ANEKS 11
SYSTEMY SKOMPUTERYZOWANE

Reguła

Niniejszy Aneks ma zastosowanie do wszystkich rodzajów systemów komputerowych stosowanych w ramach działalności podlegającej regulacjom GMP.

Oprogramowania użytkowe zainstalowane na określonej platformie lub sprzęcie komputerowym, zapewniające określoną funkcjonalność (aplikacje) powinny być zwalidowane, a infastruktura IT powinna być skwalifikowana.

Zastąpienie systemem komputerowym operacji wykonywanych manualnie nie może prowadzić do obniżenia jakości produktu, poziomu kontroli procesu czy zapewnienia jakości. Nie powinno również prowadzić do zwiększenia ogólnego ryzyka procesu.

Zasady ogólne

1. Zarządzane ryzykiem

Zarządzanie ryzykiem powinno być stosowane w ciągu całego cyklu życia systemu komputerowego, ze względu na bezpieczeństwo pacjenta, spójność danych i jakość produktów. Decyzje związane z zakresem walidacji i kontroli spójności danych, będące częścią systemu zarządzania ryzykiem, powinny się opierać na uzasadnionej i udokumentowanej ocenie ryzyka systemu komputerowego.

Komentarz [WK1]: Procedura nadzorowania systemu

2. Personel

Należy zapewnić ścisłą współpracę pomiędzy całym niezbędnym personelem, takim jak osoba odpowiedzialna za proces, administrator systemu komputerowego, Osoby Wykwalifikowane oraz specjaliści w dziedzinie informatyki. Wszyscy pracownicy powinni mieć odpowiednie kwalifikacje i poziom dostępu do systemu komputerowego oraz zdefiniowane obowiązki niezbędne do wykonywania swych zadań.

Komentarz [WK2]: Procedura nadawania uprawnień

3. Dostawcy i usługodawcy

3.1 Jeżeli niektóre działania są wykonywane przez stronę trzecią, która nie jest bezpośrednio zarządzana przez podmiot posiadający zezwolenie na wytwarzanie lub import (np. dostawców, usługodawców), muszą być podpisane formalne umowy między wytwórcą a tą stroną trzecią. Umowy te powinny zawierać jednoznaczne deklaracje dotyczące odpowiedzialności strony trzeciej. Analogicznie powinny być traktowane działy IT. Działania wymagające takich umów to na przykład: dostarczanie, instalacja, konfigurowanie, integracja, walidacja, obsługa techniczna (np. poprzez zdalny dostęp), a także modyfikacje i utrzymanie systemu komputerowego lub związanych z nim usług czy też przetwarzanie danych.

3.2 Kluczowymi czynnikami przy wyborze dostawcy produktów lub usług są jego kompetencje i rzetelność. Potrzeba przeprowadzenia audytu u dostawcy powinna być oparta na ocenie ryzyka.

3.3 Dokumentacja dostarczona wraz z produktami będącymi standardowymi pakietami oprogramowania (COTS) powinna zostać poddana przeglądowi przez uprawnionego użytkownika w celu sprawdzenia, czy produkt spełnia jego wymagania.

3.4 Informacje dotyczące systemu jakości oraz dokumentacja z przeprowadzonego audytu u dostawców lub producentów oprogramowania i stosowanych systemów komputerowych powinny być dostępne na żądanie inspektorów do spraw wytwarzania Głównego Inspektoratu Farmaceutycznego.

Faza projektowa

4. Walidacja

4.1 Dokumentacja i raporty walidacyjne powinny obejmować odpowiednie etapy cyklu życia systemu komputerowego. Wytwórcy powinni uzasadnić, w oparciu o przeprowadzoną ocenę ryzyka, standardy, protokoły, kryteria akceptacji, procedury i zapisy.

4.2 Dokumentacja walidacyjna powinna zawierać zapisy z kontroli zmian (jeżeli dotyczy)oraz raporty z wszelkich odchyleń zaobserwowanych w czasie procesu walidacji.

4.3 Powinny być dostępne aktualne wykazy (inwentaryzacja) wszystkich istotnych systemów komputerowych i ich funkcjonalność w odniesieniu do GMP.

Komentarz [WK3]: Wykaz systemów

Dla systemów komputerowych o znaczeniu krytycznym powinien być dostępny aktualny opis zastosowanych rozwiązań fizycznych i logicznych, przepływu danych oraz interfejsów z innymi systemami komputerowymi lub procesami oraz sprzętem komputerowym i oprogramowaniem stosowanym uprzednio, a także stosowane środki bezpieczeństwa.

