TYTUŁ-ŻYWNOŚĆ I LEKI

ROZDZIAŁ I - FOOD AND DRUG ADMINISTRATION,

CZĘŚĆ 11 – DOKUMENTY I PODPISY ELEKTRONICZNE

Podrozdział A—Przepisy ogólne

§11.1 Zakres.

(a) Przepisy niniejszego rozdziału ustalają kryteria, według których agencja uznaje dokumenty (zapisy) elektroniczne, podpisy elektroniczne oraz własnoręczne podpisy złożone na dokumentach elektronicznych za wiarygodne, rzetelne i ogólnie biorąc równoważne dokumentom papierowym i własnoręcznym podpisom złożonym na papierze.

(b) Niniejsza część ma zastosowanie do zapisów w formie elektronicznej, które są tworzone, modyfikowane, archiwowane, pobierane lub przesyłane zgodnie z wymogami uregulowań agencji. Niniejsza część ma również zastosowanie do dokumentów (zapisów) elektronicznych złożonych w agencji zgodnie z wymaganiami Federal Food, Drug, and Cosmetic Act (Ustawa Federalna o Żywności, Używkach i Kosmetykach) oraz Public Health Service Act (Ustawa o Publicznej Służbie Zdrowia), nawet jeśli te dokumenty (zapisy) nie są wyraźnie wymienione w uregulowaniach agencji. Część ta nie ma jednak zastosowania do dokumentów papierowych, które są lub były przesyłane drogą elektroniczną.

(c) Gdy podpisy elektroniczne oraz dokumenty elektroniczne, do których przynależą, spełniają wymagania niniejszej części, agencja uzna podpisy elektroniczne za równoważne podpisom, parafom oraz innym ogólnym znakom wykonanym własnoręcznie, zgodnie z uregulowaniami agencji, o ile nie zostaną one wyraźnie wyłączone przez uregulowania wchodzące w życie począwszy od dnia 20 sierpnia 1997 r.

(d) Dokumenty elektroniczne spełniające wymagania niniejszej części mogą być stosowane zgodnie z §11.2 zamiast dokumentów papierowych, o ile dokumenty papierowe nie są wyraźnie wymagane.

(e) Systemy komputerowe (w tym sprzęt i oprogramowanie), środki kontroli i towarzysząca im dokumentacja prowadzona zgodnie z wymogami niniejszej części, powinny być łatwo dostępne i podlegają kontroli FDA.

§11.2 Wdrożenie.

(a) Dokumenty, których przechowywanie jest wymagane, ale nie jest wymagane przedłożenie ich agencji, można wykorzystywać dokumenty elektroniczne zamiast dokumentów papierowych lub podpisy elektroniczne zamiast podpisów tradycyjnych, w całości lub w części, pod warunkiem, że zostaną spełnione wymagania niniejszej części.

(b) W przypadku dokumentów przedkładanych agencji, można wykorzystywać dokumenty elektroniczne zamiast dokumentów papierowych lub podpisy elektroniczne zamiast podpisów tradycyjnych, w całości lub w części, pod warunkiem, że:

(1) Wymagania niniejszej części zostaną spełnione oraz

(2) Dokument lub część dokumentu, który ma być przedłożony figuruje w publicznym rejestrze Nr 92S-0251, jako typ dokumentu, który agencja akceptuje w formie elektronicznej. Rejestr ten wyraźnie ustala, które typy dokumentów lub części dokumentów można przedkładać w postaci elektronicznej, bez dokumentów papierowych wraz z jednostką(ami) przyjmującymi agencji (np. konkretne centrum, biuro, dział, oddział), gdzie takie dokumenty można składać. Dokumenty złożone w jednostce(kach) je przyjmujących w agencji, nie wymienione w publicznym rejestrze

jako oficjalne, nie będą traktowane jak oficjalne, jeśli zostaną złożone w formie *elektronicznej*; jako oficjalne będą traktowane dokumenty takie złożone w formie papierowej i muszą być dołączone do wszelkich dokumentów elektronicznych. Niezbędne jest skontaktowanie się z właściwą jednostką przyjmującą agencji, w sprawie szczegółowych informacji dotyczących sposobu (np. metody transmisji, nośników, formatów plików i protokołów technicznych) oraz, czy można te dokumenty składać w formie elektronicznej.

§11.3 Definicje.

(a) Dla celów niniejszej części mają zastosowanie definicje i interpretacje zawarte w Artykule 201 Ustawy.

