SNAS SLOVENSKÁ NÁRODNÁ AKREDITAČNÁ SLUŽBA

METODICKÁ SMERNICA PRE SPRÁVNU LABORATÓRNU PRAX

INTEGRITA ÚDAJOV
(OECD Guideline No. 22)

MSA-G/22

Vydanie: 1

Aktualizácia: 0

BRATISLAVA

September 2022

Táto metodická smernica je prekladom dokumentu OECD Series on Principles of Good Laboratory Practice and Compliance Monitoring, No. 22,
Advisory Document of the Working Party on Good Laboratory Practice on GLP Data Integrity.
ENV/CBC/MONO(2021)26

Publikované so súhlasom OECD, Paríž.
Za kvalitu slovenského prekladu a jeho kompatibilitu s pôvodným textom a národnou legislatívou zodpovedá SNAS.

Spracoval: ***Ing. Kvetoslava Foríšeková***
Ing. Henrieta Bóriková

Preskúmal: ***RNDr. Lívia Kijovská, PhD.***

Schválil:. ***Mgr. Martin Senčák***

Účinnosť od: ***01.09.2022***

Táto MSA neprešla jazykovou úpravou.

Dostupnosť MSA: https://www.snas.sk

OBSAH

Strana

1 ÚVODNÉ USTANOVENIA

1.1 PREDHOVOR

Tento poradný dokument vypracovala Pracovná skupina OECD pre správnu laboratórnu prax (GLP). Vypracovanie dokumentu iniciovalo a viedlo Spojené kráľovstvo a jeho súčasťou bola prípravná skupina pod vedením Stephena Vintera (Spojené kráľovstvo) a Thomasa Lucotta (France Medical Products). V prípravnej skupine boli zástupcovia z Argentíny, Rakúska (Medical Products), Belgicka, Dánska (Medical Products), Talianska, Mexika, Holandska, USA (EPA) a USA (FDA). Proces zahŕňal obdobie verejného pripomienkovania, preskúmanie a schválenie dokumentu pracovnou skupinou pre správnu laboratórnu prax.

Za zverejnenie tohto dokumentu zodpovedá Výbor pre chemikálie a biotechnológiu, ktorý 8. septembra 2021 súhlasil s jeho odtajnením.

2 DEFINÍCIA POJMOV

Prevzaté z OECD Series on Principles of Good Laboratory Practice and Compliance Monitoring, No.1, OECD Principles of Good Laboratory Practice (as revised in 1997).

2.1 SLP

Zásady správnej laboratórnej praxe - systém kvality vzťahujúci sa na proces organizácie a podmienky, za ktorých sa neklinické štúdie plánujú, vykonávajú, overujú, zaznamenávajú, ukladajú a oznamujú. Neklinické štúdie sa vykonávajú na testovacích pracoviskách, ktorými sú laboratóriá, skleníky a polia.

Národný program dodržiavania zásad SLP (NP SLP) – zisťuje, či testovacie pracoviská zaviedli zásady SLP do praxe a či sú schopné zabezpečiť, že výsledné údaje majú zodpovedajúcu kvalitu. NP SLP vymedzuje pôsobnosť a rozsah programu, poskytuje informáciu o mechanizme, prostredníctvom ktorého testovacie pracovisko vstúpi do programu, o druhoch inšpekcií testovacích pracovísk a auditov štúdií, opisuje rôzne druhy inšpekcií, ako aj ich frekvenciu a vymedzuje právomoci inšpektorov.

Osvedčenie SLP - je dokument, ktorým sa deklaruje, že testovacie pracovisko (laboratórium) vykonáva štúdie (testy, skúšky) v súlade so zásadami Správnej laboratórnej praxe.

Národná monitorovacia autorita v dokumentoch OECD a EC = akreditujúca osoba (SNAS) v legislatíve SLP na Slovensku

2.2 POJMY TÝKAJÚCE SA TESTOVACIEHO PRACOVISKA

Testovacie pracovisko – pracovisko uvedené v zákone[1] vrátane osôb, priestorov a prevádzkových jednotiek potrebných na vykonávanie neklinických štúdií zdravotnej a environmentálnej bezpečnosti. Pre multicentrové štúdie, teda také, ktoré sú vykonávané na viacerých miestach, sa pod testovacím pracoviskom rozumie miesto, kde pracuje vedúci štúdie spolu so všetkými ďalšími testovacími miestami zúčastňujúcimi sa na štúdii.

[1] § 2 písm. e) zákona č. 67/2010 Z.z. o podmienkach uvedenia chemických látok a chemických zmesí na trh a o zmene a doplnení niektorých zákonov (chemický zákon).

Testovacie miesto – znamená také miesto, kde je vykonávaná určitá časť štúdie.

Vedenie testovacieho pracoviska - osoba(y), ktorá je zodpovedná za organizáciu a chod testovacieho pracoviska podľa zásad správnej laboratórnej praxe. Vykonáva právne úkony, administratívno-správne úkony vo všetkých veciach testovacieho pracoviska na základe zmluvy o zriadení pracoviska zakladajúcou listinou alebo zákonom.

Vedenie testovacieho miesta – (ak bolo vymenované) – osoba(y) zodpovedajúca za to, aby časť štúdie, za ktorú zodpovedá, bola vykonávaná v súlade so zásadami SLP.

Vedúci testovacieho pracoviska – v prípade zložitejšej organizačnej štruktúry testovacieho pracoviska osoba, ktorá je priamo zodpovedná za konkrétnu činnosť testovacieho pracoviska podľa zásad správnej laboratórnej praxe (riaditeľ odboru, vedúci laboratória...). Právomoci na zabezpečenie činnosti podľa zásad SLP má delegované od vedenia testovacieho pracoviska buď poverením alebo definovaním v pracovnej náplni.

Objednávateľ štúdie – subjekt, ktorý si objednáva, finančne zabezpečuje a predkladá neklinickú štúdiu zdravotnej a environmentálnej bezpečnosti na posúdenie.

(Pozri aj Nariadenie vlády č. 320/2010 Z. z. v znení neskorších predpisov, § 3, (5)).
Poznámka
Objednávateľom môže byť:

- *Subjekt*, ktorý prichádza s návrhom vykonať a podporuje, poskytnutím finančných alebo iných zdrojov, neklinické štúdie zdravotnej a environmentálnej bezpečnosti;*
- *Subjekt*, ktorý predkladá neklinické štúdie zdravotnej a environmentálnej bezpečnosti oprávnenej autorite pri registrácii produktu, alebo pri inej žiadosti, pre ktorú je súlad so zásadami SLP vyžadovaný.*

* *„Subjektom" môže byť jednotlivec, obchodná spoločnosť, združenie, vedecký, alebo akademický ústav, vládna agentúra alebo ich organizačné jednotky, alebo akýkoľvek iný právne identifikovateľný subjekt.*

Vedúci štúdie – osoba zodpovedajúca za celkové vykonanie neklinickej štúdie bezpečnosti zdravia a životného prostredia, vrátane plánu štúdie a záverečnej správy.

Vedúci čiastkovej štúdie - osoba, ktorá v prípade štúdie vykonávanej na viacerých miestach koná v mene vedúceho štúdie a zodpovedá za jemu pridelené časti štúdie.

Program zabezpečenia kvality - definovaný systém, zahŕňajúci zamestnancov, ktorý je nezávislý od vykonávania štúdie a slúži na zabezpečenie súladu postupu prác v testovacom pracovisku so zásadami správnej laboratórnej praxe.

Štandardné pracovné postupy (ŠPP) - sú dokumentované postupy, ktoré opisujú, ako vykonávať testy alebo činnosti, ktoré nie sú detailne špecifikované v študijných plánoch alebo v oficiálnych a všeobecne akceptovaných testovacích metódach (OECD, REACH).

Master Schedule – súbor informácií o vykonávaných štúdiách na testovacom pracovisku, slúži na sledovanie štúdií a vyťaženosti testovacieho pracoviska.

2.3 POJMY TÝKAJÚCE SA NEKLINICKÝCH ŠTÚDIÍ ZDRAVOTNEJ A ENVIRONMENTÁLNEJ BEZPEČNOSTI

Neklinická štúdia zdravotnej a environmentálnej bezpečnosti – ďalej len „štúdia“ – znamená experiment alebo súbor experimentov, ktorými je testovaná látka skúmaná v laboratórnych podmienkach alebo v životnom prostredí, s cieľom získať údaje o jej vlastnostiach a/alebo zdravotnej a environmentálnej bezpečnosti, ktoré sú plánované ako podklad pre rozhodnutie príslušnej regulačnej autority pred jej povolením do používania.

Krátkodobá štúdia – štúdia krátkeho trvania so všeobecne používanými bežnými technikami.

Multicentrová štúdia - akákoľvek štúdia, ktorej niektoré fázy sú vykonávané na viac ako jednom mieste. Takéto štúdie sú nevyhnutné, ak je potrebné využiť miesta, ktoré sú zemepisne vzdialené, organizačne rozdielne alebo ináč oddelené. To sa týka aj oddelenia organizácie, ktoré slúži ako testovacie miesto, kým iné oddelenie tej istej organizácie pôsobí ako testovacie pracovisko.

Fáza / etapa štúdie - definovaná činnosť alebo súbor činností pri uskutočňovaní štúdie.

Plán štúdie – dokument, ktorý definuje ciele a experimentálne plánovanie skúšok na vykonávanie štúdie, vrátane jeho zmeny a doplnky.

Doplnok plánu štúdie – predstavuje cielenú zamýšľanú zmenu plánu štúdie.

Odchýlka od plánu štúdie – neočakávaná odchýlka od plánu štúdie po dátume začatia štúdie.

Testovací systém – biologický, fyzikálny alebo chemický systém alebo ich kombinácia použitá v štúdii.

Primárne údaje – všetky pôvodné záznamy a dokumentácia vypracovaná v testovacom pracovisku, alebo ich verifikované kópie, ktoré sú výsledkom pozorovaní a činností vykonaných v štúdii. Primárne údaje môžu zahŕňať aj fotografie, mikrofilmy, počítačové médiá na uchovávanie údajov, diktované pozorovania, záznamy z automatizovaných prístrojov alebo iné záznamové médiá určené na uchovávanie dát.

Vzorka – každý materiál odobratý z testovacieho systému za účelom vyšetrenia, analýzy alebo uchovávania.

Dátum začiatku štúdie – dátum, kedy vedúci štúdie podpísal plán štúdie.

Dátum experimentálneho začiatku štúdie – dátum, kedy boli získané prvé údaje zo štúdie.

Dátum ukončenia experimentu – posledný deň, kedy boli získané údaje zo štúdie.

Dátum ukončenia štúdie – dátum, kedy vedúci štúdie podpísal záverečnú správu zo štúdie.

2.4 POJMY TÝKAJÚCE SA TESTOVANEJ LÁTKY

Testovaná látka

je definovaná ako látka, ktorá je predmetom SLP štúdie. Závery SLP štúdie poskytnú informácie o vlastnostiach testovanej látky, ktoré umožnia zhodnotiť, aké riziko predstavuje testovaná látka pre bezpečnosť ľudí, zvierat alebo pre životné prostredie.

Treba upozorniť že v niektorých OECD Test Guidelines sa pre „testovanú látku“ používa aj pojem "test chemical”. (odsúhlasené v júni 2013, OECD's Joint Meeting of the Chemicals Committee and the Working Party on Chemicals, Pesticides and Biotechnology). Teda môžeme sa stretnúť aj s pojmami "test item", "test compound", "test substance". Cieľom tohto návrhu nebolo zavedenie novej definície pojmu “chemikália”, ale skôr išlo o zosúladenie terminológie s definíciou uvedenou v UN GHS pre klasifikáciu a označovanie, kde sa pod chemikáliou myslí aj “látka a zmes”

Šarža

Je definovaná ako špecifické množstvo testovanej alebo referenčnej látky vyrobené v jednom cykle výroby, takým spôsobom, že sa dá očakávať, že látka má jednotný a homogénny charakter a dá sa za takú pokladať.

