POČÍTAČOVÉ SYSTÉMY

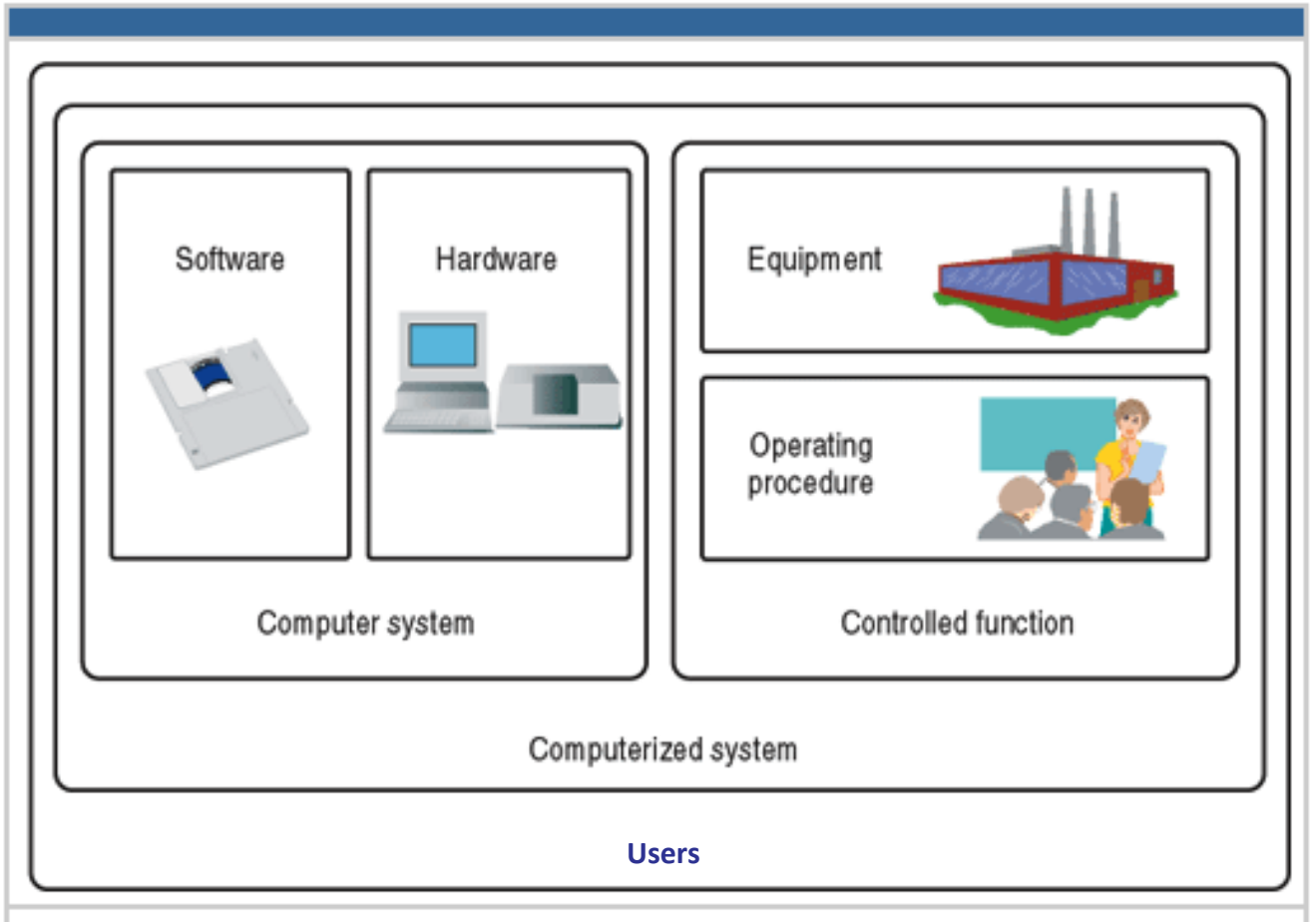
Dana Machutková

Praha 12.11.2022

Osnova

- Definice PS
- Proč ověřovat funkčnost PS
- Mýty o validaci
- Životní cyklus PS – řízení rizik
- Životní cyklus PS – role a odpovědnosti
- Životní cyklus PS – projektová fáze
- Životní cyklus PS – operační fáze
- Životní cyklus PS – ukončení používání
- PS – Průběh kontroly
- PS – Časté a kritické nedostatky
- Co nás čeká