4.4 Specyfikacje Wymagań Użytkownika (URS) powinny opisywać wymagane przez użytkownika funkcje systemu komputerowego i powinny być oparte na udokumentowanej ocenie ryzyka i wpływu systemu komputerowego na spełnienie wymagań GMP. Wymagania użytkowników powinny być identyfikowalne w całym cyklu życia systemu komputerowego.

4.5 Użytkownik uprawniony powinien podjąć wszelkie uzasadnione kroki w celu zapewnienia, że system komputerowy został stworzony zgodnie z odpowiednim systemem zarządzania jakością. Dostawca powinien być odpowiednio oceniany.

4.6 W celu walidacji systemów komputerowych indywidualnie dostosowanych lub zaprojektowanych do prowadzonej działalności klienta powinien zostać przeprowadzony proces, który zapewni formalną ocenę i raport, odnoszące się do jakości i wydajności pomiarów na wszystkich etapach cyklu życia systemu komputerowego.

4.7 Powinna istnieć ewidencja wykazująca, że zastosowano odpowiednie metody badań i scenariusze testowe. W szczególności należy wziąć pod uwagę wartości graniczne parametrów systemu komputerowego (procesu), limity danych i zarządzanie odchyleniami. Powinna istnieć udokumentowana ocena przydatności zautomatyzowanych narzędzi badawczych i środowisk testowych.

4.8 Jeżeli dane są transferowane do innego formatu lub systemu komputerowego, walidacja powinna obejmować sprawdzenie, czy podczas tego procesu nie zostały zmienione wartość lub znaczenie danych.

Faza działania

5. Dane

W celu zminimalizowania ryzyka, komputerowe systemy elektronicznej wymiany danych z innymi systemami komputerowymi, powinny zawierać wbudowane odpowiednie elementy kontrolujące poprawność i bezpieczeństwo wprowadzania i przetwarzania danych.

6. Kontrola poprawności

Dla danych krytycznych wprowadzanych ręcznie, należy dodatkowo sprawdzić ich poprawność. Sprawdzenia te mogą być wykonywane przez drugiego operatora lub przy użyciu zwalidowanych narzędzi elektronicznych. Krytyczność i potencjalne konsekwencje błędnie lub nieprawidłowo wprowadzonych do systemu komputerowego danych powinny podlegać zarządzaniu ryzykiem.

7. Przechowywanie danych

7.1 Dane powinny być zabezpieczone przed uszkodzeniem zarówno fizycznie, jak i w sposób elektroniczny. Przechowywane dane powinny być sprawdzone pod kątem dostępności, poprawności i możliwości odczytu. Dostęp do danych powinien zostać zapewniony przez cały okres ich przechowywania.

7.2 Regularnie powinny być wykonywane kopie bezpieczeństwa wszelkich istotnych danych. Spójność i rzetelność kopii zapasowych i możliwość przywrócenia danych powinny być sprawdzane w trakcie walidacji i okresowo monitorowane.

8. Wydruki

8.1 Powinno być możliwe czytelne drukowanie danych przechowywanych elektronicznie.

8.2 W przypadku zapisów stanowiących podstawę do zwolnienia serii do obrotu powinno być możliwe otrzymanie wydruków wskazujących, czy jakiekolwiek dane zostały zmienione od momentu pierwotnego wprowadzenia (wygenerowania).

9. Dziennik nadzoru

Na podstawie oceny ryzyka należy rozważyć wbudowanie do systemu komputerowego elementu tworzącego rejestr wszystkich zmian i skreśleń istotnych w aspekcie GMP (system generujący „dziennik nadzoru"). W celu zmiany lub usunięcia danych istotnych dla GMP, powinien zostać udokumentowany powód takiego postępowania. Dzienniki nadzoru powinny być dostępne i możliwe do wygenerowania w postaci zrozumiałych formularzy i regularnie kontrolowane.

Komentarz [WK4]: Aktualna: specyfikacja funkcjonalna FS, specyfikacja projektowa software SDS, specyfikacja projektowa hardware HDS. W przypadku zmian należy aktualizować w/w dokumenty.

Komentarz [WK5]: Procedura backup i restore wraz dowodami poprawnego funkcjonowania (np. log oraz rejestr sprawdzeń).