Nosič / Vehikulum

Je definovaný ako akákoľvek látka, ktorá slúži ako nosič na zmiešavanie, dispergovanie, vytvorenie suspenzie, alebo zvyšovanie rozpustnosti testovanej látky a/alebo referenčnej látky na uľahčenie jej podávania/aplikácie testovaciemu systému.

Formulácia (test. látka + nosič)

Formulácia (alebo zmesi) je kombinácia testovanej látky a rôznych rôznych prísad, ako pomocných látok, ktoré sú skombinované a podávané a/alebo aplikované testovaciemu systému v rôznych formách (napr. tabletky, kapsule, roztok...).

Príprava testovanej látky

Príprava testovanej látky (alebo pripravená testovaná látka) môže byť formuláciou (alebo zmesou) obsahujúcou testovanú látku, alebo testovanú látku v nosiči, kde sa táto kombinácia získa riedením, miešaním, dispergovaním, vytvorením suspenzie, rozpustením a/alebo iným procesom so zámerom aplikovať ju testovaciemu systému. Testovaciemu pracovisku môže byť dodaná testovaná látka (na priame podanie), alebo testovaná látka, ktorá ešte musí byť nejako pripravená alebo už vopred upravenú látku, ktorú možno priamo podať alebo aplikovať testovaciemu systému (tiež nazývaná "ready-to-use").

Testovaná látka, ktorá je zapuzdrená (encapsulated) alebo balená iným spôsobom, pri neprítomnosti pomocných látok alebo nosiča, sa nepovažuje za to isté ako „pripravená testovaná látka" opisovaná v tomto dokumente.

Charakterizácia

Charakterizácia určuje vlastnosti testovanej látky a poskytuje dôkazy na podporu vhodnosti jej použitia v SLP štúdiách.

Identifikácia

Identifikácia testovanej látky je proces kontroly a hodnotenia testovanej látky porovnaním s dodanými informáciami, s cieľom určiť, či testovaná látka je tá, ako bola očakávaná. Poskytnutými informáciami môžu byť prepravné doklady, e-maily od dodávateľa, označenie etiketou na testovanej látke, atď. Typickými znakmi používanými na identifikáciu testovanej látky môžu byť – názov, číslo šarže, čistota, koncentrácia, zloženie, chemické, fyzikálne a biologické parametre. Identifikácia môže tiež zahŕňať fyzikálnu a/alebo analytickú kontrolu. Proces identifikácie musí byť vykonaný pred začiatkom experimentálnej fázy SLP štúdie.

Dátum exspirácie

Dátum exspirácie je stanovený dátum, do ktorého sa očakáva, že testovaná látka si zachová svoje vlastnosti v rámci špecifikácií, pokiaľ je skladovaná za definovaných podmienok a po uplynutí ktorého už nemôže byť použitá.

Dátum retestovania

Dátum retestovania je dátum, kedy testovaná látka môže byť znovu otestovaná, s cieľom ubezpečiť sa, že je ešte stále vhodná na použitie.

2.5 POJMY TÝKAJÚCE SA INŠPEKCIE TESTOVACIEHO PRACOVISKA

Inšpekcia testovacieho pracoviska - je kontrola postupov testovacieho pracoviska a praktických činností smerujúcich k dosiahnutiu stupňa zhody so zásadami SLP, počas ktorej

sa skontrolujú systémy riadenia a pracovné postupy testovacieho pracoviska, ako aj integrita údajov, aby sa zabezpečilo, že výsledné údaje majú náležitú kvalitu na posúdenie a rozhodovanie národnými regulačnými orgánmi.

Inšpektor - je osoba, vykonávajúca inšpekcie testovacích pracovísk a audity neklinických štúdií v zastúpení akreditujúcej osoby (SNAS).

Audit štúdií - je porovnanie prvotných údajov a súvisiacich záznamov v predbežnej alebo záverečnej správe, s cieľom určiť, či primárne údaje boli presne zaznamenané, či sa testovanie vykonalo v súlade s plánom štúdie a štandardnými pracovnými postupmi, získať dodatočné informácie neuvedené v správe a stanoviť, či postupy použité pri spracovaní údajov mohli ovplyvniť ich validitu.

Správa o inšpekcii - je oficiálny písomný doklad o vykonanej inšpekcii, v ktorej sú identifikované všetky posudzované prvky a činnosti, menovite uvedené všetky nedostatky a posúdená miera dodržiavania zásad SLP. Určuje kvalitu a integritu údajov preverovaného testovacieho pracoviska.

3 SKRATKY

GLP	Good Laboratory Practice
MSA	Metodická smernica na akreditáciu
OECD	(Organisation for Economic Cooperation and Development) Organizácia pre hospodársku spoluprácu a rozvoj
SLP	Správna laboratórna prax
SNAS	Slovenská národná akreditačná služba
ŠPP	Štandardný pracovný postup
SR	Slovenská republika
ÚZK	Útvar zabezpečenia kvality

4 SÚVISIACE PREDPISY

Zákon 67/2010 Z. z. o podmienkach uvedenia chemických látok a chemických zmesí na trh a o zmene a doplnení niektorých zákonov (chemický zákon)

Nariadenie vlády č. 320/2010 Z. z., ktorým sa upravujú činnosti testovacích pracovísk a činnosti inšpektorov vykonávajúcich inšpekcie, audit a overovanie dodržiavania zásad správnej laboratórnej praxe.

Nariadenie vlády SR č. 92/2012 Z. z., ktorým sa mení a dopĺňa nariadenie vlády Slovenskej republiky č. 320/2010 Z. z., ktorým sa upravujú činnosti testovacích pracovísk a činnosti inšpektorov vykonávajúcich inšpekcie, audit a overovanie dodržiavania zásad správnej laboratórnej praxe**.**

Zákon č. 505/2009 Z. z. o akreditácii orgánov posudzovania zhody a o zmene a doplnení zákonov v platnom znení.

MSA série G - všetky MSA vydané SNAS, týkajúce sa SLP dostupné na webovej stránke www.snas.sk

EU

Smernica 2004/9/ES o inšpekcii a overovaní správnej laboratórnej praxe (kodifikovaná verzia)

Smernica 2004/10/ES o zosúlaďovaní zákonov, predpisov a správnych opatrení uplatňovaných na zásady správnej laboratórnej praxe a overovanie ich uplatňovania pri testoch chemických látok (kodifikovaná verzia)

Nariadenie Európskeho parlamentu a Rady (ES) č. 1907/2006 z 18. decembra 2006 o registrácii, hodnotení, autorizácii a obmedzovaní chemikálií **(REACH)** a o zriadení európskej chemickej agentúry (ECHA), o zmene a doplnení smernice 1999/45/ES a o zrušení nariadenia Rady (EHS) č. 793/93 a nariadenia Komisie (ES) č. 1488/94, smernice rady76/769/EHS a smerníc Komisie 91/155/EHS, 93/67/EHS, 93/105/ES A 2000/21/ES, v platnom znení.

Nariadenie Európskeho parlamentu a Rady (ES) č. 1272/2008 zo 16. decembra 2008 o klasifikácii, označovaní a balení látok a zmesí, o zmene, doplnení a zrušení smerníc 67/548/EHS a 1999/45/ES a o zmene a doplnení nariadenia (ES) č. 1907/2006, platnom znení.

Nariadenie Komisie č. 440/2008 z 30. mája 2008, ktorým sa ustanovujú testovacie metódy podľa nariadenia EP a R č. 1907/2006 o registrácii, hodnotení, autorizácii a obmedzovaní chemických látok **(REACH).**

OECD

1981 Council Act Decision [C (81)30/Final] on the Mutual Acceptance of Data in the Assessment of Chemicals,

1989 Council Decision Recommendation on Compliance with Principles of Good Laboratory Practice [C (89)87/Final],

OECD (1997), OECD Series on Principles of Good Laboratory Practice and Compliance Monitoring Number 1: OECD Principles on Good Laboratory Practice (revised in 1997). [1]

OECD (2007), OECD Series on Principles of Good Laboratory Practice and Compliance Monitoring Number 15: Advisory Document of the Working Group on Good Laboratory Practice : Establishment and Control of Archives that Operate in Compliance with the Principles of GLP. [2]

OECD (2014), OECD Series on Principles of Good Laboratory Practice and Compliance Monitoring Number 16: Advisory Document of the Working Group on Good Laboratory Practice : Guidance on the GLP Requirements for Peer Review of Histopathology. [3]

OECD (2016), OECD Series on Principles of Good Laboratory Practice and Compliance Monitoring Number 17: Advisory Document of the Working Group on Good Laboratory Practice : Application of GLP Principles to Computerised Systems. [4]

5 VECNÁ ČASŤ

5.1 ÚVOD

Jednou zo základných úloh zásad správnej laboratórnej praxe (SLP) je zabezpečiť kvalitu a integritu údajov testov neklinických štúdií zdravotnej bezpečnosti.

Spôsob, akým sa údaje zo štúdií, na podporu hodnotenia bezpečnosti ľudí, zvierat a životného prostredia, generujú, spracúvajú, vykazujú, uchovávajú a archivujú sa naďalej vyvíja, v súlade so zavádzaním a neustálym vývojom podporných technológií. Môžeme sem zaradiť rastúce používanie elektronického zberu údajov, integráciu a automatizáciu systémov a iných technológií. Systémy sa môžu meniť od manuálnych procesov s papierovými záznamami až po používanie zložitých počítačových systémov. Avšak, hlavný účel požiadaviek zásad SLP však zostáva rovnaký – mať dôveru ku kvalite, integrite údajov a mať možnosť rekonštruovať všetky činnosti vykonané v priebehu neklinických štúdií bezpečnosti.

5.2 ROZSAH PÔSOBNOSTI

Na tento dokument sa vzťahujú nasledujúce aspekty:

1. Tento dokument poskytuje návod pre testovacie pracoviská alebo testovacie miesta, ktoré vykonávajú štúdie SLP alebo časti štúdie SLP.
   Na účely tohto dokumentu pojem „testovacie pracovisko“ zahŕňa aj testovacie miesta; pojem „štúdia“ zahŕňa aj čiastkové štúdie; a výraz „vedúci štúdie“ zahŕňa aj zodpovednosti vedúceho čiastkovej štúdie, ak je to vhodné.
2. Cieľom usmernenia je podporiť prístup založený na hodnotení rizika pri spravovaní údajov, ktorý zahŕňa riziko údajov, ich kritickosť a životný cyklus údajov. Používatelia tohto dokumentu musia porozumieť tokom údajov, za ktoré sú zodpovední alebo ktorých sa zúčastňujú (ako životný cyklus), aby mohli identifikovať údaje, ktoré môžu mať vplyv na súlad s dodržiavaním zásad SLP. Na druhej strane takýto prístup podporí identifikáciu a implementáciu najefektívnejších a najúčinnejších kontrol založených na analýze rizika.
3. Integrita údajov je miera, do akej sú údaje úplné, konzistentné, presné, dôveryhodné a do akej miery sú tieto charakteristiky údajov zachované počas celého životného cyklu údajov. Údaje sa majú zhromažďovať a uchovávať bezpečným spôsobom, aby boli priraditeľné, čitateľné, priebežne zaznamenané a presné, či už ide o primárne údaje alebo ich overenú kópiu.
4. Usmernenie sa vzťahuje na skratku ALCOA (Attributable, Legible, Contemporaneous, Original and Accurate) – teda priraditeľné, čitateľné, súčasné, originálne a presné. ALCOA sa historicky považuje za atribúty údajov, ktoré sú vhodné pre regulačné účely. ALCOA+ sa v poslednom čase spomínalo aj na zdôraznenie ďalších atribútov Complete, Consistent, Enduring a Available - kompletné, konzistentné, trvalé, dostupné. Neexistuje žiadny rozdiel medzi očakávaniami týkajúcimi sa integrity údajov pre obe tieto systémy, pretože opatrenia na správu údajov majú zabezpečiť, aby boli údaje úplné, konzistentné, trvalé a dostupné počas celého životného cyklu údajov.
5. Usmernenie sa zaoberá integritou údajov a nie kvalitou údajov, pretože kontroly požadované na integritu nezaručujú zároveň aj kvalitu údajov (pozri tiež definície v bode 5.3.4 a 5.3.5). Integrita údajov poskytuje kontrolu nad údajmi (t. j. či im možno dôverovať), zatiaľ čo kvalita údajov sa týka charakteristík údajov, ktoré zabezpečujú,

že vytvorené údaje sú generované v súlade s platnými normami a môžu byť použité na určený účel.