Definice PS



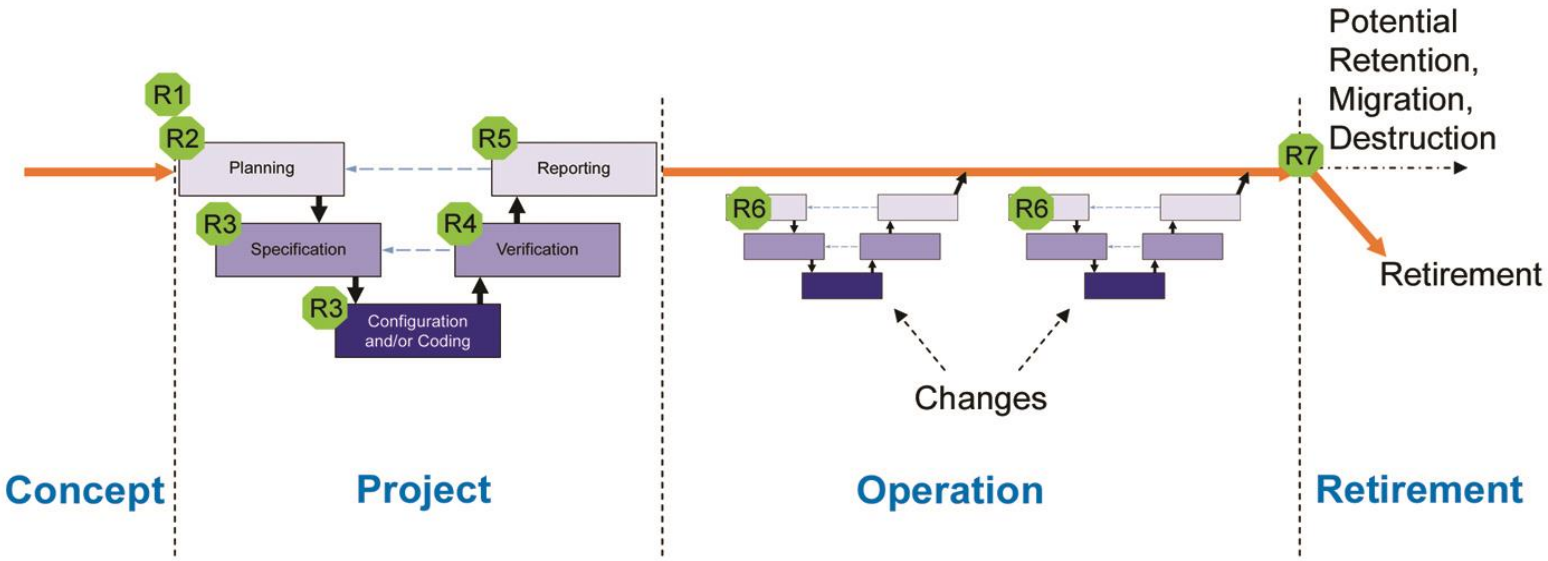
Proč validovat PS?

- Ochrana zdraví pacientů
  - Kvalita, bezpečnost a účinnost léčivého přípravku
- Ochrana investičních i provozních finančních prostředků
  - Včasná detekce defektu (relativní náklady na opravu defektu ve fázi požadavků 2X po fázi implementace 200X)
- Ochrana duševního zdraví zaměstnanců
  - Opakovatelnost transakce, dohledatelnost a spolehlivost dat, jednoznačné a přehledné manuály
- Legislativní požadavky
  - VYR-32, Doplněk 11, verze 1 (The Rules Governing Medicinal Products in European Union, EU Guidelines to GMP, Annex 11: Computerized Systems)

Mylné představy o validaci:

