VYR-32 DOPLNĚK 11 verze 1 POKYNY PRO SPRÁVNOU VÝROBNÍ PRAXI - POČÍTAČOVÉ SYSTÉMY

Tento pokyn je překladem The Rules Governing Medicinal Products in the European Union, Volume 4, EU Guidelines to Good Manufacturing Practice, Annex 11, Computerised Systems, ve znění platném k **30.6.2011**.
Tento pokyn nahrazuje pokyn VYR-32 Doplněk 11.

Právní základ pro vydávání podrobných pokynů: Článek 47 směrnice 2001/83/ES o kodexu společenství týkajícím se humánních léčivých přípravků pro humánní použití a článek 51 směrnice 2001/82/ES o kodexu Společenství týkajícím se veterinárních léčivých přípravků. Tento dokument poskytuje návod pro výklad zásad a pokynů pro správnou výrobní praxi (SVP) pro léčivé přípravky podle směrnice 2003/94/ES pro léčivé přípravky pro humánní použití a směrnice 91/412/EHS pro veterinární použití.

Stav dokumentu: revize 1

Důvody pro změny: příloha byla revidována v reakci na zvýšené využívání počítačových systémů a větší složitost těchto systémů. Vyplývající změny jsou také navrženy pro kapitolu 4 Pokynů pro SVP.

Zásady

Tento doplněk se vztahuje na všechny formy počítačových systémů používaných v rámci aktivit regulovaných SVP. Elektronický systém je sada softwarových a hardwarových komponent, které společně plní určité funkce.

Používání má být ověřeno; IT infrastruktura má být kvalifikována.

V případě, kdy počítačový systém nahrazuje ruční ovládání, nemá dojít k následnému snížení jakosti výrobků, kontroly procesů a jištění jakosti. Nemělo by docházet k nárůstu celkového rizika v procesu.

Obecné

1. Řízení rizik

Řízení rizik má být použito v celém životním cyklu počítačového systému s ohledem na bezpečnost pacienta, integritu dat a jakost výrobků. V rámci systému řízení rizik má být rozhodnutí o rozsahu validací a kontrolách integrity dat založeno na odůvodněném a zdokumentovaném posouzení rizik počítačového systému.

2. Personál

Má existovat úzká spolupráce mezi všemi příslušnými pracovníky, jako jsou vlastník procesu, vlastník systému, kvalifikovaná osoba a IT. Všichni pracovníci mají mít odpovídající kvalifikaci, přístupová práva a definované odpovědnosti k plnění svých přidělených povinností.

3. Dodavatelé a poskytovatelé služeb

3.1 Pokud jsou využívány třetí strany (např. dodavatelé, poskytovatelé služeb), např. pro poskytování, instalaci, konfiguraci, integraci, ověřování, údržbu (např. prostřednictvím vzdáleného přístupu), změnu nebo archivaci počítačového systému nebo související služby, nebo pro zpracování dat, musí existovat formální dohody mezi výrobcem a jakoukoliv třetí osobou, a tyto dohody mají obsahovat jasné prohlášení o odpovědnosti třetích stran. Obdobně se mají brát v úvahu IT oddělení.

3.2 Kompetence a spolehlivost dodavatele jsou klíčovými faktory při výběru produktu nebo poskytovatele služeb. Potřeba auditu má být založena na posouzení rizik.

3.3 Dokumentace dodaná s běžnými komerčními produkty má být přezkoumána regulovanými uživateli za účelem ověření, že jsou splněny uživatelské požadavky.

3.4 Systém jakosti a informace z auditu týkající se dodavatele nebo projektanta softwaru a zavedených systémů mají být zpřístupněny inspektorům na vyžádání.

Fáze projektu

4. Validace

4.1 Validační dokumentace a zprávy mají zahrnovat příslušné kroky v životním cyklu počítačového systému. Výrobci mají být schopni odůvodnit své standardy, protokoly, akceptační kritéria, postupy a záznamy na základě jejich hodnocení rizik.

4.2 Validační dokumentace má obsahovat záznamy o řízení změn (pokud je aplikovatelné) a zprávy o případných odchylkách pozorovaných při validačním procesu.

4.3 Má být k dispozici aktuální seznam všech příslušných systémů a podrobný přehled (soupis) jejich funkcí v oblasti SVP.
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.

4.4 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.

4.5 Regulovaný uživatel má přijmout veškerá přiměřená opatření, aby zajistil, že systém byl vypracován v souladu s vhodným systémem řízení jakosti. Dodavatel má být přiměřeně posouzen.

4.6 Pro validaci počítačových systémů vytvořených na zakázku nebo vlastních má být zaveden na místě vhodný postup, který zajišťuje formální hodnocení a podávání zpráv o hodnocení kvality systému a jeho fungování v průběhu všech stadií životního cyklu systému.

4.7 Má být prokázána vhodnost zkušebních metod a scénářů. Zejména se mají vzít v úvahu limitní parametry systému (procesu), datové limity a řešení chybových hlášení. Automatizované zkušební přístroje a zkušební prostředí mají mít dokumentované posouzení jejich přiměřenosti (zda jsou odpovídající).