(b) W niniejszej części mają również zastosowanie następujące definicje:

(1) *Ustawa* oznacza Ustawę Federalną o Żywności, Używkach i Kosmetykach (artykuły 201-903 (21 U.S.C. 321-393)).

(2) *Agencja* oznacza Food and Drug Administration (Agencję ds. Żywności i Leków).

(3) *Biometria* oznacza metodę weryfikacji tożsamości osoby fizycznej, opartą na pomiarze takich cech fizycznych lub charakterystycznych zachowań osoby fizycznej, które są zarówno unikalne dla tej osoby i jak mierzalne.

(4) *System zamknięty* oznacza środowisko, w którym dostęp do systemu jest kontrolowany przez osoby odpowiedzialne za zawartość zapisów elektronicznych znajdujących się w tym systemie.

(5) *Podpis cyfrowy* oznacza podpis elektroniczny oparty na wykorzystaniu kryptograficznych metod uwierzytelnienia autora, tworzony dzięki wykorzystaniu szeregu reguł oraz zestawu parametrów w taki sposób, że zarówno tożsamość osoby podpisującej jak i integralność danych może być weryfikowana.

(6) *Dokument (zapis) elektroniczny* oznacza dowolną kombinację informacji tekstowych, graficznych, danych, głosowych, obrazów lub informacji podawanych innymi sposobami przedstawiania, tworzonych, modyfikowanych, utrzymywanych, archiwowanych, odczytywanych lub rozpowszechnianych w systemie komputerowym.

(7) *Podpis elektroniczny* oznacza kompilację danych w postaci elektronicznej, złożonych z dowolnego symbolu lub serii symboli, złożony, zastosowany lub autoryzowany przez osobę fizyczną, jako prawnie wiążący odpowiednik własnoręcznego podpisu tej osoby

(8) *Podpis ręczny* oznacza rękopis nazwiska lub znaku graficznego osoby fizycznej, napisany własnoręcznie przez tę osobę i złożony lub przyjęty z zamiarem poświadczenia dokumentu w sposób trwały. Zachowany jest charakter czynności podpisu za pomocą przyboru do pisania lub znakowania, np. pióra lub rylca. Rękopis nazwiska lub znaku graficznego, konwencjonalnie stawiany na papierze, może być również stawiany na innych środkach wyrazu, w celu utrwalenia nazwiska lub znaku.

System *otwarty* oznacza środowisko, w którym dostęp do systemu nie jest kontrolowany przez osoby odpowiedzialne za zawartość zapisów elektronicznych znajdujących się w tym systemie.

Podrozdział B—Dokumenty (zapisy) elektroniczne

§11.10 Nadzór na systemami zamkniętymi.

Osoby korzystające z systemów zamkniętych do tworzenia, utrzymywania lub przesyłania dokumentów elektronicznych powinny stosować procedury i środki kontroli służące zapewnieniu autentyczności, integralności i, o ile to stosowne, poufności dokumentów elektronicznych, oraz zapewnienia, że osoba podpisująca nie może łatwo odrzucić podpisanych dokumentów, jako nieautentycznych. Takie procedury i środki kontroli powinny obejmować:

(a) Walidację systemów w celu zapewnienia dokładności, wiarygodności, konsekwentnego zamierzonego funkcjonowania oraz rozpoznawania nieważnych lub zmienionych zapisów.

(b) Zdolność do generowania dokładnych i kompletnych kopii zapisów, zarówno w formie możliwej do odczytu przez ludzi, jak i elektronicznej, nadającej się do kontroli, analizy i skopiowania przez agencję. Osoby te powinny kontaktować się z agencją, czy istnieją jakiekolwiek wątpliwości co do zdolności agencji do przeprowadzenia takiej analizy i kopiowania zapisów elektronicznych.

(c) Ochrona zapisów, umożliwiająca ich dokładny i bezpośredni odczyt przez cały okres utrzymywania tych zapisów.

(d) Ograniczenie dostępu do systemu osobom nieuprawnionym.

(e) Użycie bezpiecznych, generowanych komputerowo, znakowanych czasem raportów pouadytowych, w celu niezależnego rejestrowania daty i czasu dokonania wpisu przez operatora lub czynności tworzenia, modyfikowania lub usuwania zapisów elektronicznych. Zmiany zapisów nie powinny przesłaniać informacji zapisanych wcześniej. Taka dokumentacja poaudytowa powinna być przechowywana przynajmniej przez okres wymagany dla odpowiednich zapisów elektronicznych oraz powinna być dostępna do przeglądu i skopiowania przez agencję.