6. Toto usmernenie sa má rovnako uplatňovať na kontrolu všetkých typov údajov a formátov. Niektoré body sú však zamerané a konkrétne uplatniteľné len na elektronické údaje a elektronické systémy.
7. Toto usmernenie je potrebné čítať v spojení s dokumentmi OECD:
   No. 1 (OECD Principles on Good Laboratory Practice) (OECD, 1997[1]),
   No. 15 (Establishment and Control of Archives that Operate in Compliance with the Principles of GLP) (OECD, 2007[2]), No 16 (Guidance on the GLP Requirements for Peer No. 16 (Review of Histopathology) (OECD, 2014[3])
   No. 17 (Application of GLP Principles to Computerised Systems) (OECD, 2016[4]) a platnými vnútroštátnymi predpismi.
   Zásady SLP, ktoré odkazujú na integritu údajov, možno nájsť v časti II, 1.1.2.b to 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 dokumentu No. 1 (OECD Principles of Good Laboratory Practice).
   Keď sú doplňujúce informácie obsiahnuté v tomto dokumente a aj v iných dokumentoch, odkaz je uvedený v texte.

5.3 DEFINÍCIE A POJMY

5.3.1 Údaje/Data

Údaje sú kvantitatívne alebo kvalitatívne fakty, čísla a štatistiky zhromaždené za účelom referencie alebo analýzy. Patria sem všetky pôvodné záznamy a overené kópie pôvodných záznamov vrátane primárnych údajov a metadát a všetkých následných transformácií, ktoré sa vygenerujú alebo zaznamenajú v čase činnosti vykonávanej v súlade so zásadami SLP a umožňujú vykonať úplnú rekonštrukciu a vyhodnotenie SLP činnosti.

Údaje môžu mať rôzne formáty (napr. analógové, digitálne), rôznu štruktúru, rozloženie (napr. na papieri alebo na obrazovke), zdroje (napr. chromatografické záznamy, text, obrázok, video atď.) a médiá používané na uchovávanie alebo prezentáciu (papier, DVD, film, páska, elektronické súbory, atď.).

Údaje môžu byť zachytené alebo zaznamenané:

- manuálnym zaznamenaním pozorovania alebo činnosti na papier alebo do elektronického systému;
- automatickým záznamom na papier (automatickou tlačou) alebo v elektronickom systéme s použitím zariadení, ktoré môžu byť od jednoduchých nástrojov až po zložité vysoko konfigurovateľné počítačové systémy;
- používanie hybridného systému, kde kombinácie papiera (alebo iných neelektronických médií) a elektronických záznamov vytvárajú primárne údaje;
- na iných médiách, ako je fotografia, zobrazovacie metódy a technológie, chromatografické platne atď., ktoré môžu byť generované manuálne, automaticky alebo pomocou hybridného systému.

Primárne údaje/Raw data

Zásady SLP definujú primárne údaje ako všetky pôvodné záznamy a dokumentáciu testovacieho pracoviska alebo ich overené kópie, ktoré sú výsledkom pôvodných pozorovaní

a činností v štúdii a umožňujú kompletnú rekonštrukciu a vyhodnotenie činností SLP. Primárne údaje môžu tiež zahŕňať napríklad fotografie, kópie na mikrofilmoch alebo mikrofišoch, počítačom čitateľné médiá, diktované pozorovania, zaznamenané údaje z automatizovaných prístrojov alebo akékoľvek iné médium na ukladanie údajov, ktoré bolo uznané ako schopné poskytnúť bezpečné uloženie informácií na určité časové obdobie.

Záznam/Record

Záznam je časť informácie (napr. údaj). Termín pôvodný (primárny) záznam sa používa na označenie prvého zdroja informácií alebo zberu údajov. Pôvodné záznamy sú vo všeobecnosti nespracované údaje. Ak pôvodný záznam spĺňa definíciu primárnych údajov, ale za taký sa nepovažuje, musí to byť odôvodnené.

Overená kópia/Verified copy

Overená/verifikovaná kópia je verným zobrazením originálu v čase vytvorenia kópie. Overená kópia môže byť uložená v inom formáte alebo type dokumentu ako originál.

Overené kópie sa robia preto, aby bolo možné:

- vytvoriť duplikát originálov, pre vloženie do rôznych súborov (napr. primárne údaje spoločné pre niekoľko štúdií);
- predĺžiť dobu uchovávania niektorých údajov, ktorých formát neumožňuje uchovávanie (napr. výtlačky na termocitlivom papieri);
- umožniť uchovávanie údajov, ak originál nemožno ponechať bez toho, aby nepredstavoval riziko pre iné archivované materiály (napríklad primárne údaje na papieri znečistenom tekutinami zvierat, chemikáliami atď.);
- uľahčiť výmenu údajov;
- podporiť činnosti pri archivácii.

Najbežnejšie procesy na generovanie overených kópií zo statických záznamov sú:

- fotokópia papierového záznamu (papier na papier);
- skenovanie papierového záznamu (z papiera do elektronickej podoby);
- obrázok z papierového záznamu (papier na obrázok, napr. pdf z word dokumentu);
- snímka obrazovky a výtlačok elektronického záznamu (z elektronickej na papier).

Odvodené údaje/Derived data

Odvodené údaje sa získajú a zrekonštruujú z primárnych údajov (napr. konečné koncentrácie vypočítané tabuľkovým procesorom na základe primárnych údajov získaných z prístroja; výsledkové tabuľky vygenerované systémom správy laboratórnych informácií /LIMS/, atď.). Odvodené údaje sa získavajú spracovaním údajov.

Metaúdaje/Metadata

Metaúdaje (metadáta) sú údaje poskytujúce informácie používané na identifikáciu, opis a vzťahy medzi údajmi. Metadáta dávajú údajom význam, poskytujú kontext, definujú štruktúru a umožňujú získavanie naprieč systémami a použiteľnosť, autenticitu a auditovateľnosť údajov v čase. Pre elektronické údaje môžu byť časti metaúdajov generované v systéme sledovania zmien (audit trailoch).

Metaúdaje tvoria neoddeliteľnú súčasť údajov. Bez kontextu poskytovaného metaúdajmi nemajú údaje žiadny alebo majú len obmedzený význam. Chýbajúce metaúdaje znižujú schopnosť správne interpretovať údaje.

Sledovanie zmien/Audit trail

Audit trail je forma metaúdajov, ktorá obsahuje informácie spojené s akciami, ktoré sa týkajú vytvárania, úpravy alebo vymazania elektronických údajov. Sledovanie zmien poskytuje automatizovaný bezpečný spôsob zaznamenávania podrobností jednotlivých krokov v životnom cykle údajov, ako je vytváranie, pridávanie, mazanie alebo zmeny informácií v elektronickom zázname bez zakrytia alebo prepísania pôvodného záznamu. Audit trail uľahčuje rekonštrukciu histórie takýchto udalostí súvisiacich so záznamom, vrátane „kto, čo, kedy a prečo“ vykonal.

5.3.2 Štruktúra údajov/Data structure

Údaje môžu mať rôznu štruktúru.

Statický formát/Static format

Statický formát záznamu, ako je papierový alebo elektronický záznam, je ten, ktorý je nemenný a neumožňuje interakciu medzi používateľom a obsahom záznamu. Napríklad všetky papierové záznamy sú statické záznamy. Elektronické záznamy, ktoré neobsahujú žiadne prepojenie na iné záznamy umožňujúce interakciu, sú tiež statické záznamy. Príkladom statického záznamu z elektronického systému je napr. vytlačený záznam z jednoduchej elektronickej váhy, kde sa elektronické údaje nijako neukladajú.

Dynamický formát/Dynamic format

Záznamy v dynamickom stave sú väčšinou elektronické záznamy, ktoré umožňujú interaktívny vzťah medzi používateľom a obsahom záznamu. Príkladom dynamického formátu môžu byť chromatografické údaje uchovávané ako elektronické záznamy, ktoré používateľovi umožňujú priblížiť základnú líniu, jasnejšie zobraziť integráciu, alebo mať priamy prístup prostredníctvom elektronických odkazov k postupnosti analýzy, tabuľke výsledkov, kontrolným záznamom a metódam získavania a integrácie. Elektronicky podpísané záznamy sú tiež dynamické záznamy, pretože obsahujú prepojenie s overením podpisu.

Štruktúra súboru/File structure

Spôsob, akým je väčšina elektronických údajov štruktúrovaná v prostredí SLP, závisí od toho, na čo sa budú údaje používať a koncovému používateľovi to bude takmer vždy určovať softvér / počítačový systém, ktorý má k dispozícii.

Jednoduché súbory /Flat files

Jednoduchý súbor pozostáva z jednej tabuľky údajov, nemá žiadnu vnútornú hierarchiu a umožňuje používateľovi špecifikovať atribúty údajov, t. j. jeho dátová štruktúra je nezávislá a obmedzená.

Je možné predstaviť si takéto súbory ako jednotlivé lístky v zásuvke klasickej kartotéky, čo je kolekcia jednotlivých záznamov, z ktorých každý obsahuje samostatné údaje. Najbežnejšie sú to súbory končiace príponou .csv alebo .xls alebo bežný textový dokument programu Microsoft Word™.

Relačné databázy/Relational databases

Relačné databázy sú kolekciou tabuliek, ktoré sú navzájom prepojené pomocou spoločných údajov, ako je napríklad číslo štúdie, a môžu byť usporiadané tak, aby zvýraznili špecifické informácie pre ad hoc dotazy. Relačná databáza je nástroj na vyhľadávanie, ktorý poskytuje

možnosť zachytiť širokú škálu typov údajov. Relačné databázy sa zvyčajne nepoužívajú na zaznamenávanie primárnych údajov.

Relačné databázy uchovávajú rôzne zložky pridružených údajov a metaúdajov na rôznych miestach. Každý jednotlivý záznam sa vytvorí a možno ho získať kompiláciou údajov a metadát na kontrolu pomocou nástrojov databázy.

Napríklad elektronické záznamy v databázovom formáte umožňujú používateľovi ich sledovať, sledovať trendy a vyhľadávať údaje.

5.3.3 Elektronický podpis/Elektronic signature

Elektronický podpis je podpis v digitálnej podobe, ktorý zastupuje vlastnoručne napísaný („mokrý“) podpis.