- Koupili jsme „validovaný“ systém
- Postačuje částečná validace systému
- Dlouhodobé používání se rovná validaci
- Validace nevyžaduje dokumentaci
- GMP (Giant Mass of Paper = Obrovské množství papíru)
- Validace se rovná testování softwaru
- Validace je úkolem IT nebo QA
- Validace je jednorázová činnost

Životní cyklus PS



- Ověřování funkčnosti / validace PS není jednorázová činnost. Mělo by začínat fází uživatelských požadavků a mělo by skončit, jakmile bude vyřazen poslední záznam vygenerovaný z tohoto systému.
- V celém životním cyklu je nutné používat hodnocení a řízení rizik.

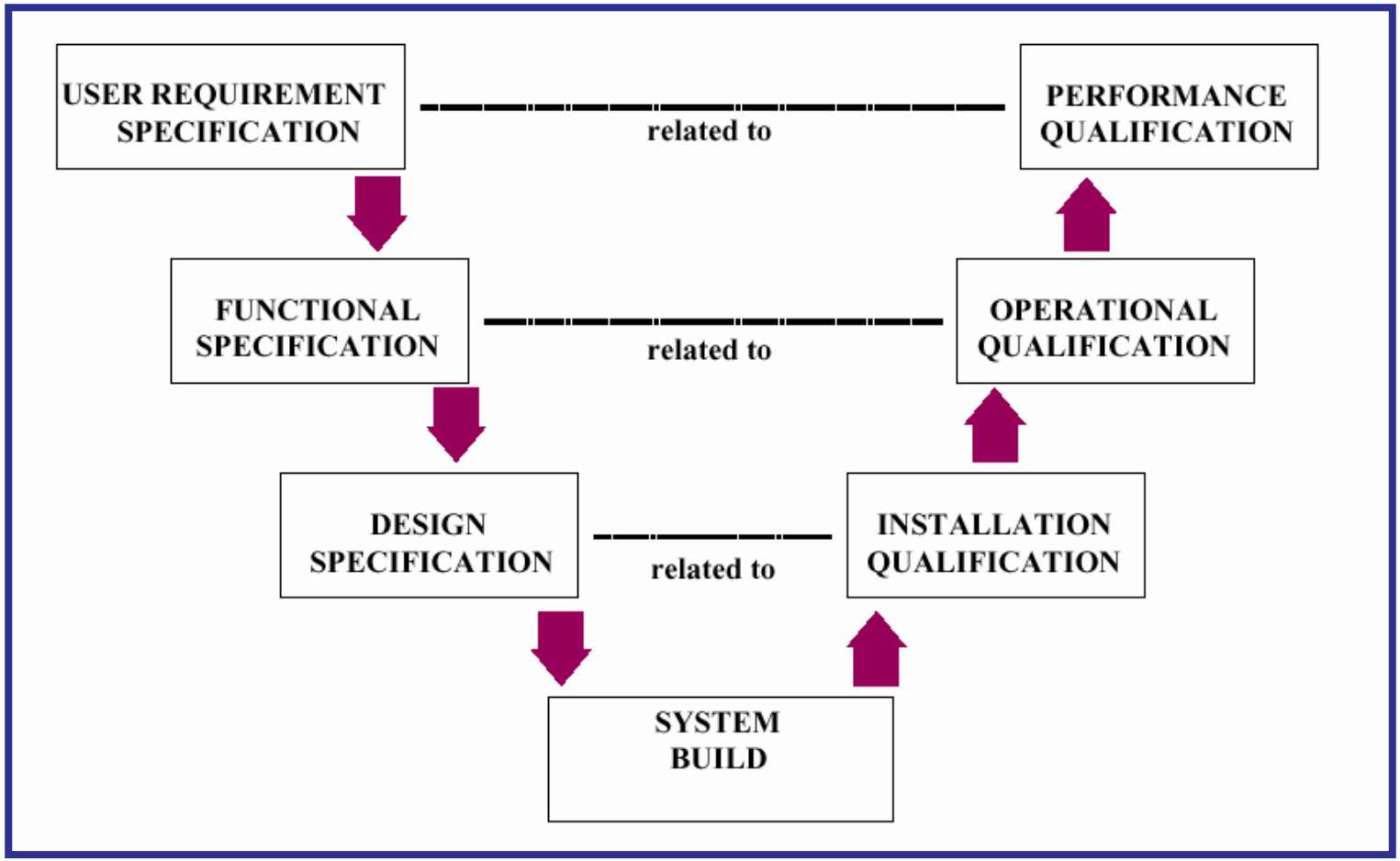
Životní cyklus PS – role a odpovědnosti

- Nutná spolupráce mezi všemi pracovníky zapojenými do systému, včetně IT a externích dodavatelů:
  - Vlastník procesu: osoba odpovědná za proces (obvykle vedoucí pracovník).
  - Vlastník systému: osoba odpovědná za dostupnost a údržbu PS a bezpečnost dat uložených v daném systému (obvykle odborný garant zařízení).
  - Formální dohody mezi výrobcem a jakoukoliv třetí stranou; tyto dohody mají obsahovat jasné prohlášení o odpovědnosti třetích stran. Analogicky se mají brát v úvahu IT oddělení (vymezení odpovědnosti ve vnitropodnikovém dokumentu, příp. smlouva, audity).
  - Výběr dodavatele - kompetence a spolehlivost.
  - Audity na základě hodnocení rizik.
  - Přezkoumání dodané dokumentace uživatelem.
  - Informace o systému jakosti a auditech vztahující se k dodavatelům systémů – k dispozici inspektorům na vyžádání.

Životní cyklus PS – fáze projektu

- Uživatelské specifikace by měly popsat požadované funkce počítačového systému a být založeny na zdokumentovaném posouzení rizik a vlivu na SVP. Požadavky uživatele mají být sledovatelné po celou dobu životního cyklu.
- Pro kritické systémy má být k dispozici aktuální popis systému podrobně popisující fyzické a logické uspořádání, toky dat a rozhraní s jinými systémy nebo procesy, veškeré základní požadavky na hardware a software a bezpečnostní opatření.
