Projekt z dnia 26 stycznia 2011 r.

ROZPORZĄDZENIE

MINISTRA ZDROWIA [1)]

z dnia .....2012 r.

w sprawie Systemu Monitorowania Zagrożeń

Na podstawie art. 26 ust. 9 ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz. U. Nr 113, poz. 657 i Nr 174, poz. 1039), zarządza się co następuje:

§ 1. Rozporządzenie określa:

1) minimalną funkcjonalność Systemu Monitorowania Zagrożeń, zwanego dalej „systemem";
2) warunki organizacyjno – techniczne gromadzenia i udostępniania danych gromadzonych w systemie.

§ 2. Określenia użyte w rozporządzeniu oznaczają:

1) bezpieczny podpis elektroniczny – podpis elektroniczny w rozumieniu art. 3 pkt 2 ustawy z dnia 18 września 2001 r. o podpisie elektronicznym (Dz. U. Nr 130, poz. 1450, z późn. zm[2)]);
2) centralne repozytorium wzorów dokumentów elektronicznych – miejsce, o którym mowa w art. 19b ust. 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. Nr 64 poz. 565, z późn. zm[3)]);
3) podpis osobisty – podpis osobisty w rozumieniu art. 2 ust. 1 pkt 11 ustawy z dnia 6 sierpnia 2010 r. o dowodach osobistych (Dz. U. Nr 167 poz. 1131, oraz z 2011 r. Nr 133, poz. 768);

[1)] Minister Zdrowia kieruje działem administracji rządowej – zdrowie, na podstawie § 1 ust. 2 rozporządzenia Prezesa Rady Ministrów z dnia 18 listopada 2011 r. w sprawie szczegółowego zakresu działania Ministra Zdrowia (Dz. U. Nr 248, poz. 1495 i Nr 284, poz.1672).

[2)] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2002 r. Nr 153, poz. 1271, z 2003 r. Nr 124, poz. 1152, Nr 217, poz. 2125, z 2004 r. Nr 96, poz. 959, z 2005 r. Nr 64, poz. 565, z 2006 r. Nr 145, poz. 1050, z 2009 r. Nr 18, poz. 97, z 2010 r. Nr 40, poz. 230, Nr 182, poz. 1228 oraz z 2011 r. Nr 106, poz. 622.

[3)] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2006 r. Nr 12, poz. 65 i Nr 73, poz. 501, z 2008 r. Nr 127, poz. 817, z 2009 r. Nr 157, poz. 1241, z 2010 r. Nr 40, poz. 230, Nr 167, poz. 1131 i Nr 182, poz. 1228 oraz z 2011 r. Nr 112, poz. 654, Nr 185, poz. 1092 i Nr 204, poz. 1195.

4) profil zaufany ePUAP – zestaw informacji w rozumieniu art. 3 pkt 14 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne;

5) ustawa – ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia.

§ 3. 1. System w zakresie minimalnej funkcjonalności zapewnia następujące usługi:

1) przyjęcia i potwierdzenia przyjęcia elektronicznego formularza zgłoszeniowego wraz z ewentualnymi załącznikami;
2) automatycznej rejestracji elektronicznego formularza zgłoszeniowego;
3) weryfikacji elektronicznego formularza zgłoszeniowego pod względem braków formalnych i jego nieprzyjęcia w przypadku ich wystąpienia;
4) nadawania statusu sprawie;
5) generowania i publikacji raportów, w tym statystycznych;
6) automatycznego tworzenia wykazu elektronicznych formularzy zgłoszeniowych i ich udostępniania administratorom danych, o których mowa w art. 26 ust. 6 ustawy;
7) udostępniania uprawnionym podmiotom, o których mowa w art. 26 ust. 2 ustawy, informacji o zagrożeniach i niepożądanych zdarzeniach stanowiących zagrożenie dla zdrowia lub życia, przy wykorzystaniu systemów Elektronicznej Platformy Gromadzenia, Analizy i Udostępnienia Zasobów Cyfrowych o Zdarzeniach Medycznych, o której mowa w art. 7 ustawy, i Systemu Wspomagania Ratownictwa Medycznego, o którym mowa w art. 25 ustawy.

2. Raporty, o których mowa w ust. 1 pkt 5, mogą być publikowane na portalu edukacyjno – informacyjnym, o którym mowa w art. 36 ustawy.