Existujú rôzne typy systémov od jednoduchých (napr. interná identifikácia používateľa heslom) až po zložité systémy podpisov (napr. s externou, certifikovanou službou elektronického podpisu, ktorá poskytuje časovú pečiatku a zašifrované informácie za podpisom). Aby bolo možné uznať elektronický podpis z právneho hľadiska, súvisiaca úroveň požadovanej kontroly je definovaná miestnymi predpismi (tam, kde je to relevantné).

5.3.4 Integrita údajov/Data integrity

Integrita údajov je miera, do akej sú údaje úplné, konzistentné, presné, dôveryhodné a spoľahlivé a že tieto vlastnosti údajov sú zachované počas celého životného cyklu údajov. Zabezpečenie integrity údajov si vyžaduje vhodné systémy riadenia kvality a rizík vrátane dodržiavania spoľahlivých vedeckých zásad, osvedčených postupov dokumentácie a školenia zamestnancov.

5.3.5 Kvalita údajov/Data quality

Kvalita údajov je záruka, že produkované údaje sú generované podľa platných noriem a sú vhodné na zamýšľaný účel. Kvalita údajov je zabezpečená vhodným návrhom štúdie, ktorá presne a vedecky rieši experimentálnu otázku a skúmané hypotézy, a dostupnosťou primeraných zdrojov. Kvalita údajov ovplyvňuje hodnotu a celkovú prijateľnosť údajov z hľadiska rozhodovania alebo ďalšieho použitia.

5.3.6 Životný cyklus údajov/Data life cycle

Životný cyklus údajov zahŕňa všetky fázy životnosti údajov od generovania a zaznamenávania cez spracovanie (vrátane analýzy, transformácie alebo migrácie), použitie, uchovávanie údajov, archiváciu, vyhľadávanie a zničenie.

- Schválenie údajov/Data approval: Schválenie údajov je akt autorizácie údajov po zbere, spracovaní alebo overení, aby sa zaznamenalo, že údaje sú vhodné na ich zamýšľané použitie.
- Prepis/Transcription: Prepis je proces, pri ktorom sa údaje ručne skopírujú zo zdroja do iného záznamu súboru údajov.

  Prepis môže nastať, keď:

  - rovnaké informácie sú zaznamenané v rôznych záznamoch (napríklad dátum príchodu testovanej látky je zaznamenaný vo viacerých záznamoch, ako sú denníky alebo formuláre);

- údaje sa vkladajú do počítačového systému na výpočty. Prepis manuálnych záznamov do elektronického systému predstavuje príklad hybridného systému.

- Spracovanie údajov/Data processing: Spracovanie údajov je postupnosť operácií vykonávaných s údajmi s cieľom extrahovať, prezentovať, vypočítať alebo získať odvodené údaje v definovanom formáte. Príklady môžu zahŕňať výpočty v tabuľkovom procesore, štatistickú analýzu údajov jednotlivých testovacích systémov na prezentovanie trendov alebo konverziu primárneho elektronického signálu na chromatogram a následne vypočítaný numerický výsledok.
- Migrácia údajov/Data migration: Migrácia údajov je proces presúvania elektronických údajov medzi rôznymi typmi dátových úložísk, počítačovými systémami alebo jednoducho presun dát z jedného formátu do druhého. To môže zahŕňať zmenu formátu údajov, nie však obsahu alebo významu, aby boli použiteľné alebo viditeľné v alternatívnom počítačovom systéme.
- Transakcia počítačového systému/Computerised system transaction: Transakcia v počítačovom systéme je postupnosť operácii v počítačovom systéme, ktorá musí byť vykonaná buď celá alebo vôbec, ako keby išlo o jednu logickú operáciu. Jednotlivé operácie tvoriace transakciu nesmú spôsobovať permanentné zmeny v uložených dátach - transakcia sa smie vykonať až vtedy, keď ju buď používateľ dokončí (napríklad stlačením tlačidla Uložiť, viď "schvaľovanie údajov") alebo keď si samotný systém vynúti jej ukončenie a spracovanie.
- Uchovávanie údajov/Data retention: Uchovávanie údajov je uchovávanie údajov, ktoré môže slúžiť na účely archivácie (chránené údaje na dlhodobé uchovávanie) alebo zálohovania (elektronické údaje alebo na účely obnovy po havárii).
- Zálohovanie/Back-up: Zálohovanie údajov je kópia aktuálnych údajov, metadát a nastavení konfigurácie systému, ktorá je uchovávaná na účely obnovy vrátane obnovy po havárii.

  Zálohovanie umožňuje vykonať opatrenia na obnovu dátových súborov alebo softvéru, reštartovanie spracovania alebo použitie alternatívneho počítačového vybavenia po zlyhaní systému alebo jeho zničení.

- Archív/Archive: Archív znamená určený priestor alebo zariadenie (napr. kabinet, miestnosť, budova alebo počítačový systém) na bezpečné uloženie a uchovávanie záznamov a materiálov.

5.3.7 Správa údajov/Data governance

Správa údajov je súhrn opatrení na zabezpečenie toho, aby údaje (bez ohľadu na formát, v ktorom sú zachytené, generované, zaznamenané, spracované, uchovávané, archivované a používané) boli priraditeľné, čitateľné, súčasné, pôvodné (alebo overená kópia), presné, úplné, konzistentné, trvalé a presné (ALCOA+) počas celého životného cyklu.

Tieto opatrenia môžu pozostávať z jedného samostatného systému alebo z kombinácie systémov v rámci testovacieho pracoviska.

5.4 SLP ZODPOVEDNOSTI ZA ÚDAJE , OD VYTVORENIA PO ARCHIVÁCIU

Pracovníci podieľajúci sa na štúdii

Všetci pracovníci podieľajúci sa na štúdii sú zodpovední za rýchle a presné zaznamenávanie primárnych údajov a v súlade so zásadami SLP.

Vedúci štúdie

Vedúci štúdie musí zabezpečiť, že:

- všetky primárne údaje sú plne zdokumentované a zaznamenané;
- počítačové systémy použité v štúdii boli validované, vrátane požiadaviek spojených s integritou údajov; a
- po ukončení (vrátane predčasného ukončenia) štúdie sa plán štúdie, záverečná správa, primárne údaje a podporný materiál archivujú tak, aby všetok materiál, vrátane údajov potrebných na rekonštrukciu štúdie, zostal k dispozícii.

Archivár

Archivár je osoba, zodpovedná za riadenie, činnosti a postupy archivácie v súlade so zásadami SLP, vrátane archivácie údajov, fyzicky a elektronicky.

Vedenie testovacieho pracoviska

Vedenie testovacieho pracoviska (Test Facility Management /TFM) zodpovedá za organizáciu a fungovanie pracoviska, kde sa generujú údaje. TFM musí:

- zabezpečiť, aby bol k dispozícii dostatočný počet kvalifikovaných zamestnancov, vhodné zariadenia, vybavenie a materiály na včasné a správne vykonanie štúdie vrátane zdrojov na zabezpečenie správy údajov;
- zabezpečiť vedenie záznamov o kvalifikácii, školeniach, skúsenostiach a opise práce pre každého pracovníka (vedecký pracovník aj technik);
- zabezpečiť, aby pracovníci jasne rozumeli činnostiam, ktoré majú vykonávať a v prípade potreby im poskytnúť školenia pre tieto činnosti, vrátane školenia o integrite údajov;
- zabezpečiť vytvorenie a dodržiavanie vhodných a technicky platných štandardných pracovných postupov (ŠPP) a schváliť všetky pôvodné a revidované ŠPP vrátane tých, ktoré sa týkajú systému správy údajov;
- zabezpečiť, aby bola identifikovaná osoba, zodpovedná za správu archívov, vrátane archivácie údajov, papierovej a elektronickej archivácie;
- zaviesť postupy na zabezpečenie toho, aby boli počítačové systémy vhodné na zamýšľaný účel a boli overené, prevádzkované a udržiavané v súlade so zásadami SLP, vrátane funkcionalít spojených s integritou údajov;
- implementovať systémy, ktoré sú v súlade so súčasnými regulačnými požiadavkami; a
- zabezpečiť, aby sa identifikovali a zmiernili zvyškové riziká spojené s integritou údajov.

Zamestnanci útvaru zabezpečenie kvality

Zamestnanci útvaru zabezpečenia kvality (Quality Assurance Personnel /QA) majú vykonávať inšpekcie, aby sa zistilo, či sa všetky štúdie vykonávajú v súlade so zásadami SLP. To môže zahŕňať zber údajov, systémy zberu údajov, implementované opatrenia na riadenie údajov a súvisiace ŠPP a majú byť zahrnuté do programu kontroly zabezpečenia kvality testovacieho pracoviska.

5.5 ZÁKLADNÉ ČINNOSTI NA ZABEZPEČENIE INTEGRITY ÚDAJOV

1. TFM musí zabezpečiť, aby systémy implementované v testovacom pracovisku vytvárali údaje, ktoré sú priraditeľné, čitateľné, súčasné, pôvodné, presné, úplné, konzistentné, trvalé a dostupné (ALCOA+) vo všetkých formách, t. j. v papierovej aj elektronickej podobe. Vedúci štúdie musí overiť, či implementované systémy sú vhodné pre zabezpečenie integrity údajov štúdie.
2. Očakáva sa, že TFM zavedie plne zdokumentovaný systém s podporným zdôvodnením, ktorý poskytne prijateľný stav kontroly na základe rizika integrity údajov. Príkladom vhodného prístupu je vykonanie hodnotenia rizika integrity údajov, pri ktorom sú zmapované procesy, ktoré vytvárajú, spracúvajú a/alebo uchovávajú údaje, identifikuje sa každý z formátov a ich kontroly a zdokumentuje sa kritickosť údajov, inherentné riziká a ich vhodné zmiernenia. Prijateľné môžu byť aj iné zdokumentované prístupy k identifikácii a kontrole rizík integrity údajov.
3. Opatrenia, zavedené v testovacom pracovisku s ohľadom na organizáciu a zamestnancov, systémy a zariadenia, majú byť navrhnuté, prevádzkované a tam, kde je to vhodné, prispôsobené tak, aby podporovali vhodné pracovné prostredie, t. j. poskytovali vhodné prostredie na umožnenie fungovania účinných kontrol integrity údajov.
4. Riadenie údajov sa musí uplatňovať počas celého životného cyklu údajov, aby sa zabezpečila integrita údajov. Správa údajov sa má zaoberať vlastníctvom údajov a zodpovednosťou a zvážiť návrh, prevádzku a monitorovanie procesov/systémov, s cieľom splniť požiadavky na integritu údajov, vrátane kontroly nad všetkými zmenami údajov. Systémy správy údajov majú tiež zabezpečiť, aby boli údaje ľahko dostupné a prístupné. Elektronické údaje musia byť dostupné v čitateľnej forme.
5. Prístupy, používané na riadenie správy údajov, majú využívať techniky riadenia rizík, na zisťovanie rizík zlyhania integrity údajov v systémoch testovacieho pracoviska, na minimalizáciu potenciálneho rizika pre integritu údajov a na identifikáciu akéhokoľvek zvyškového rizika. Postupy, používané na riadenie správy údajov (napr. ŠPP), musia byť vždy schválené vedením testovacieho pracoviska. Účinnosť riadenia údajov musí byť pravidelne monitorovaná a hodnotená, tak často, ako to zadefinuje vedenie testovacieho pracoviska.
6. Očakáva sa, že vedenie testovacieho pracoviska zabezpečí primerané zdroje a školenia. Systémy správy údajov majú zahŕňať školenie zamestnancov o význame integrity údajov a vytvorenie pracovného prostredia, ktoré umožňuje transparentnosť a aktívne podporuje oznamovanie chýb, opomenutí a abnormálnych výsledkov.
7. Rizikami pre údaje môžu byť možnosti ich neúmyselného alebo úmyselného vymazania, doplnenia, ich zmeny alebo vylúčenia bez povolenia, alebo bez možnosti odhaliť takéto činnosti a udalosti. Riziká pre údaje môžu byť zvýšené zložitými, nekonzistentnými alebo chýbajúcimi procesmi s otvorenými a subjektívnymi výsledkami. Na zmiernenie takýchto rizík je potrebné stanoviť jednoduché, dobre definované úlohy, ktoré sa vykonávajú dôsledne a majú jasný cieľ.
8. Posúdenie rizika integrity údajov (alebo ekvivalent) má zvážiť všetky faktory potrebné na sledovanie procesu, alebo vykonávanie činnosti. Vedenie testovacieho pracoviska nominuje zamestnancov, ktorí vykonajú hodnotenia rizika a odporúča sa, aby ho vykonal