(f) Przeprowadzanie kontroli systemu operacyjnego w celu wyegzekwowania dozwolonej kolejności działań, i zdarzeń, stosownie do okoliczności.

(g) Stosowanie kontroli uprawnień, w celu zapewnienia, aby wyłącznie osoby uprawnione mogły korzystać z systemu, składać podpisy elektroniczne pod dokumentami, miały dostęp do systemu operacyjnego lub urządzenia wejściowego lub wyjściowego systemu komputerowego, zmieniać zapisy lub wykonywać czynności kontrolne.

(h) Przeprowadzanie kontroli urządzeń (np. terminali), w celu określenia, stosownie do okoliczności, poprawności wprowadzanych danych wejściowych lub instrukcji operacyjnych.

(i) Ustalanie, czy osoby, które opracowują, utrzymują lub eksploatują systemy dokumentacji elektronicznej/ podpisów elektronicznych posiadają wykształcenie, przeszkolenie i doświadczenie do wykonywania wyznaczonych im zadań.

(j) Ustanowienie i przestrzeganie pisemnych polityk, które czynią poszczególna osoby odpowiedzialnymi za czynności rozpoczynające się od złożenia przez nie podpisu elektronicznego, w celu zniechęcenia do fałszowania dokumentów i podpisów.

(k) Stosowanie odpowiednich środków kontroli dokumentacji systemowych, w tym:

(1) Odpowiednich środków kontroli dystrybucji, dostępu i korzystania z dokumentacji dotyczącej obsługi i konserwacji systemu.

(2) Procedury nadzoru nad zmianami, uwzględniające prowadzenie raportu poaudytowego, dokumentującego kolejność czasową czynności opracowywania i zmian w dokumentacji systemowej.

§11.30 Nadzór na systemami otwartymi.

Osoby korzystające z systemów otwartych do tworzenia, modyfikowania, prowadzenia lub przesyłania dokumentów elektronicznych powinny stosować procedury i środki kontroli służące

zapewnieniu autentyczności, integralności i, stosownie do okoliczności, poufności dokumentów elektronicznych, od miejsca ich utworzenia do miejsca odbioru. Takie procedury i środki kontroli powinny obejmować elementy wymienione już w §11.10, stosownie do okoliczności, oraz dodatkowe środki takie, jak szyfrowanie dokumentów i stosowanie odpowiednich standardów podpisów cyfrowych w celu zapewnienia, w razie potrzeby w danych okolicznościach, autentyczności, integralności i poufności dokumentów.

§ 11.50 Znaki podpisu.

(a) Podpisane dokumenty elektroniczne powinny zawierać informacje związane z czynnością podpisu, które jednoznacznie określają każdy z następujących elementów:

(1) Drukowane imię i nazwisko osoby podpisującej;

(2) Datę i czas, kiedy podpis został złożony, oraz

(3) Znaczenie związane z podpisem (np. przegląd, zatwierdzenie, odpowiedzialność lub autorstwo).

(b) Elementy wymienione w punktach (a)(1), (a)(2) i (a)(3) niniejszego rozdziału podlegają takim samym środkom kontroli, jak zapisy elektroniczne i powinny być uwzględnione w dowolnej formie zapisu elektronicznego, możliwej do odczytania dla człowieka (np. na wyświetlaczu elektronicznym lub wydruku).

§11.70 Łączenie podpisu z rekordem elektronicznym.

Podpisy elektroniczne i podpisy ręczne złożone w dokumentach elektronicznych powinny być połączone z odpowiednimi dokumentami elektronicznymi w celu zapewnienia, że te podpisy nie mogą być usunięte, skopiowane lub w inny sposób przeniesione w celu sfałszowania dokumentu elektronicznego zwykłymi metodami.

Podrozdział C—Podpisy elektroniczne

§ 11.100 Wymagania ogólne.

(a) Każdy podpis elektroniczny powinien być unikatowy dla danej osoby i nie może być ponownie wykorzystany ani przydzielony komukolwiek innemu.

(b) Zanim organizacja ustanowi, przydzieli, potwierdzi lub w inny sposób zaaprobuje podpis elektroniczny osoby fizycznej lub jakikolwiek element takiego podpisu, organizacja ta musi zweryfikować tożsamość tej osoby.

