EudraLex
Zasady dotyczące produktów leczniczych w Unii Europejskiej
Tom 4
Dobrej Praktyki Wytwarzania
Produktów Leczniczych Stosowanych u Ludzi i w Weterynarii
Załącznik 11: Systemy komputerowe

Źródło: SANCO/C8/AM/sl/ares(2010)1064599, z 27 stycznia 2011, o ile w tekście nie podano inaczej.

Podstawa prawna publikacji szczegółowe wytyczne: Artykuł 47 dyrektywy 2001/83/WE w sprawie wspólnotowych przepisów odnoszących się do produktów leczniczych stosowanych u ludzi oraz art 51 dyrektywy 2001/82/WE w sprawie wspólnotowych przepisów odnoszących się do weterynaryjnych produktów leczniczych. Dokument ten zawiera wytyczne do interpretacji zasad i wytycznych dobrej praktyki wytwarzania (GMP) dla produktów leczniczych określonych w dyrektywie 2003/94/WE dla produktów leczniczych stosowanych u ludzi oraz dyrektywy 91/412/EWG stosowanej w weterynarii.

Status dokumentu: wersja 1

Przyczyna zmiany: załącznik został zmieniony w odpowiedzi na zwiększone wykorzystanie systemów komputerowych i wzrost złożoności tych systemów. Wynikające stąd zmiany są również zaproponowane w rozdziale 4 GMP Guide.

Reguła
Niniejszy załącznik ma zastosowanie do wszystkich typów systemów komputerowych używanych w ramach działalności regulowanej przez GMP. System komputerowy jest zestawem oprogramowania i elementów sprzętu, które razem spełniają określone funkcje.

Aplikacja powinna zostać zwalidowana; Infrastrukturę IT należy skwalifikować.

Zastąpienie wszelkich operacji ręcznych systemem komputerowym nie może prowadzić do obniżenia jakości produktu oraz kontroli procesów i poziomu zapewnienia jakości. Nie powinno nastąpić zwiększenie ogólnego ryzyka procesu.

Ogólne
1. Zarządzanie ryzykiem
Należy stosować zarządzanie ryzykiem w całym cyklu życia systemu komputerowego, biorąc pod uwagę bezpieczeństwo pacjenta, integralność danych i jakość produktu. W ramach zarządzania ryzykiem, decyzje o zakresie walidacji i kontroli integralności danych powinny opierać się na uzasadnionej i udokumentowanej ocenie ryzyka systemu komputerowego.
2. Personel
Należy zapewnić ścisłą współpracę pomiędzy personelem kluczowym jak Właściciel Procesu, Właściciel Systemu, Osoby Wykwalifikowane oraz pracownikami obsługującymi systemy komputerowe. Każdy pracownik powinien mieć odpowiednie kwalifikacje, poziom dostępu i obowiązki określone w celu realizacji swoich zadań.
3. Dostawcy i usługodawcy
3.1 Jeżeli usługi instalacji, konfiguracji, integracji, walidacji, serwisu (np. poprzez zdalny dostęp), zmiany, utrzymanie systemu komputerowego; przetwarzanie danych lub podobne prace są realizowane przez stronę trzecią (np. dostawcy, usługodawcy), to powinna być zawarta umowa w formie pisemnej pomiędzy wytwórcą a stroną trzecią, precyzująca odpowiedzialność strony trzeciej. Działy IT powinny być traktowane analogicznie.

3.2 Kompetencje i wiarygodności dostawcy są kluczowymi czynnikami przy wyborze dostawcy produktów lub usług. Należy wykonać audyt oparty na ocenie ryzyka.

3.3 Dostarczona dokumentacja wraz informacjami handlowymi produktu powinna zostać poddana przeglądowi przez kompetentnych użytkowników, w celu sprawdzenia czy są spełnione wymagania użytkownika.

3.4 System jakości oraz informacje z audytu dostawców wdrażających system lub producentów oprogramowania powinny być dostępne dla inspektorów na życzenie.

Fazy projektu

4. Walidacja

4.1 Dokumentacja walidacyjna i raporty powinny obejmować istotne etapy cyklu życia systemu. Wytwórcy powinni być w stanie uzasadnić swoje standardy, protokoły, kryteria akceptacji, procedury i zapisy w odniesieniu do wyników oceny ryzyka.

4.2 Dokumentacja walidacyjna powinna zawierać zapisy zmian oraz raporty z wszelkich odchyleń zaobserwowane w procesie walidacji.