- Doplněk 11 nestanovuje validační přístup, ale pokud je vybrán, musí obstát před regulační autoritou. Výrobci mají být schopni odůvodnit své standardy, protokoly, akceptační kritéria, postupy a záznamy na základě jejich hodnocení rizik.

Životní cyklus PS – fáze projektu



Životní cyklus PS – operační fáze

- **Integrita a správnost dat** - při výměně dat s jinými systémy nutné vestavěné kontroly pro správné a bezpečné zadávání a zpracování dat, při ručním zadávání kritických dat je zapotřebí další kontrola správnosti dat.
- **Uchovávání dat** - zajištění jak fyzickými, tak elektronickými prostředky před poškozením. Uložená data mají být kontrolována na přístupnost, srozumitelnost a správnost. Přístup k datům má být zajištěn po celou dobu uchovávání.
- **Pravidelné zálohování** - integrita a správnost zálohování dat a schopnost obnovit data mají být kontrolovány během validace a pravidelně monitorovány.
- **Tiskové výstupy** - má být možné získat zřetelné tištěné kopie elektronicky uložených dat, pro záznamy, které jsou podporou pro propuštění šarže, má být možné vytvořit tiskové výstupy udávající, zda některý z údajů byl změněn oproti původnímu záznamu.

Životní cyklus PS – operační fáze

- **Dohledatelnost** – je nutné zvážit, na základě posouzení rizik, zda do systému zabudovat vytváření záznamů o všech významných změnách a odstranění údajů týkajících se SVP. Má být zdokumentován důvod pro změnu nebo odstranění významných údajů SVP. Revizní stopa musí být dostupná, převeditelná do obecně srozumitelné formy a pravidelně přezkoumávána.
- **Řízení změn a konfigurací** – jakékoli změny počítačového systému včetně jeho konfigurace mají být provedeny pouze kontrolovaným způsobem v souladu s definovaným postupem.
- **Správa incidentů** – všechny incidenty (selhání systému, chyby v datech, neoprávnění přístupy) mají být hlášeny a vyhodnoceny. Příčiny kritické události mají být objasněny a mají tvořit základ nápravných a preventivních opatření