multidisciplinárny tím odborníkov na danú problematiku, ktorý môže zahŕňať členov so znalosťami procesov, vedúcich štúdií, špecialistov na informačné technológie (IT), QA a všetky ostatné relevantné funkcie. Očakáva sa, že sa bude posudzovať nielen systém izolovane, ale aj všetky podporné činnosti a funkcie, ako sú predpisy, procesy, rozhrania s inými systémami, ľudský zásah, školenia a systémy kvality. Automatizácia alebo používanie validovaného systému môže znížiť, ale nie eliminovať riziko pre integritu údajov. Tam, kde dochádza k zásahu človeka, najmä pri ovplyvňovaní toho, ako alebo aké údaje sa zaznamenávajú alebo oznamujú, môže dôjsť k zvýšenému riziku nedostatočnej kontroly alebo overenia údajov, v dôsledku prílišného spoliehania sa na validovaný stav systému.

9. Ak posúdenie rizika integrity údajov (alebo ekvivalent) identifikovalo oblasti na nápravu, potom určený tím má zdokumentovať stanovenie priorít opatrení, vrátane prijatia primeranej úrovne zvyškového rizika a oznámiť to na schválenie vedeniu testovacieho pracoviska. Majú sa vykonávať pravidelné kontroly hodnotenia rizík, aby sa zohľadnili implementované opatrenia a možné zmeny v procesoch. V situáciách, keď sú identifikované dlhodobé nápravné opatrenia, treba identifikovať, zdokumentovať a oznámiť na schválenie vedeniu testovacieho pracoviska krátkodobé opatrenia na zníženie rizika a implementovať ich tak, aby poskytovali prijateľnú úroveň kontroly pri správe údajov, kým sa nezavedie trvalejšie riešenie.
10. Regulačné rozhodovanie si vyžaduje, aby údaje štúdie boli relevantné a spoľahlivé. Kritickosť údajov sa môže určiť zvážením toho, ako údaje ovplyvňujú ciele, platnosť a súlad štúdie so SLP.
11. Úsilie a zdroje vynaložené na zabezpečenie integrity údajov majú byť primerané riziku a dopadu súvisiaceho so zlyhaním integrity údajov.
12. Testovacie pracoviská si musia byť vedomé toho, že vhodné kontroly integrity údajov sú potrebné tak pre počítačové systémy, ako aj pre systémy založené na papieroch, hoci kontroly nemusia byť rovnaké. Hybridné systémy možno použiť, ak sa preukáže ich schopnosť zabezpečiť integritu údajov (pozri tiež časť 7.3 „Prehľad údajov z hybridných systémov

5.6 POŽIADAVKY NA INTEGRITU ÚDAJOV POČAS ŽIVOTNÉHO CYKLU ÚDAJOV

5.6.1 Všeobecné požiadavky na údaje

Testovacie pracovisko musí mať primeranú úroveň porozumenia procesu a technických znalostí systémov používaných na zaznamenávanie údajov vrátane ich možností, obmedzení a zraniteľností.

Je nevyhnutné zabezpečiť pracovné prostredie, ktoré umožňuje vykonávanie úloh a zaznamenávanie údajov podľa potreby. Príkladom môže byť primeraný priestor, dostatok času na úlohy a správne fungujúce vybavenie.

Nasledujúce požiadavky sa vzťahujú na všetky údaje.

Údaje by mali byť:

A - priraditeľné osobe, ktorá generuje/upravuje/kontroluje údaje

L - čitateľné

C - súčasné

O - originálny záznam (alebo jeho overená kópia)

A - presné

Opatrenia na riadenie údajov majú tiež zabezpečiť, aby údaje boli úplné, konzistentné, trvalé a dostupné počas celého životného cyklu (ALCOA+), kde:

Kompletné - údaje musia byť celé, kompletný súbor

Konzistentné - údaje musia byť konzistentné a bez rozporov medzi sebou

Trvalé - trvalé, trvajúce počas celého životného cyklu údajov

Dostupné - ľahko dostupné

Vygenerované údaje musia byť v čase zaznamenávania identifikované jednotlivcom (osobou) zodpovednou za zadávanie údajov.

Návrh počítačového systému má vždy zabezpečiť uchovanie úplných záznamov audit trailu, aby sa zobrazili všetky zmeny údajov bez zakrytia pôvodného záznamu. Musí byť možné spojiť všetky zmeny údajov s osobou, ktorá tieto zmeny vykonala, a dátumom, kedy boli vykonané, napríklad pomocou audit trailu údajov alebo ekvivalentných mechanizmov alebo časovaných a datovaných (elektronických) podpisov. Dôvod zmien musí byť uvedený.

5.6.2 Generovania, zbieranie alebo zaznamenávanie primárnych údajov

Primárne údaje získané počas vykonávania štúdie sa musia zaznamenávať priamo, rýchlo, čitateľne a presne. Všetky primárne údaje musia byť podpísané a datované, či už elektronicky alebo na papieri alebo na inom médiu. Ak sa primárne údaje generujú ako výsledok priameho zadávania z počítača (napr. zadaním hodnoty), nespracované údaje musia byť identifikované podľa identity osoby zodpovednej za záznam a podľa času zadania.

Ak sa pôvodné elektronicky zozbierané údaje nepovažujú za primárne údaje, musí to byť zdôvodnené a zdokumentované.

Manuálne zaznamenávanie

Údaje zaznamenané manuálne môžu vyžadovať nezávislé overenie na základe hodnotenia rizika integrity údajov alebo iných požiadaviek. Príklady môžu zahŕňať priebežné (alebo v krátkom čase) overovanie zadávania údajov druhou osobou, alebo krížové kontroly súvisiacich zdrojov informácií (napríklad denníky zariadení, údaje testovacieho systému atď.), alebo preskúmanie údajov. Úroveň kontroly má byť primeraná identifikovanému riziku chyby pri manuálnom zaznamenávaní.

Manuálne pozorovania majú byť priamo a priebežne zaznamenávané pozorovateľom. Ak existuje potreba potvrdiť manuálne pozorovania (napr. z dôvodu ich vysokej kritičnosti pre platnosť štúdie), možno zvážiť ďalšie opatrenia na preukázanie integrity údajov (ako je urobenie snímky alebo prítomnosť svedka na potvrdenie pozorovanie). Záznamy o dodatočných činnostiach, ktoré vykonal pozorovateľ a prípadne svedok, sa musia uchovávať ako dodatočné údaje k prvotným údajom zaznamenaným pozorovateľom.

Použitie zapisovačov na súčasné zaznamenávanie činnosti v mene iného pracovníka, ktorý danú činnosť vykonáva, možno zvážiť v odôvodnených prípadoch, napríklad:

- Vykonávanie záznamu v čase vykonávania danej činnosti, ju môže ohroziť (napr. dokumentovanie prípravy testovanej látky za sterilných podmienok personálom štúdie).

- Vyšetrovanie živých testovacích systémov.

Záznam druhou osobou má byť vykonávaný súbežne s vykonávanou úlohou a v záznamoch musí byť identifikovaný tak pracovník štúdie vykonávajúci úlohu, ako aj osoba, ktorá záznam urobila. Pracovníci štúdie vykonávajúci úlohu musia záznam kontrasignovať, aby sa formalizovala skutočnosť, že činnosť vykonali (nie akceptáciu zaznamenaných údajov). Proces dokončenia dokumentácie zapisovateľom má byť opísaný v ŠPP, v ktorom majú byť špecifikované aj činnosti, na ktoré sa tento proces vzťahuje.

Aktuálne verzie šablón alebo formulárov používaných na zaznamenávanie primárnych údajov musia byť dostupné na miestach, kde prebiehajú činnosti, aby sa údaje dali rýchlo zaznamenať. Počet použitých formulárov/šablón v porovnaní s počtom dostupných vyplnených sa má kontrolovať, aby sa predišlo duplicite a aby sa podporila identifikácia problémov s integritou údajov, ako je zisťovanie znovuvytvorenia alebo prepis záznamu. Ak sú šablóny alebo formuláre na zaznamenávanie údajov dostupné vytlačením, počet výtlačkov musí byť kontrolovaný.

Posúdenie rizika má určiť potrebnú úroveň kontroly a absencia úplnej kontroly a zosúladenia sa musí odôvodniť hodnotením rizika, aby sa určilo, prečo sú niektoré situácie vyňaté z tejto požiadavky.

Používanie čistých papierových formulárov na zaznamenávanie primárnych údajov má byť obmedzené a kontrolované, ale malo by byť tiež dostupné, aby sa umožnilo priebežné zaznamenávanie neočakávaných udalostí. Musí sa zaviesť kontrola a zosúladenie medzi dostupnými súbormi prázdnych formulárov na začiatku a po vyplnení všetkých vydaných formulárov (napr. číslovaním). Vhodným riešením môže byť použitie očíslovaných stránkovaných kníh, aby bolo možné zistiť odstránenie strán. Posúdením rizika sa určí potrebná úroveň kontroly a absencia úplnej kontroly a zosúladenia sa musí zdôvodniť.

Napriek tomu, systém implementovaný na kontrolu prístupu k formulárom má umožňovať ľahkú dostupnosť správneho dokumentu, aby sa predišlo prípadnému nesprávnemu záznamu údajov na neschválenom formulári a následne nesprávnemu prepisu.

Údaje generované ako priamy počítačový vstup majú byť identifikované v čase zadávania údajov jednotlivcom (osobami) zodpovednými za priame zadávanie údajov.

V prípade elektronických údajov by prístup k aplikáciám nemal brániť súčasnému zaznamenávaniu údajov. Prístupové práva používateľov musia zabrániť neoprávnenému vkladaniu údajov.

Automatické zaznamenávanie

Externé zariadenia alebo metódy, ktoré eliminujú manuálne zadávanie údajov a ľudskú interakciu s počítačovým systémom, ako sú skenery čiarových kódov, čítačky ID kariet alebo tlačiarne, možno použiť až po ich validácii.

Riziká súvisiace s integritou údajov môžu závisieť od toho, do akej miery možno nakonfigurovať a overiť zariadenia alebo počítačové systémy, ktoré automaticky zachytávajú, zaznamenávajú alebo generujú údaje, a od možnosti manipulácie alebo straty údajov v rámci systému.

Hybridné systémy

V prípade základného elektronického zariadenia, ktoré neuchováva elektronické údaje alebo poskytuje iba tlačený výstup údajov (napr. určité typy váh alebo pH metre), potom výtlačok predstavuje primárne údaje.