4.3 Powinien być dostępny aktualny wykaz wszystkich istotnych systemów i ich funkcjonalność w odniesieniu do GMP.

Dla systemów o znaczeniu krytycznym powinny być dostępne szczegółowe opisy rozwiązania w zakresie fizycznym (np. rozmieszczenia sprzętu) i logicznym, przepływ danych, interfejsy z innymi systemami lub procesami, zastosowany sprzęt i oprogramowanie oraz środki bezpieczeństwa.

4.4 Specyfikacja Wymagań Użytkownika powinna zawierać niezbędne funkcje systemu komputerowego w oparciu o udokumentowaną ocenę ryzyka i wpływ GMP. Wymagania użytkowników, powinny być identyfikowalne w całym cyklu życia systemu.

4.5 Użytkownik powinien podjąć wszelkie kroki, aby zapewnić, że system komputerowy został utworzony zgodnie z odpowiednim systemem zarządzania jakością. Dostawca powinien być oceniany w odpowiedni sposób.

4.6 Walidacja systemu „szytego na miarę" lub modyfikowanego powinna być realizowana w miejscu/środowisku, które zapewnia możliwość formalnej oceny, raportowanie jakości oraz wydajności na wszystkich etapach cyklu życia systemu.

4.7 Dowody odpowiednich metod badań i scenariuszy testowych powinny być udokumentowane. Szczególnie dotyczy to systemu (procesu) wartości parametrów granicznych, limitu danych oraz obsługi błędów. Należy ocenić przydatność zautomatyzowanych narzędzi do testów oraz środowisk testowych.

4.8 Jeżeli dane są transferowane do innego formatu danych lub systemu, walidacja powinna obejmować sprawdzenie, że dane nie zmieniają wartości i / lub znaczenia w procesie migracji.

Faza operacyjna

5. Dane

Komputerowe systemy elektronicznej wymiany danych z innymi systemami powinny zawierać wbudowany własny mechanizm kontroli poprawnego i bezpiecznego wprowadzania oraz przetwarzania danych, w celu zminimalizowania ryzyka.

6. „Dokładność" kontroli

Dla danych krytycznych wprowadzanych ręcznie, należy dodatkowo sprawdzać poprawność danych. Sprawdzenie danych może być wykonywane przez drugiego operatora lub przez zwalidowany mechanizm/środek elektroniczny. Krytyczne informacje, potencjalne błędy lub nieprawidłowo wprowadzone dane do systemu należy objąć zarządzaniem ryzyka.

7. Przechowywanie danych

7.1 Dane powinny być zabezpieczone za pomocą środków fizycznych lub elektronicznych przed uszkodzeniem. Przechowywane dane powinny być sprawdzane pod kątem ich dostępności, trwałości i dokładności. Powinien być zapewniony dostęp do danych przez cały okres ich przechowywania.

7.2 Należy wykonywać regularne kopie zapasowe wszelkich istotnych danych. Podczas walidacji oraz okresowych przeglądów należy weryfikować integralność i dokładność kopii danych oraz możliwość ich przywrócenia.

8. Wydruki

8.1 Powinna istnieć możliwość drukowania danych przechowywanych elektronicznie.

8.2 Dla zapisów elektronicznych wykorzystywanych do zwolnienia serii powinna istnieć możliwość wygenerowania wydruków ze wskazaniem, czy jakiekolwiek dane zostały zmienione od czasu ich wprowadzenia.

9. Ścieżki audytu Audit Trails

Należy wziąć pod uwagę ocenę ryzyka, do implementacji w systemie mechanizmu rejestracji wszystkich istotnych wg GMP zmian oraz usunięć danych (generowany przez system "audit trail"). Powinno dokumentować się zmiany lub usunięcia danych istotnych wg GMP. Audit trails powinien być dostępny i przekształcalny do ogólnie zrozumiałej formy oraz powinien podlegać regularnym przeglądom.

10. Zarządzania konfiguracją i zmianami

Wszelkie zmiany w systemie komputerowym, w tym konfiguracji systemu powinny być dokonywane jedynie w sposób kontrolowany, zgodnie z określoną procedurą.

11. Oceny okresowe

Systemy komputerowe powinny być okresowo oceniane w celu potwierdzenia, że pozostają one w prawidłowym stanie i są zgodne z GMP. Oceny okresowe powinny obejmowa

, aktualny zakres funkcjonalności, odchylenia, zdarzenia, problemy, aktualizację historii, wydajność, niezawodność, bezpieczeństwo oraz status raportów walidacji.