(c) Osoby używające podpisów elektronicznych powinny przed lub z chwilą jego użycia poświadczyć w agencji, że w ich systemie podpisy elektroniczne, używane od 20 sierpnia 1997 mają być prawnie wiążącymi odpowiednikami tradycyjnych własnoręcznych podpisów.

(1) Poświadczenie powinno być złożone w formie papierowej i podpisane tradycyjnym, własnoręcznym podpisem, w Office of Regional Operations (Biurze Operacji Regionalnych) (HFC-100), 5600 Fishers Lane, Rockville, MD 20857.

(2) Osoby używające podpisów elektronicznych powinny na żądanie agencji dostarczyć dodatkowe poświadczenie lub świadectwo, że konkretny podpis elektroniczny jest prawnie wiążącym odpowiednikiem własnoręcznego podpisu sygnatariusza.

§ 11.200 Elementy składowe podpisu elektronicznego oraz środki kontroli.

(a) Podpisy elektroniczne, które nie są oparte na biometrii powinny:

(1) Stosować co najmniej dwa różne elementy identyfikujące takie, jak kod identyfikacyjny i hasło.

(i) Gdy dana osoba składa szereg podpisów w trakcie pojedynczego, ciągłego okresu

kontrolowanego dostępu do systemu, pierwszy podpis powinien być złożony z użyciem wszystkich elementów składowych podpisu elektronicznego; następne podpisy należy składać z użyciem co najmniej jednego elementu składowego podpisu elektronicznego, który może być złożony i jest przeznaczony do wykorzystania wyłącznie przez tę osobę.

(ii) Gdy dana osoba składa jeden lub więcej podpisów nie podczas jednego, ciągłego cyklu kontrolowanego dostępu do systemu, każdy podpis powinien być złożony z użyciem wszystkich elementów składowych podpisu.

(2) Być używane wyłącznie przez ich oryginalnych właścicieli, oraz

(3) Być administrowane i składane w taki sposób, który zapewnia, że próba wykorzystania podpisu elektronicznego danej osoby przez kogokolwiek innego poza jego oryginalnym właścicielem, wymaga współdziałania dwóch lub więcej osób.

(b) Podpisy elektroniczne oparte na biometrii powinny być tak zaprojektowane, aby zapewnić, że nie będą one mogły być użyte przez kogokolwiek innego poza ich oryginalnym właścicielem.

§ 11.300 Środki kontroli kodów identyfikacyjnych/ hasła.

Osoby używające podpisów elektronicznych opartych na kodach identyfikacyjnych w połączeniu z hasłami, powinny stosować środki kontroli zapewniające ich bezpieczeństwo i integralność. Takie środki kontroli obejmują:

(a) Utrzymywanie niepowtarzalności każdej kombinacji kodu identyfikacyjnego i hasła tak, aby dwie osoby nie miały tej samej kombinacji kodu identyfikacyjnego i hasła.

(b) Zapewnienie, aby wydania kodu identyfikacyjnego i hasła były okresowo sprawdzane, odwoływane lub zmieniane (np. w celu uwzględnienia takich okoliczności, jak dezaktualizacja hasła).

(c) Przestrzeganie procedur postępowania w przypadku utraty, w celu elektronicznego unieważnienia zagubionych, ukradzionych, zaginionych lub w inny sposób potencjalnie narażonych na szwank nośników danych uwierzytelniających, kart i innych urządzeń zawierających lub generujących kod identyfikacyjny lub hasło, oraz wydawanie tymczasowych lub stałych zamienników, przy stosowaniu odpowiednich, rygorystycznych środków kontroli.

(d) Używanie zabezpieczeń transakcji w celu uniemożliwienie nieautoryzowanego użycia haseł i/lub kodów identyfikacyjnych oraz wykrywania i natychmiastowego rejestrowania wszelkich prób ich nieautoryzowanego użycia w jednostce bezpieczeństwa systemu oraz, stosownie do okoliczności, w zarządzaniu organizacją.

(e) Wstępne i okresowe badania urządzeń takich, jak nośniki danych uwierzytelniających lub karty, które zawierają lub generują kod identyfikacyjny lub hasło, w celu upewnienia się, że działają poprawnie i nie zostały w sposób nieuprawniony przerobione.

Źródło: 62 FR 13464 20.03.1997.