Životní cyklus PS – operační fáze

- **Zabezpečení** - mají být zajištěny kontroly omezující přístup k počítačovému systému na oprávněné osoby (použití klíče, přístupových karet, osobních kódů s hesly, biometrie, omezený přístup k výpočetní technice a oblasti ukládání dat), rozsah bezpečnostních kontrol závisí na kritičnosti počítačového systému.
- Vytvoření, změna a zrušení povolení přístupu mají být zaznamenány.
- Systémy řízení dat a dokumentů mají být navrženy tak, aby zaznamenávaly totožnost operátorů, kteří vkládají data, provádějí jejich změny, potvrzení nebo odstranění, včetně zaznamenávání data a času.
- Elektronický podpis (stejný dopad jako rukou psané podpisy v rámci společnosti, trvalé propojení s jejich příslušným záznamem, zahrnují i čas a datum jejich použití) – nutné minimálně při certifikaci LP.

Životní cyklus PS – operační fáze

- **Pravidelné hodnocení** - počítačové systémy mají být pravidelně vyhodnocovány, aby se potvrdilo, že zůstávají ve validním stavu a jsou v souladu s SVP. Hodnocení zahrnovat současný rozsah funkčnosti, záznamy o odchylkách, události, problémy, historii aktualizací, fungování, spolehlivost, bezpečnost a zprávy o stavu jejich validací.

Ukončení používání PS

- **Kontinuita činnosti** - pro dostupnost PS podporujících kritické procesy mají být zavedena taková opatření, která zajistí nepřetržitou podporu těchto procesů v případě poruchy systému (např. manuální nebo alternativní systém). Doba potřebná k zavedení alternativních uspořádání do provozu má být založena na riziku a vhodná pro daný systém a podnikový proces, který podporuje. Tato opatření mají být dostatečně zdokumentována a otestována.
- **Archivace** - archivovaná data mají být kontrolována z hlediska přístupnosti, srozumitelnosti a integrity. Pokud mají být provedeny příslušné změny v systému (např. počítačové vybavení nebo programy), pak má být zajištěna schopnost získání a testování dat.
- **Ověřování a hodnocení PS může skončit, jakmile bude vyřazen poslední záznam vygenerovaný z tohoto systému.**

Počítačové systémy – průběh kontroly

- Seznam počítačových a počítačově řízených systémů a jejich rozdělení z hlediska SVP relevance a kritičnosti
- Kontrola předpisové dokumentace (popisy systému/návody k použití, rozdělení zodpovědností, způsoby zálohování, kontroly audit trailů, řízení přístupů a změn, řešení incidentů)
- Kontrola záznamů
- Kontrola školení interních pracovníků a ověření vhodnosti a kompetentnosti externích dodavatelů, interní audity
- Kontrola smluv spojených s vývojem, implementací, případně správou automatizovaných systémů
- Kontrola periodického hodnocení systémů
- Kontrola vybraných validací/kvalifikací automatizovaných systémů

Počítačové systémy – časté nedostatky

- Seznam SVP relevantních systémů chybí nebo není kompletní.
- V seznamu (nebo v jiném dokumentu) chybí jasně definovaná odpovědnost za systém, kritičnost systému, stav kvalifikace, případně další informace (datum rekvalifikace apod.) vztahující se k automatizovanému systému.
- Nedostatečně nebo nejasně definované kompetence v rámci implementace a správy SW a automatizovaných systémů.
- Pro SW není vytvořen předpis na jeho ovládání.
- Není prováděna interní kontrola (audit) oddělení IT.
- Pracovníci, odpovědní za IT (včetně pracovníků externích společností), nejsou školení ze zásad SVP, nebo je jejich školení nedostatečné.
- Ve smlouvě s externí společností není uvedena oblast SVP.
- Pracovníci nejsou proškoleni z ovládání SW.