Ak elektronické zariadenie uchováva elektronické údaje, ale uchováva len určitý objem údajov pred ich prepísaním ďalšími, musí sa vynaložiť maximálne úsilie na extrakciu a kontrolu údajov a metaúdajov ako elektronických údajov. Vytlačenie na papier, ak je okamžite podpísané a datované, alebo jeho transformácia do iného formátu je prijateľná, ak sa nestratia žiadne informácie. Údaje (vrátane metaúdajov) v ich uchovávanom formáte sa musia overiť pred ich vymazaním z elektronického zariadenia.

Iné médiá

Údaje môžu byť zachytené fotografiou alebo zobrazovacími metódami a technológiami (prípadne inými médiami), požiadavky na vysledovateľnosť záznamu zostávajú rovnaké.

Zaznamenávanie do textových súborov (flat files)

Bežné textové súbory zväčša neumožňujú zistenie totožnosti osoby, ktorá do nich zaznamenala údaje, ani dátum a čas, kedy sa to stalo. Niektoré súbory môžu mať priradené základné metaúdaje, napr. čas vytvorenia a čas poslednej zmeny, tieto ale nie sú dostatočné pre potreby audit trailu. Takéto súbory sa preto nemajú používať na priame zaznamenávanie ani uchovávanie primárnych údajov.

Ak je nutné používanie takýchto súborov a kontrola údajov sa nedá zabezpečiť alternatívnou metódou, potom je nutné prijať opatrenia na zníženie rizika, ktoré z používania takýchto súborov vyplýva. Medzi takéto opatrenia patrí napr. šifrovanie, kontrola prístupu k lokalite, kde sa súbory nachádzajú, alebo technické riešenia, pomocou ktorých sa dajú zvonka priebežne odhaliť a zaznamenávať všetky zmeny urobené v súbore.

5.6.3 Metaúdaje

Aby mali primárne údaje plný význam, vyžadujú si metaúdaje a sú považované za súčasť údajov (pozri tiež časť 5.6.13 „Sledovanie zmien“).

Metaúdaje sa musia generovať súčasne s údajmi a uchovávať so súvisiacimi údajmi.

5.6.4 Elektronické podpisy

Elektronický podpis je rovnocenný s vlastnoručným podpisom podpisovateľa a môže sa použiť na vyjadrenie schválenia, autorizácie alebo overenia špecifických údajov.

Aby sa zabezpečila integrita údajov, používanie elektronických podpisov musí byť primerane kontrolované s ohľadom na to:

- ako možno podpis pripísať jednotlivcovi a účelu, na ktorý sa používa (napr. schválenie, overenie, potvrdenie);
- ako je akt podpisu zaznamenaný v systéme tak, aby ho nebolo možné zmeniť alebo s ním manipulovať bez toho, aby sa znehodnotil podpis alebo stav záznamu;
- ako je zaznamenaný čas a dátum podpisu spolu s menom vlastníka a významom podpisu;
- ako bude záznam podpisu spojený s vykonaným záznamom a ako to možno overiť; a
- ako je zabezpečená bezpečnosť elektronického podpisu, t. j. aby ho mohol použiť iba vlastník tohto podpisu.

Vložený obrázok podpisu alebo poznámka pod čiarou označujúca, že dokument bol elektronicky podpísaný (ak bol vložený iným spôsobom ako overený elektronický podpis), nepostačujú.

Ak sa, v súvislosti s funkcionalitou elektronického podpisu, tradičná autentifikácia pozostávajúca z ID užívateľa a tajného hesla nahradí biometrickou autentifikáciou (napr. snímač odtlačkov prstov, ruky, tváre alebo dúhovky), takéto implementované riešenie musí byť dôkladne validované a zdokumentované.

(Pozri tiež časť 3.9 dokumentu *OECD Document No 17 (OECD, 2016[4]).*)

5.6.5 Generovanie overovanie/verifikovaných kópií

Verifikovaná kópia údajov (bez ohľadu na typ použitého média) musí byť potvrdená (t.j. zdokumentovaná s datovaným podpisom alebo generovaním prostredníctvom validovaného procesu), aby obsahovala rovnaké informácie, vrátane údajov, ktoré opisujú kontext, obsah a štruktúru, ako pôvodné údaje. Originály a verifikované kópie musia zachovať integritu (presnosť, úplnosť, obsah a význam) údajov.

Verifikácia musí byť pripísaná osobe, ktorá overenie vykonáva. Dátum (a prípadne čas, ak je to potrebné) vytvorenia overenej kópie sa má uchovávať spolu s príslušnou kópiou.

Elektronickú overenú kópiu údajov zaznamenaných na papieri možno vygenerovať za predpokladu, že existuje zdokumentovaný proces, ktorý zabezpečí, že výsledkom bude overená kópia.

5.6.6 Oprava alebo doplnenie údajov

Akákoľvek zmena v primárnych údajoch má byť vykonaná tak, aby nezakryla predchádzajúci záznam, má obsahovať dôvod zmeny a musí byť datovaná a podpísaná alebo parafovaná osobou, ktorá zmenu vykonala.

Pre údaje, generované ako priamy počítačový vstup, by mal počítačový systém vždy umožňovať uchovávanie úplných záznamov auditu trailu/sledovania zmien, aby sa zobrazili všetky zmeny údajov bez zakrytia pôvodného záznamu. Všetky zmeny údajov musí byť možné priradiť k osobám, ktoré tieto zmeny vykonali, napríklad pomocou časovaných a datovaných (elektronických) podpisov (pozri tiež časť 5.6.13 „Sledovanie zmien“). Je potrebné uviesť a zaznamenať dôvod zmien.

5.6.7 Prepis

Treba sa vyhnúť prepisom, pretože zvyšujú riziko chýb a nezrovnalostí. Ak sa prepisom nedá vyhnúť, má ich overiť druhá osoba alebo ich musí vykonať validovaný systém. Pôvodné záznamy sa považujú za primárne údaje a musia sa uchovávať.

5.6.8 Zrušenie platnosti alebo vylúčenia údajov

Údaje možno zrušiť alebo vylúčiť len vtedy, ak je možné preukázať, na základe riadneho vedeckého alebo technického zdôvodnenia alebo logického zmyslu, že údaje nie sú reprezentatívne pre zaznamenanú udalosť. Relevantnými príkladmi sú napr. vyradenie analytických výsledkov v dôsledku poruchy zariadenia, alebo zneplatnenie klinického pozorovania uhynutého zvieraťa.

Je potrebné nájsť príčiny generovania údajov, ktoré musia byť zrušené alebo vylúčené. Vo všetkých prípadoch sa opodstatnenosť zneplatnenia alebo vylúčenia údajov musí zdokumentovať a zohľadniť počas preskúmania údajov a písania správ. Pre bežné prípady (napr. nekoherentné analytické výsledky pre jednu vzorku alebo nesplnenie akceptačných kritérií) sa pravidlá na vylúčenie alebo znehodnotenie údajov majú definovať vopred v pláne štúdie alebo v ŠPP. Všetky údaje (aj keď sú zneplatnené) sa majú uchovávať so súborom údajov a musia byť k dispozícii na preskúmanie vo formáte, ktorý umožňuje potvrdiť platnosť rozhodnutia o zneplatnení alebo vylúčení údajov.

5.6.9 Spracovanie údajov

V rámci spracovania údajov musí existovať primeraná vysledovateľnosť akýchkoľvek parametrov definovaných používateľom, vrátane priradenia toho, kto danú činnosť vykonal. Príklady zahŕňajú výpočty alebo (s príslušnými povoleniami na prístup) výber a aplikáciu parametrov chromatografickej integrácie alebo výber parametrov na analýzu testu prietokovej cytometrie. Pravidlá spracovania údajov majú byť jasne definované a kontrolované štandardnými pracovnými postupmi.

Primárne údaje a dostupné záznamy o sledovaní zmien (audit trail procesu) procesu sa musia uchovávať. Uchovávané záznamy musia umožniť rekonštrukciu všetkých činností spracovania údajov bez ohľadu na to, či sa výstup tohto spracovania následne dostane do správy. Ak sa spracovanie údajov opakovalo s postupnou úpravou parametrov spracovania, musí to byť viditeľné so zdokumentovaným odôvodnením, aby sa zabezpečilo, že parametre spracovania sa neupravovali s cieľom dosiahnuť želanejší koncový bod.

5.6.10 Migrácia údajov

Postupy migrácie údajov majú obsahovať odôvodnenie a majú byť dôkladne navrhnuté a overené, aby sa zabezpečilo zachovanie integrity údajov počas životného cyklu údajov. Pozorne sa musí zvážiť pochopenie formátu údajov a možnosti zmeny v každej fáze generovania údajov, migrácie a následného uchovávania. Musia byť zavedené opatrenia na zabezpečenie a preukázanie toho, že údaje sa nemenia počas žiadneho kroku procesu.

Problémy spojené s migráciou údajov sa často podceňujú, najmä pokiaľ ide o zachovanie plného významu a integrity záznamov vrátane súvisiacich metadát.

V prípade migrácie od jednej strany („odosielateľ“) na inú („príjemca“), údaje a súvisiace metadáta, dátum/čas migrácie, očakávaný formát a špecifikácia prenosového protokolu alebo zmluvy použitej na migráciu údajov majú byť definované pred migráciou. Mechanizmy komunikácie a koordinácie medzi odosielateľom a príjemcom musia byť zavedené, aby sa zabezpečilo, že prijaté dáta budú mať rovnaké atribúty ako odosielané dáta.

(Pozri tiež časť 2.8 dokumentu *OECD Document No 17 (OECD, 2016[4])*.)

5.6.11 Relačná databáza

Načítanie informácií z relačnej databázy vyžaduje databázový reportovací nástroj alebo pôvodnú aplikáciu, ktorá záznam vytvorila.

Úpravy údajov sa nemajú vykonávať priamo v poliach databázy, ale majú sa vykonávať prostredníctvom softvérového balíka pôvodcu, aby zostali v platnosti príslušné záznamy o audit traile a kontrole. Ak sa však vyžaduje zmena údajov správcom systému priamo v databáze, musí byť zmena odôvodnená, kontrolovaná, zdokumentovaná, so súhlasom vedúceho štúdie a proces musí byť opísaný v ŠPP.

Prístupové práva na vstup do databázy alebo zmeny a doplnenia musia byť kontrolované a v súlade s požiadavkami na prístup používateľov do počítačového systému/role správcu systému

(Pozri tiež časť 5.8.2 „Prístup do počítačových systémov a roly“.)

5.6.12 Počítačové systémové transakcie

Transakcia počítačového systému, kde parameter musí byť v rámci definovaného limitu, rozsahu alebo distribúcie, aby sa zabezpečila kvalita údajov, sa považuje za kritickú. Počítačové systémy majú byť navrhnuté tak, aby zabezpečili, že vykonávanie takýchto transakcií sa bude zaznamenávať priebežne. Ak sa používajú transakčné systémy, má sa zabrániť kombinovaniu viacerých jednotkových operácií do jednej kombinovanej transakcie (napríklad viacnásobné zadávanie údajov pred uložením) a časové intervaly pred uložením údajov sa majú minimalizovať. Systémy majú byť navrhnuté tak, aby vyžadovali uloženie údajov do trvalej pamäte pred výzvou používateľovi na vykonanie zmien. Výnimky z týchto požiadaviek majú byť odôvodnené.

Vedenie testovacieho pracoviska musí počas vývoja systému (napr. prostredníctvom špecifikácie požiadaviek používateľa) definovať, aké kritické transakcie sú s týmto systémom spojené na základe funkcionality a úrovni rizika spojeného so systémom. Kritické transakcie majú byť zdokumentované pomocou procesných kontrol, ktoré zohľadňujú návrh systému (prevenciu), spolu s procesmi monitorovania a kontroly. Dohľad nad aktivitami má upozorniť na zlyhania, ktoré nie sú riešené v návrhu procesu. Činnosti dohľadu nad kritickými transakciami sú považované za súčasť programu kontroly kvality.