4.8 Pokud jsou data převáděna na jiný datový formát nebo systém, validace mají zahrnovat kontroly, že se nemění hodnota dat a / nebo jejich význam během tohoto procesu přenosu.

Operační fáze

5. Data

Počítačové systémy, které si vyměňují data elektronicky s jinými systémy, mají zahrnovat vhodné vestavěné kontroly pro správné a bezpečné zadávání a zpracování dat, aby se minimalizovaly rizika.

6. Kontroly správnosti

Tam, kde se kritická data zadávají ručně, je zapotřebí další kontrola správnosti dat. Tato kontrola může být provedena druhým operátorem nebo ověřenými elektronickými prostředky. Kritičnost a možné následky chybných nebo nesprávně zadaných údajů do systému mají být pokryty řízením rizik.

7. Uchovávání dat

7.1 Data mají být zajištěna 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.

7.2 Má být prováděno pravidelné zálohování všech příslušných dat. Integrita a správnost zálohování dat a schopnost obnovit data mají být kontrolovány během validace a pravidelně monitorovány.

8. Tiskové výstupy

8.1 Má být možné získat zřetelné tištěné kopie elektronicky uložených dat.

8.2 Pro záznamy, které jsou podporou pro propuštění šarže, má být možné vytvořit tiskové výstupy udávající, zda některý z údajů byl změněn oproti původnímu záznamu.

9. Dohledatelnost

Má se zvážit, na základě posouzení rizik, zda do systému zabudovat vytváření záznamů o všech významných změnách a odstranění údajů týkajících se SVP (systém dohledatelnosti / revizní stopy). Má být

zdokumentován důvod pro změnu nebo odstranění významných údajů SVP. Revizní stopa musí být dostupná, převeditelná do obecně srozumitelné formy a pravidelně přezkoumávána.

10. Řízení změn a konfigurací
Jakékoli změny počítačového systému včetně jeho konfigurace mají být provedeny pouze kontrolovaným způsobem v souladu s definovaným postupem.

11. Pravidelné hodnocení
Počítačové systémy mají být pravidelně vyhodnocovány, aby se potvrdilo, že zůstávají ve validním stavu a jsou v souladu s SVP. Kde je to vhodné, má takové hodnocení zahrnovat současný rozsah funkčnosti, záznamy o odchylkách, události, problémy, historii aktualizací, fungování, spolehlivost, bezpečnost a zprávy o stavu jejich validací.

12. Zabezpečení
12.1 V místě mají být zajištěny fyzické a/nebo logické kontroly omezující přístup k počítačovému systému na oprávněné osoby. Vhodné metody zabraňující neoprávněnému vstupu do systému mohou zahrnovat použití klíče, přístupových karet, osobních kódů s hesly, biometrie, omezený přístup k výpočetní technice a oblasti ukládání dat.

12.2 Rozsah bezpečnostních kontrol závisí na kritičnosti počítačového systému.

12.3 Vytvoření, změna a zrušení povolení přístupu mají být zaznamenány.

12.4 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.

13. Správa incidentů
Všechny incidenty, a to nejen selhání systému a chyby v datech, mají být hlášeny a vyhodnoceny. Příčiny kritické události mají být objasněny a mají tvořit základ nápravných a preventivních opatření.

14. Elektronický podpis
Elektronické záznamy mohou být podepsány elektronicky. Od elektronických podpisů se očekává, že:
a. mají stejný dopad jako rukou psané podpisy v rámci společnosti,
b. jsou trvale propojeny s jejich příslušným záznamem,
c. zahrnují i čas a datum jejich použití.

15. Propouštění šarží
Pokud je počítačový systém používán pro certifikaci a propouštění šarží, má umožnit pouze kvalifikovaným osobám, aby potvrdily propuštění šarží, a má jasně identifikovat a zaznamenat osobu, která propouští nebo certifikuje šarží. Má to být provedeno s použitím elektronického podpisu.

16. Kontinuita činnosti
Pro dostupnost počítačových systémů 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.

17. Archivace
Data mohou být archivována. Tato 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.

Definice pojmů:
Aplikace: Software nainstalovaný na definovanou platformu / hardware poskytující konkrétní funkčnost

Počítačový systém na zakázku nebo vlastní: elektronický systém individuálně navržený tak, aby vyhovoval konkrétnímu podnikovému procesu

Komerční software: Software komerčně dostupný, jehož vhodnost pro použití je prokázána širokým spektrem uživatelů.

IT infrastruktura: hardware a software ve formě softwarových sítí a operačních systémů, které umožňují fungování aplikací.

Životní cyklus: všechny fáze životnosti systému od počátečních požadavků do ukončení používání, zahrnující návrh, specifikaci, programování, testování, instalaci, provoz a údržbu.

Vlastník procesu: osoba odpovědná za podnikový proces.

Vlastník systému: osoba odpovědná za dostupnost a údržbu počítačového systému a za bezpečnost dat uložených na tomto systému.

Třetí strana: Strany, které nejsou přímo řízeny držitelem povolení k výrobě a/nebo dovozu.