Počítačové systémy – časté nedostatky

- Systém nebyl validován/kvalifikován vůbec. (SW pro ovládání VZT, stanice pro ovládání přístroje, např. ve formě tabletu na mineralizační peci).
- Rozsah validace není dostatečný (nejsou kvalifikovány kritické funkce SW, jako např. pro propouštění léčiv na trh, audit trail, integrita dat).
- Není provedena validace při update nebo rozšíření systému (pozor na migraci Win 7 na Win 10).
- Rozsah provedených zkoušek v rámci validace/kvalifikace neodpovídá požadavkům v URS nebo ve validačních/kvalifikačních protokolech.
- Validace/kvalifikace nebyla provedena na základě hodnocení rizik.
- Validační/kvalifikační dokumentace nebyla kontrolována pracovníky kontrolované osoby.
- Chybějící dokumentace (protokoly, záznamy o provedení testů)

Počítačové systémy – časté nedostatky

- Systém neumožňuje uzamčení.
- Není popsán postup pro změnu hesla a jeho síly (heslo 1234).
- Systém umožňuje připojení neschváleného HW (hot-spot!)
- Sdílení stejného hesla, práce pod jiným přihlášeným uživatelem (přihlášení čipem jiného zaměstnance).
- Heslo je napsáno na místě v okolí PC stanice.
- Pracovník po odchodu od stanice nechá systém zapnutý.
- O změnách v SW systémech nejsou vedeny záznamy
- Upgrade SW není řešen v rámci změnového řízení.
- Upgrade SW se neřídí systémem pro kontrolu rizik.
- Není žádný záznam o kontrole audit trailů

Počítačové systémy – časté nedostatky

- Není vytvořen předpis pro hodnocení automatizovaných systémů.
- Periodické hodnocení SW systémů není prováděno vůbec nebo pouze pro část používaných systémů.
- Hodnocení je provedeno formálně, neobsahuje relevantní informace o změnách, incidentech a dalších činnostech, provedených na systémech a nehodnotí tudíž jejich aktuální stav.

PS – kritické nedostatky

- SW systém umožní propuštění šarže léčivého přípravku do distribuce před jeho certifikací kvalifikovanou osobou a k tomuto propuštění dojde.

- SW systém umožňuje falšování dat nebo záznamové dokumentace a tato možnost je využívána.

- Kontrolovaná osoba neřeší dříve nalezené nedostatky, týkající se nálezů z kontrol státních autorit, zvláště pak ty, které se týkají integrity dat.

Co nás čeká? Doplněk 11 – upřesnění a nové definice

- U kritických systémů ověřených a/nebo provozovaných poskytovateli služeb (např. „cloudové“ služby) by očekávání měla jít nad rámec toho, že „musí existovat formální dohody“. Regulovaní uživatelé by měli mít přístup k úplné dokumentaci pro validaci a bezpečný provoz systému a měli by být schopni tuto dokumentaci předložit během regulačních inspekcí, např. s pomocí poskytovatele služeb.
- Upřesnění termínu „komerční běžně dostupné produkty“ (COTS), který zatím není dostatečně definován a může být snadno chápán příliš široce.
- Stanovení pokynů pro klasifikaci kritických údajů a kritických systémů.
- Zavedení povinnosti sledovatelnosti specifikace uživatelských požadavků.

Co nás čeká? Doplněk 11 – Zálohování

- Stanovení povinností k procesům zálohování, např. na to, co je pokryto zálohou (např. pouze data nebo data a aplikace), jaké typy záloh se provádějí (např. přírůstkové nebo úplné), jak často se zálohují (všechny typy), jak dlouho jsou zálohy uchovávány, jaké médium se používá pro zálohy a kde jsou zálohy uchovávány (např. fyzické oddělení).
- Stanovení povinnosti na možnost získat údaje v elektronické podobě včetně úplného audit trailu.