5.6.13 Sledovanie zmien

Ak sa počítačové systémy používajú na zbieranie, spracovanie, úpravu, oznamovanie, uchovávanie alebo archiváciu údajov elektronicky, návrh systému musí vždy umožňovať uchovávanie revíznych záznamov/audit trial na zobrazenie všetkých zmien alebo vymazania údajov pri zachovaní predchádzajúcich údajov. Všetky údaje a zmeny údajov má byť možné priradiť k osobám, ktoré tieto zmeny vykonali a zmeny majú byť označené dátumom a časovou pečiatkou (čas a prípadne aj časového pásma, ak je to potrebné). Treba zaznamenať aj dôvod

zmeny. Položky zahrnuté v audit trail/revíznom zázname majú byť relevantné, aby umožnili rekonštrukciu procesu alebo činnosti.

Kontrolné záznamy/audit trail majú byť počas činností SLP vždy zapnuté. Žiadny personál s priamym záujmom o údaje (vedúci štúdií, vedúci analytických oddelení, pracovníci štúdie, atď.) nesmie mať možnosť upravovať alebo vypínať funkčnosť audit trailu. Ak správca systému zmení alebo vypne funkciu audit trail, audit trail to má zaznamenať automaticky a automaticky sa to má zaznamenať aj vtedy, keď bude funkcia audit trailu opäť zapnutá.

Ak príslušná funkcia audit trail neexistuje alebo systémy nespĺňajú očakávania audit trail a jednotlivých používateľských účtov (napríklad v rámci starších systémov), pri riešení týchto nedostatkov musí byť k dispozícii preukázaný pokrok (ako sa situácia bude riešiť). Malo by to byť buď prostredníctvom doplnkového softvéru, ktorý poskytuje tieto dodatočné funkcie, alebo inováciou na vyhovujúci systém. Náprava musí byť identifikovaná a vykonaná včas.

Ak systém nemá možnosť pre audit trail a preskúmanie dostupných systémov nedokáže identifikovať alternatívy a technologické úpravy alebo doplnky k existujúcemu systému (t.j. náprava nie je možná), musí to byť odôvodnené dôkazom, že sa pracuje na vyhovujúcom riešení a aké aktivity na zmiernenie, ako napríklad alternatívna úroveň kontroly, dočasne podporujú ďalšie používanie. Alternatívne úrovne kontroly možno dosiahnuť napríklad použitím manuálnych denníkov alebo definovaním striktne obmedzených prístupových práv do systému. Ak je zabezpečená integrita údajov, vrátane metadát, môžu sa zvážiť aj výtlačky údajov. Musí byť preukázané, že alternatívne kontrolné opatrenia sú účinné, založené na hodnotení rizika, definované v ŠPP a sú pravidelne prehodnocované.

Niektoré orgány monitorujúce dodržiavanie zásad SLP nemusia akceptovať systémy bez funkcie audit trail, vrátane tých s alternatívnymi kontrolnými opatreniami.

(Pozri tiež časť 3.4 dokumentu *OECD Document No 17 (OECD, 2016[4])*.)

5.6.14 Uchovávanie údajov

Je potrebné zbierať a uchovávať údaje, ktoré umožnia úplnú rekonštrukciu činností počas vykonávania štúdie. Údaje sa majú uchovávať s príslušnými metaúdajmi, kde je to potrebné. Odvodené údaje sa majú uchovávať s príslušnými primárnymi údajmi, ak je to potrebné na rekonštrukciu štúdie.

Opatrenia na uchovávanie údajov a dokumentov musia zabezpečiť ochranu záznamov pred zamýšľanou alebo neúmyselnou zmenou alebo stratou. Na zabezpečenie integrity údajov záznamu počas obdobia uchovávania musia byť zavedené bezpečnostné kontroly.

Zvolená metóda uchovávania musí zabezpečiť, aby sa údaje primeranej presnosti, úplnosti, obsahu a významu zhromažďovali a uchovávali na zamýšľané použitie.

Uchovávanie dynamických údajov

Informácie, ktoré sú zachytené v dynamickom stave, musia zostať dostupné v rovnakom stave. Napríklad videozáznam používaný na preukázanie nejakej aktivity nemožno zredukovať na jeden statický obrázok alebo na sériu jednotlivých obrázkov.

Počítačové systémy, ktoré generujú dynamické záznamy, majú umožňovať uchovávanie dynamickej povahy údajov.

Tlačiť dynamické záznamy na papier bez straty interaktívneho vzťahu medzi používateľom a obsahom záznamu môže byť problém.

Všetky výtlačky by mali obsahovať všetky súvisiace dostupné metaúdaje a mali by zachovať prepojenie, ktoré ich spája s nespracovanými údajmi. Napríklad, ak sú súvisiace metaúdaje vytlačené na inej stránke ako primárne údaje, integrita prepojenia nie je zabezpečená a vzťah k primárnym údajom je otázny.

Ak elektronické nespracované údaje nemožno previesť na overené kópie (napr. vytlačiť alebo vo formáte PDF) bez straty informácií (napr. súvisiacich metaúdajov), musia zostať dostupné v pôvodnom stave.

Ak nie je možné udržiavať počítačový systém, napr. ak už nie je podporovaný, záznamy sa budú archivovať podľa zdokumentovanej stratégie archivácie pred vyradením počítačového systému z prevádzky. Je možné, aby sa niektoré údaje generované elektronickými prostriedkami uchovávali v prijateľnom papierovom alebo elektronickom formáte, ak je možné dokázať, že statický záznam zachováva integritu primárnych údajov. V procese uchovávania údajov však musí byť preukázané, že zahŕňa overené kópie všetkých primárnych údajov, metaúdajov, relevantných záznamov z audit trail a súbory výsledkov, akékoľvek variabilné nastavenia konfigurácie softvéru/systému špecifické pre každý záznam a všetky spracovania údajov (vrátane metód a záznamov z audit trail), potrebné na rekonštrukciu daného súboru primárnych údajov.

Keď je zvoleným riešením tlač na papier, vyžaduje sa, pomocou nejakého validovaného postupu, overenie, že vytlačené záznamy presne reprezentujú súbor údajov.

Všetky informácie sa musia uchovávať. Akákoľvek strata informácií sa musí identifikovať a riziko pre integritu súboru údajov posúdiť a zdokumentovať.

Zachovanie elektronického podpisu

Elektronicky podpísaný dokument je vo všeobecnosti dynamický záznam. Ak je dokument podpísaný elektronicky, metadáta spojené s podpisom (t. j. vytlačené meno podpisovateľa, význam podpisu a dátum a čas podpisu) sa uchovávajú elektronicky. Dokument, ktorý je podpísaný elektronicky, je platný iba vtedy, ak je uchovávaný elektronicky, pokiaľ papierový výtlačok alebo kópia vo formáte pdf nezachováva všetku vysledovateľnosť identity podpisujúceho, dátumu, času a významu podpisu.

Zachovanie elektronickej komunikácie

Elektronická komunikácia je ďalším príkladom záznamov v dynamickom stave.

Ak sú údaje podporované elektronickou komunikáciou, ako sú e-mail a elektronické správy (napr. umožňujúce overenie SLP činností a zodpovedností), musia byť zavedené postupy na zabezpečenie uchovávania a porovnávania elektronickej komunikácie (vrátane ubezpečenia, že záznamy sú úplné a integrita neporušená). Takéto mechanizmy treba navrhnúť tak, aby sa zachovala priraditeľnosť a integrita týchto príslušných elektronických komunikácií, ako napríklad zabezpečenie toho, aby bolo možné určiť odosielateľa a príjemcu spolu s príslušnými dátumami a časmi. Akékoľvek prílohy musia zostať spojené s príslušnou správou a reťazce správ sa majú zachovať.

Ak je to možné, majú sa zachovať v pôvodnom formáte, ale ak to nie je možné, vedenie testovacieho pracoviska musí zaviesť procesy na verný prepis a overenie v formáte, v ktorom budú uchované.

Výtlačok na papieri alebo migrácia elektronickej komunikácie vo formáte pdf nemôže zabezpečiť požadovanú integritu.

Uchovávanie verifikovaných (overených) kópií

Verifikované kópie z elektronických dynamických záznamov (vygenerované migráciou) sa majú uchovávať v dynamickom stave, aby verifikovaná kópia mohla obsahovať metaúdaje (napr. formáty dátumu, kontext, rozloženie, elektronické podpisy a autorizácie) potrebné na zabezpečenie toho, že úplný význam údajov sa uchováva a históriu dynamického záznamu, vrátane vytvorenia overenej kópie, je možné rekonštruovať.

Verifikované kópie sa môžu ponechať namiesto originálu za predpokladu, že je zavedený dokumentovaný systém na overenie a zaznamenanie integrity kópie. Je potrebné zvážiť akékoľvek riziko spojené so zničením pôvodných záznamov. Treba si byť vedomý toho, že niektoré regulačné orgány vyžadujú, aby sa originály uchovávali.

Uchovávanie údajov z hybridných systémov

Ak sa vyžaduje použitie hybridných systémov, musí byť jasne zdokumentované, čo tvorí celý súbor údajov, a v ŠPP definovať, ktoré záznamy sa budú uchovávať.

Uchovávanie údajov na iných médiách

Ak sú údaje zachytené fotografickými alebo zobrazovacími metódami a technológiami (alebo inými médiami), požiadavky na uchovávanie tohto formátu počas jeho životného cyklu sa riadi rovnakými úvahami ako pre všetky iné údaje, pričom treba zvážiť dodatočné kontroly vyžadované pre daný formát. Ak nie je možné zachovať pôvodný formát kvôli problémom s degradáciou, treba zvážiť alternatívne mechanizmy záznamu vrátane overenia vernosti procesu (napr. fotografovanie alebo digitalizácia) a následného uloženia a zdokumentovať odôvodnenie výberu.

5.6.15 Zálohovanie

Je potrebné zvážiť mechanizmy na zabezpečenie kontroly úspešného dokončenia záloh. Používané systémy musia byť validované a každá záloha overená, aby sa zabezpečilo, že funguje správne, napr. potvrdením, že veľkosť údajov a ďalšie skopírované vlastnosti sa zhodujú s veľkosťou pôvodného záznamu.

Procesy zálohovania a obnovy elektronických údajov sa majú testovať v prípade potreby. Napríklad, keď dôjde k zmenám buď v procese alebo v nástrojoch alebo aplikáciách používaných počas zálohovania alebo obnovy. Okrem toho je potrebné pravidelne overovať funkčnosť niektorých elektronických médií používaných na zálohovanie (ako sú CD, DVD atď.).

Postupy zálohovania majú byť opísané v ŠPP a činnosti zálohovania zdokumentované.

Zálohy na účely obnovy nenahrádzajú potrebu archivácie dát a metadát pre účely rekonštrukcie činnosti počas vykonávania štúdie.

5.6.16 Archív

Údaje sa musia archivovať bezpečne, pod kontrolou vymenovaného archivára, vrátane, ak je to relevantné, vhodného elektronického úložiska, či už je to v pôvodnom systéme alebo inde, pod náležitou kontrolou alebo v samostatnom elektronickom archíve.

Všetky archívne miesta (fyzické aj elektronické) v ktorých sa archivujú údaje, musia byť identifikované a zdokumentované.

Zásady SLP pre archiváciu sa musia dôsledne uplatňovať na elektronické a neelektronické údaje. Je preto dôležité, aby sa elektronické údaje uchovávali s rovnakými úrovňami kontroly prístupu a indexovania ako neelektronické údaje.