10. Zarządzanie zmianami i konfiguracjami

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

11. Ocena okresowa

Systemy komputerowe powinny być okresowo oceniane w celu potwierdzenia, że pozostają one w stanie zwalidowanym i są zgodne z GMP. Ocena ta powinna obejmować, jeżeli to konieczne, bieżący zakres funkcjonalności, zapisy z odchyleń, incydentów, problemów, historię aktualizacji, wydajność, niezawodność, bezpieczeństwo i raporty statusu walidacji.

12. Bezpieczeństwo

12.1 W celu ograniczenia dostępu do systemu komputerowego tylko dla osób upoważnionych powinny być wprowadzone zabezpieczenia fizyczne lub logiczne. Odpowiednimi metodami zapobiegania nieupoważnionym wejściom do systemu komputerowego mogą być klucze, karty dostępu, osobiste kody z hasłami, dane biometryczne, ograniczony dostęp do sprzętu komputerowego i miejsc przechowywania danych.

12.2 Zakres zabezpieczeń zależy od krytyczności systemu komputerowego.

12.3 Ustanawianie, zmiana i cofnięcie dostępu powinny być rejestrowane.

12.4 Systemy zarządzania danymi i dokumentami powinny być tak zaprojektowane, aby rejestrować tożsamość osób wprowadzających, potwierdzających i usuwających dane oraz dokonujących w nich zmian, w tym datę i godzinę wykonania czynności.

13. Zarządzanie incydentami

Wszystkie incydenty, nie tylko awarie systemu komputerowego i błędne dane, powinny być zgłaszane i oceniane. Główna przyczyna incydentu krytycznego powinna zostać zidentyfikowana i powinna stanowić podstawę działań korygujących i zapobiegawczych.

14. Autoryzowanie w sposób elektroniczny

Zapisy elektroniczne mogą być autoryzowane w sposób elektroniczny. Autoryzacja powinna spełniać następujące wymagania:

1) w obszarze przedsiębiorstwa być równoważna z podpisem odręcznym;
2) być trwale związana z zapisem, którego dotyczy;
3) zawierać datę i godzinę użycia.

15. Zwolnienie serii

System komputerowy, stosowany do rejestrowania certyfikacji i zwolnienia serii, powinien zezwalać na przeprowadzanie tych czynności tylko Osobom Wykwalifikowanym. System komputerowy powinien również jednoznacznie identyfikować i rejestrować osobę zwalniającą lub certyfikującą serię. Czynności te w obszarze przedsiębiorstwa powinny być autoryzowane w sposób, o którym mowa w pkt 14.

16. Ciągłość działania

W celu prawidłowego funkcjonowania systemów komputerowych wspierających procesy krytyczne należy wprowadzić przepisy zapewniające ciągłość i dostępność danych, będących podstawą tych procesów, na wypadek awarii systemu komputerowego (np. zapisy odręczne lub alternatywny system komputerowy). Czas potrzebny na wdrożenie rozwiązań alternatywnych powinien być oparty na ocenie ryzyka i odpowiedni dla danego systemu komputerowego oraz prowadzonej działalności. Ustalenia te powinny być odpowiednio udokumentowane i sprawdzone.

17. Archiwizacja

Dane mogą być archiwizowane w systemie komputerowym. Dane te powinny być sprawdzone pod kątem dostępności, czytelności i spójności. Jeżeli do systemu komputerowego mają zostać wprowadzone istotne zmiany (np. zmiana sprzętu komputerowego lub oprogramowania), to powinna zostać zapewniona i przetestowana możliwość odzyskiwania danych.

Komentarz [WK6]: Procedura kontroli zmian

Komentarz [WK7]: Procedura nadzorowania systemu (w tym cykliczny przegląd dziennika nadzoru pkt 9 – audit trail).
Ocenę okresową można zrealizować również w oparciu o mechanizmy Audytu Wewnętrznego funkcjonującego w firmie

Komentarz [WK8]: Jeżeli system nie rejestruje zmian w zakresie uprawnień, należy rejestrować zmiany zgodnie z zapisami Procedura nadawania uprawnień / zarządzania systemem.

Komentarz [WK9]: Procedura nadzorowania systemu

Komentarz [WK10]: Procedura postępowania podczas awarii systemu. Jeżeli firma wstrzymuje pracę, podczas awarii systemu, należy zapewnić dostęp do informacji pozwalających na wycofanie produktu.

Komentarz [WK11]: Procedura backup i restore wraz dowodami poprawnego funkcjonowania (np. log oraz rejestr sprawdzeń).