12. Bezpieczeństwo

12.1 Powinny być przeprowadzane fizyczne i / lub logiczne kontrole dostępu do systemu komputerowego dla osób upoważnionych. Odpowiednie metody zabezpieczające przed dostępem osób nieupoważnionych do danych obejmują: użycie kluczy, kart kodowych, kodów osobistych z hasłem, danych biometrycznych oraz ograniczenie dostępu do sprzętu komputerowego i miejsc przechowywania danych.

12.2 Zakres kontroli bezpieczeństwa zależy od krytyczności systemu komputerowego.

12.3 Utworzenie, zmiana oraz cofnięcie uprawnień na dostęp powinny być zarejestrowane.

12.4 Systemy zarządzające danymi oraz dokumentami powinny rejestrować tożsamość operatorów wprowadzających, zmieniających, potwierdzających lub usuwających dane, w tym datę i godzinę operacji w systemie.

13. Zarządzanie odchyleniami

Wszystkie odchylenia, nie tylko błędy systemu czy błędne dane, powinny być zgłaszane/rejestrowane i oceniane. Główne przyczyny krytycznych odchyleń powinny być zidentyfikowane oraz powinny stanowić podstawę działań korygujących i zapobiegawczych.

14. Podpis elektroniczny

Elektroniczne zapisy można podpisywać elektronicznie. Założenia dla podpisów elektronicznych:

a. mają takie same znaczenie jak podpis odręczny w granicach firmy
b. powinny być trwale związane z poszczególnymi danymi,
c. powinny zawierać datę i godzinę.

15. Zwolnienie serii

Jeżeli rejestrowanie certyfikatu i/lub zwalnianie serii jest przeprowadzane z użyciem systemu komputerowego, system powinien zezwalać wyłącznie Osobie Wykwalifikowanej na wykonanie tej operacji, tzn. poświadczenie lub zwolnienie partii. Powinien również identyfikować i zapisywać dane osoby dokonującej zwolnienia lub poświadczenie serii. Operacja/czynność ta powinno być przeprowadzona przy użyciu podpisu elektronicznego.

16. Ciągłość / dostępność

W sprawie dostępności systemów komputerowych wspierających krytyczne procesy, należy wprowadzić rozwiązania zapewniające ciągłość oraz wsparcie dla tych procesów w przypadku awarii systemu (np. procedury lub alternatywny system). Czas potrzebny na zastosowanie rozwiązań alternatywnych powinien być oparty na ocenie ryzyka odpowiednio do danego systemu oraz wspieranych przez system procesów biznesowych. Ustalenia te powinny być odpowiednio udokumentowane i przetestowane.

17. Archiwizacja

Dane mogą być archiwizowane. Zarchiwizowane dane powinny być sprawdzone pod kątem dostępności, trwałości i dokładności. W przypadku wprowadzenia istotnych zmian w systemie (np. sprzęcie komputerowym lub oprogramowaniu), należy przetestować możliwość odzyskiwania danych.

Słowniczek

Aplikacja: Oprogramowanie zainstalowane na określonej platformie/sprzęcie (hardware) dostarczanie konkretnych funkcjonalność

„Szyty na miarę"/modyfikowany system komputerowy: system komputerowy indywidualnie zaprojektowany, aby pasował do konkretnych procesów biznesowych

Standardowe oprogramowanie z półki: oprogramowanie dostępne na rynku, którego przydatność użytkowa jest potwierdzona przez szerokie spektrum użytkowników.

Infrastruktura IT: sprzęt i oprogramowanie, tj. oprogramowanie sieciowe, systemy operacyjne, niezbędne do funkcjonowania systemu komputerowego.

Cykl życia: wszystkie fazy w życiu systemu począwszy od wstępnych wymagań aż do zakończenia pracy, w tym: projektowanie, specyfikacja, programowanie, testowanie, instalowanie, eksploatacja oraz konserwacja/serwis.

Właściciel procesu: osoba odpowiedzialna za proces biznesowy.

Właściciel System: osoba odpowiedzialna za dostępność i utrzymanie systemu komputerowego oraz bezpieczeństwo przechowywanych danych w systemie.

Strona trzecia: Strona nie związana bezpośrednio z wytwórcą, tj. użytkownikiem systemu.

tłumaczenie: eSynerga Sp. z o.o.