Archivovanými záznamami môžu byť originálny záznam a/alebo overená/verifikovaná kópia (pozri tiež časť 5.6.14 „*Uchovávanie verifikovaných (overených) kópií*“) a musia byť chránené tak, aby ich nebolo možné zmeniť alebo vymazať bez odhalenia takejto činnosti.

Archívne opatrenia musia byť navrhnuté tak, aby umožňovali vyhľadávanie a čitateľnosť údajov a metaúdajov počas požadovaného obdobia uchovávania.

Keď staršie systémy už nie je možné podporovať, musí sa zvážiť dôležitosť údajov a v prípade potreby aj údržba softvéru na účely dostupnosti údajov. To sa dá dosiahnuť udržiavaním softvéru vo virtuálnom prostredí. Ak to nie je možné, údaje je potrebné pred archiváciou preniesť (migrácia údajov) kontrolovaným, otestovaným a verifikovaným spôsobom do systému, v ktorom budú naďalej dostupné. Migrácia na alternatívny formát súboru, ktorý zachováva verifikované kópie atribútov údajov, môže byť potrebná so zvyšujúcim sa vekom starších údajov.

Ak migrácia s plnou funkčnosťou pôvodného záznamu nie je technicky možná, výber z dostupných možností musí byť založený na riziku a dôležitosti údajov v čase. Formát migračného súboru sa musí zvoliť s prihliadnutím na rovnováhu rizika medzi dlhodobou dostupnosťou a možnosťou zníženej funkčnosti dynamických údajov (napr. skúmanie údajov, sledovanie trendov, opätovné spracovanie atď.). Uznáva sa, že potreba zachovať prístupnosť môže vyžadovať migráciu do formátu súboru, ktorý stráca niektoré atribúty a/alebo funkčnosť dynamických údajov. Je zodpovednosťou vedenia testovacieho pracoviska posúdiť vplyv takýchto strát a udržiavať prepojenie medzi čitateľným audit trialom alebo elektronickými podpismi a auditovanými údajmi na prijateľnej úrovni.

(Pozri tiež časť 3.11 dokumentu *OECD Document No 17 (OECD, 2016[4]).*)

5.7 PRESKÚMANIE ÚDAJOV

5.7.1 Všeobecné úvahy

Preskúmanie údajov pozostáva z vhodných overení kritických údajov pre kontrolu kvality, ktoré môžu vykonávať vedúci štúdií alebo iní pracovníci.

Ciele kontroly údajov sú:

- zistiť akékoľvek vymazanie, doplnenie, zmenu alebo vylúčenie;
- pre vedúcich štúdií, aby skontrolovali, či sú všetky vytvorené prvotné údaje plne zdokumentované a zaznamenané; a

- posúdiť efektívnosť opatrení správy údajov preskúmaním úplného súboru údajov generovaného prostredníctvom procesov počas životného cyklu údajov.

Aby bola úroveň kontroly údajov a jej rozsah efektívna, treba ju definovať prostredníctvom hodnotenia rizika. Identifikované kritické údaje musia byť preskúmavané prostredníctvom kritických krokov životnosti údajov. Preskúmanie údajov má zahŕňať aj preskúmanie relevantných metaúdajov vrátane revíznych záznamov (audit trail) alebo ich prvkov.

Kontrola údajov musí byť zdokumentovaná. Záznam o preskúmaní má obsahovať akékoľvek odchýlky od zásad SLP, plánov štúdií alebo ŠPP, ktoré sa zistili počas preskúmania, dátum vykonania preskúmania a podpisy osôb vykonávajúcich preskúmanie.

Musí existovať postup, ktorý opisuje proces kontroly údajov. Postup musí tiež opísať opatrenia, ktoré sa majú prijať, ak sa pri preskúmaní údajov zistia odchýlky. Tento postup má umožniť opravy alebo objasnenia údajov tak, aby sa zabezpečila viditeľnosť pôvodného záznamu a kontrola sledovania opravy pomocou audit trail.

Mnoho softvérových balíkov umožňuje konfiguráciu reportov na podporu kontroly údajov. Zmeny konfigurácie reportu (zostavy) musia byť kontrolované, aby sa zabránilo neoprávneným zmenám. Systém musí byť validovaný a v prípade potreby výstupy reportov verifikované.

Poznámka: Preskúmanie údajov, ktoré vykonala QA, má za cieľ podporiť tvrdenie, že hlásené výsledky presne a úplne odrážajú primárne údaje zo štúdií. Môže byť účinné aj pri audite postupov riadenia integrity údajov. Úroveň kontroly musí byť naviazaná na kritickosť údajov.

5.7.2 Preskúmanie záznamov zo sledovania zmien/údajov z audit trail

Nie je potrebné, aby kontrola cez audit trail zahŕňala každú aktivitu systému.

Je potrebné identifikovať relevantné údaje medzi všetkými uchovávanými údajmi v záznamoch audit trailu, aby sa umožnilo dôkladné preskúmanie/overenie údajov. Preskúmanie musí byť vykonávané podľa zdokumentovaného postupu založeného na riziku, ktorý identifikuje kritickosť údajov, ktoré sú predmetom preskúmania, a kritickosť transakcií identifikovaných prostredníctvom toku údajov. Preskúmanie možno vykonať priamym prístupom do systému audit trail alebo použitím vhodne navrhnutých a overených systémových reportov.

Rutinné preskúmanie údajov má zahŕňať zdokumentované preskúmanie záznamov audit trail, ako sa určí na základe hodnotenia rizika. Pri navrhovaní systému na preskúmanie záznamov zo sledovania zmien (audit trail) sa preskúmanie môže obmedziť len na tie činnosti, ktoré sú relevantné pre SLP (napr. súvisiace s vytváraním údajov, spracovaním, dodržiavaním postupov, modifikáciou a vymazávaním atď.). Záznamy auditu možno preskúmať ako zoznam relevantných údajov alebo prostredníctvom procesu „nahlasovania výnimiek“. Správa o výnimkách je validovaný vyhľadávací nástroj, ktorý identifikuje a dokumentuje vopred určené „nenormálne“ údaje alebo činnosti, ktoré si vyžadujú ďalšiu pozornosť alebo preskúmanie zo strany kontrolóra údajov.

Kontrolujúci pracovníci musia mať dostatočné znalosti a systémový prístup na preskúmanie relevantných záznamov audit trailu, primárnych údajov a metaúdajov.

5.7.3 Preskúmanie údajov z hybridných systémov

Pre hybridné systémy sa vyžaduje zvýšená kontrola údajov, pretože sú citlivé na nepriraditeľné zmeny údajov. Všetky záznamy z hybridných systémov, ktoré sú definované súborom údajov musia byť preskúmané kvalifikovanou osobou. Úroveň tejto kontroly musí byť prispôsobená procesom používaným v hybridnom systéme. Preskúmanie údajov z hybridných systémov musí byť jasne definované a opísané, aby bolo možné určiť skutočné zdroje preskúmaných údajov.

5.8 PRÍSTUP K ÚDAJOM

5.8.1 Všeobecné úvahy

Prístupové práva k údajom a záznamom musia byť vždy vytvorené na základe hodnotenia rizika každej fázy životného cyklu údajov.

Prístupové právo musí byť definované tak, aby umožnilo zamestnancom plniť si povinnosti SLP.

Prístup k záznamom pre zamestnancov vykonávajúcich činnosti kontroly údajov musí byť zachovaný.

Potrebný prístup (vrátane záznamov, kontrolných záznamov (audit trail) a funkčnosti systému), povolenia a školenia musia byť k dispozícii na podporu inšpekcií útvaru zabezpečenia kvality (QA), aby verifikovali, či sa všetky štúdie vykonávajú v súlade so zásadami SLP.

5.8.2 Prístup do počítačových systémov a roly

Užívateľský prístup

Kontrola prístupu sa musí plne využívať, aby sa zabezpečilo, že zamestnanci majú prístup len k funkciám, ktoré sú vhodné pre ich prácu a úlohu v štúdii, a že akcie možno pripísať konkrétnemu jednotlivcovi. Vedenie testovacieho pracoviska musí byť schopné preukázať úrovne prístupu udelené jednotlivým zamestnancom a zabezpečiť, aby boli k dispozícii historické informácie týkajúce sa úrovne prístupu používateľov. Ak systém tieto údaje neuchováva, musí byť k dispozícii papierový záznam. Kontroly prístupu majú byť na úrovni operačného systému aj aplikácií. Individuálne heslo na úrovni operačného systému sa nemusí vyžadovať, ak sú zavedené vhodné kontroly na zabezpečenie integrity údajov (napr. individuálne heslo na úrovni aplikácie postačuje, ak úprava údajov mimo aplikácie nie je možná).

Pri systémoch, ktoré generujú, upravujú alebo uchovávajú údaje SLP, sa nesmú používať zdieľané prihlasovacie údaje ani všeobecný používateľský prístup. Ak návrh počítačového systému podporuje individuálny prístup používateľa, musí sa použiť táto funkcia. To si môže vyžadovať zakúpenie ďalších licencií.

Systémy, ktoré sa nepoužívajú len na účely SLP, ale majú v sebe aj iné prvky, ako sú schválení dodávatelia, stav zásob, umiestnenie a história transakcií, ktoré sú použiteľné aj v SLP, vyžadujú primerané posúdenie.

Vie sa, že niektoré počítačové systémy podporujú iba prihlásenie jedného používateľa alebo obmedzený počet používateľských prihlásení. Ak nie je k dispozícii vhodný alternatívny počítačový systém, ekvivalentnú kontrolu možno zabezpečiť softvérom tretej strany alebo

metódou zabezpečenia vysledovateľnosti na papieri (s kontrolou verzií). Vhodnosť alternatívnych systémov musí byť odôvodnená a zdokumentovaná.

Prístup správcu systému

Prístup pre správcu systému musí byť obmedzený na minimálny možný počet ľudí, berúc do úvahy veľkosť a charakter testovacieho pracovisko. Účet správcu systému nesmie byť dostupný na bežné použitie. Personál s prístupom správcu systému sa musí prihlásiť pomocou jedinečných prihlasovacích údajov, ktoré umožňujú priradiť akcie v záznamoch audit trail konkrétnej osobe. Zámerom je zabrániť poskytnutiu prístupu používateľom s potenciálnym konfliktom záujmov, aby sa predišlo neoprávneným zmenám, ktoré by nebolo možné vysledovať k danej osobe.

Práva správcu systému - administrátora (povoľujúce činnosti, ako je vymazanie údajov, zmena databázy alebo zmeny konfigurácie systému) sa nesmú prideľovať jednotlivcom s priamym záujmom o údaje (generovanie údajov, zmena, vymazanie, kontrola alebo schválenie). Akékoľvek zmeny údajov štúdie vykonané správcom systému sa musia vykonať len po predchádzajúcom súhlase vedúceho štúdie.

Ak nie je možné prideliť nezávislého správcu systému (napríklad v malých testovacích pracoviskách), podobnú úroveň kontroly možno dosiahnuť pomocou duálnych používateľských účtov s rôznymi privilégiami, kde všetky zmeny vykonané v rámci prístupu ako správcu systému, podliehajú náležitej kontrole a schváleniu.

Jednotlivec sa musí prihlásiť pomocou účtu s príslušnými prístupovými právami pre danú úlohu, napr. laboratórny technik vykonávajúci kontrolu údajov sa nemôže prihlásiť ako správca systému, kde je iná úroveň prístupových práv. Vhodnosť takéhoto usporiadania musí byť pravidelne prehodnocovaná.

(Pozri tiež časť 1.3.1 a 3.7 dokumentu *OECD Document No 17 (OECD, 2016[4]).*)

***