Co nás čeká? Doplněk 11 – Audit trail

- Zavedení povinné funkce auditní stopy, která automaticky zaznamenává všechny manuální interakce na kritických systémech GMP, kde lze uživatele, data nebo nastavení ručně měnit.
- Audit trail musí pozitivně identifikovat uživatele, který provedl změnu, a poskytovat úplný popis toho, co bylo změněno, tj. měly by být jasně viditelné jak nové, tak všechny staré hodnoty, měl by obsahovat plný čas a datum při provedení změny a u všech ostatních změn, kromě případů, kdy je hodnota zadána do prázdného pole nebo kde je to zcela zřejmé, by měl být uživatel vyzván k uvedení důvodu nebo zdůvodnění, proč byla změna provedena.
- Nesmí být možné upravovat data auditního záznamu nebo deaktivovat funkci auditního záznamu pro běžné nebo privilegované uživatele pracující na systému.

Co nás čeká? Doplněk 11 – Audit trail – přezkum

- Přezkum auditní stopy by se měl zaměřit na kontrolu integrity manuálních změn provedených v systému, např. ověření důvodu změn a zda byly změny provedeny v neobvyklých datech, hodinách a neobvyklými uživateli.
- Stanovení pokynů pro přijatelnou frekvenci přezkumu auditní stopy. Pro auditní záznamy kritických parametrů, např. nastavení alarmů v systémech, které upozorňují na diferenční tlak ve spojení s aseptickým plněním, by revize kontrolních záznamů měly být součástí uvolnění šarže.
- Funkce audit trail musí zachycovat údaje dostatečně podrobně a ve skutečném čase, aby poskytly úplný a přesný obraz událostí. Pokud např. systém upozorní uživatele na nesrovnalosti ve vstupu dat napsáním chybové zprávy a uživatel následně změní vstup, čímž oznámení zmizí, měl by být zachycen celý soubor událostí.
- Požadavek na možnost třídění a zpracovávání alarmů a dat o událostech a záznamů auditní stopy.

Co nás čeká? Doplněk 11 – Přezkoumání změn

- Měl by být doplněn koncept přezkoumání konfigurace. Nebude tedy stačit výčet známých změn v systému (historie upgradů), ale mělo by být v průběhu času prováděno porovnání původního a nového hardwaru a softwaru.
- Porovnání by mělo zahrnovat vysvětlení všech rozdílů a vyhodnocení potřeby rekvalifikace/validace.

Co nás čeká? Doplněk 11 – Zabezpečení

- Zaměření na důvěrnost systému a dat, integritu a dostupnost (dle ISO 27001).
- Konkrétní požadavky na očekávané ovládací prvky (vícefaktorová autentizace, firewally, správa platforem, záplatování zabezpečení, skenování virů a detekce/prevence narušení).
- Pro autentizaci na kritických systémech nebude dostačující pro identifikaci regulovaného uživatele pouze ověření pouze pomocí „karty“ (vysoké riziko při ztrátě nebo odcizení).
- Přidání dvou důležitá očekávání pro přidělování systémových přístupů; tj. „oddělení povinností“ (každodenní uživatelé systému nemají práva správce) a „princip nejmenšího privilegia“ (že uživatelé systému nemají vyšší přístupová práva, než jaká je nezbytná pro jejich pracovní funkci).

Co nás čeká? Doplněk 11 – AI & ML

- Existuje naléhavá potřeba regulačních pokynů a očekávání ohledně používání modelů umělé inteligence (AI) a strojového učení (ML) v kritických aplikacích GMP, protože průmysl již tuto technologii zavádí. Primární důraz by měl být kladen na relevanci, přiměřenost a integritu dat použitých k testování těchto modelů a na výsledky (metriky) z takového testování, spíše než na proces výběru, školení a optimalizace modelů.

MÁTE ZKUŠENOSTI SE SÚKL?

Podělte se o ně s námi!

SÚKL se jako každá organizace snaží zlepšovat a rozvíjet poskytované služby.

Budeme proto rádi, když nám dáte zpětnou vazbu vyplněním následujícího dotazníku.

DOTAZNÍK SPOKOJENOSTI

Předem děkujeme za spolupráci a za čas věnovaný odpovědím.

Děkujeme za pozornost.

STÁTNÍ ÚSTAV PRO KONTROLU LÉČIV
Šrobárova 48, 100 41 Praha 10
tel.: +420 272 185 111
fax: +420 271 732 377
e-mail: posta@sukl.cz