiedot tallennetaan samalla tasolla kuin ei-sähköiset (kulunvalvonta vs rajattu pääsy arkistoituihin tiedostoihin, indeksointi)
- Sähköinen arkistointi voi tapahtua tietovarastossa alkuperäisessä järjestelmässä tai erillään
- Arkistoidut tiedot täytyy säilyttää niin, että niitä ei voi muuttaa tai poistaa havaitsematta
- Arkistojärjestelyt on suunniteltava siten, että ne mahdollistavat tietojen hakemisen ja luettavuuden, mukaan lukien metatiedot, vaaditun säilytysajan
- Mikäli järjestelmää ei voida enää ylläpitää tulee tiedot siirtää (migraatio) uuteen järjestelmään

Yhteenveto

- Edellytyksenä riittävien varmistustoimenpiteiden määrittelylle
  - Tunnistettava GLP-kriittinen dokumentaatio ja tieto
  - Tunnistettava alkuperäinen dokumentaatio ja tieto
- Koskee myös manuaalista dokumentaatiota ei pelkästään sähköisiä järjestelmiä
- Menetelmien ei tulisi mahdollistaa tiedon manipulointia
- Arvioitava riskiperusteisesti millaisia varmistustoimenpiteitä tiedon eheyden varmistamiseksi tulee olla esim. järjestelmiin tehtävät rajoitukset, kopioiden/tiedon siirron tarkastukset (verified copy), säännölliset katselmoinnit ym.
- Huomioitava sähköisten järjestelmien hankinnassa ja ylläpidossa (audit trail, varmistukset, palautustestaukset kun tarpeellista, arkistointi, säilyykö metadata arkistoitaessa)

Mikä lopulta merkitsee?



…että tutkimustietosi ovat luotettavia!

Tiedon eheyteen liittyviä muita GxP-ohjeistoja

- PIC/S Guidance PI 041-1Good Practices for Data Management and Integrity in regulated GMP/GDP environments
- WHO Guidance on good data and record management practices
- MHRA Guidance on GxP data integrity
- EMA Q&A Data Integrity
- FDA Data Integrity and Compliance With Drug CGMP Questions and Answers Guidance for Industry

Esimerkkejä tarkastushavainnoista

- Palautustestausten puuttuminen
- Varmuuskopioita ei otettu ohjeen mukaisesti
- Varmuuskopioita ei säilytetty turvallisesti (esim. säilytettiin palvelintilassa)
- Puutteellinen uuden järjestelmän käyttöönoton dokumentointi
  - Järjestelmä oli otettu käyttöön ennen validoinnin hyväksymistä
- Käyttäjien hallinta ei ollut ajan tasalla
  - Käyttäjärooli ei vastannut nykyistä toimenkuvaa
  - Käyttäjäoikeuksia oli henkilöillä, jotka eivät työskennelleet enää yrityksessä
  - Käyttäjäoikeuksia oli myönnetty ilman koulutusta
  - Ulkoistetut administraattorit toimivat yhteistunnuksilla (ei jäljitettävyyttä)

Esimerkkejä tarkastushavainnoista

- Puutteet validointidokumentaatiossa
  - Validoinnille ei ollut asetettu hyväksymiskriteerejä
  - Audit trailille oli asetettu vaatimukset, mutta niitä ei ollut testattu validoinnissa
  - Testausdokumentaatio ei ollut kaikilta osin jäljitettävissä käyttäjävaatimuksiin
  - Validointiraportti ei kattanut poikkeamien käsittelyä (validoinnin aikaisia poikkeamia ei ollut dokumentoidusti selvitetty)
- Palvelinhuoneiden fyysinen turvallisuus ei ollut riittävä
  - Kulkuoikeudet eivät olleet ajan tasalla

Esimerkkejä tarkastushavainnoista

- Tutkimusdatan kirjaaja ei ollut jäljitettävissä sillä yhteinen käyttäjätunnus ja salasana laitteen ohjelmistoon oli laitteen vieressä kaikkien saatavilla
- Tulosten uudelleen kirjaaminen oli mahdollista, sillä tuloslomakkeita oli mahdollista tulostaa vapaasti ilman jäljitettävyyttä

Hyvää Joulua ja Vuotta 2022!

Lääkealan turvallisuus- ja kehittämiskeskus
Mirka Laavola
2.12.2021