3. System w zakresie swojej funkcjonalności ma wbudowaną funkcję umożliwiającą okresowe automatyczne wykonywanie kopii bezpieczeństwa.

4. System umożliwia rejestrację prób logowania do systemu oraz zdefiniowanie zestawu śledzonych czynności wykonywanych przez użytkowników.

§ 4. 1. System zapewnia realizację usług poprzez umieszczanie i odbieranie dokumentów elektronicznych w formacie XML w strukturach i formatach umożliwiających komunikację. z wykorzystaniem protokołów komunikacyjnych i szyfrujących, o których mowa w art. 13 ust. 2 pkt 2 lit a ustawy

z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne.

2. Struktury i formaty, o których mowa w ust. 1, udostępnia się razem z dokumentacją opisu systemu na portalu edukacyjno - informacyjnym, o którym mowa w art. 36 ustawy, oraz w Biuletynie Informacji Publicznej ministra właściwego do spraw zdrowia.

3. Dokumenty elektroniczne, o których mowa w ust. 1, podpisuje się bezpiecznym podpisem elektronicznym, podpisem osobistym albo z wykorzystaniem profilu zaufanego ePUAP.

4. Wzory dokumentów elektronicznych, o których mowa w ust. 1, przechowywane są w centralnym repozytorium wzorów dokumentów elektronicznych, na portalu edukacyjno - informacyjnym, o którym mowa w art. 36 ustawy, oraz w Biuletynie Informacji Publicznej ministra właściwego do spraw zdrowia.

§ 5. W zakresie warunków organizacyjno – technicznych gromadzenia i pobierania danych przetwarzanych w systemie, system musi być zgodny z następującymi normami, których przedmiotem są zasady gromadzenia i wymiany informacji w ochronie zdrowia:

1) PN-ISO/IEC 27001:2007 Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji – Wymagania;
2) PN-ISO/IEC 17799:2007 Technika informatyczna. Techniki bezpieczeństwa. Praktyczne zasady zarządzania bezpieczeństwem informacji;
3) PN-ISO/IEC 27005:2010 Technika informatyczna. Techniki bezpieczeństwa. Zarządzanie ryzykiem w bezpieczeństwie informacji;
4) PN-EN ISO 27799:2010 Informatyka w ochronie zdrowia. Zarządzanie bezpieczeństwem informacji w ochronie zdrowia z wykorzystaniem ISO/IEC 27002;
5) PN-EN 13606:1-4:2009 Informatyka w ochronie zdrowia. Przesyłanie elektronicznej dokumentacji zdrowotnej;
6) PN-EN ISO 13606-5:2010 Informatyka w ochronie zdrowia. Przesyłanie elektronicznej dokumentacji zdrowotnej.

- albo normami, wersjami i standardami je zastępującymi.

§ 6. Administrator systemu w zakresie niezbędnym dla właściwego działania przypisanego mu systemu opracowuje, wdraża, nadzoruje, utrzymuje oraz w uzasadnionych przypadkach modyfikuje system zarządzania bezpieczeństwem informacji, zwany dalej „SZBI".

2. Administrator systemu jest obowiązany dostosowywać SZBI do aktualnych potrzeb organizacyjnych i technicznych w sposób umożliwiający przeciwdziałanie jakimkolwiek naruszeniom bezpieczeństwa informacji.

3. Administrator systemu, zgodnie z określonym zakresem odpowiedzialności, prowadzi nie rzadziej niż raz do roku audyt SZBI, w celu kontroli stopnia przestrzegania wymagań SZBI.

4. Audyt SZBI jest przeprowadzany przez uprawnionego audytora.

5. Uzyskane w wyniku audytu SZBI informacje świadczące o możliwości zaistnienia lub zaistnieniu naruszenia bezpieczeństwa informacji zabezpiecza się i przechowuje w celach dowodowych.

§ 7. 1. Na SZBI składają się następujące działania:

1) identyfikacja i analiza zagrożeń bezpieczeństwa informacji oraz określenie zabezpieczeń odpowiednich do stwierdzonych zagrożeń;
2) klasyfikowanie i kontrolowanie dostępu do zasobów systemu teleinformatycznego oraz do informacji przetwarzanych przez ten system;
3) dobór i szkolenie personelu wykorzystującego system teleinformatyczny;
4) zabezpieczenie fizyczne obiektów i urządzeń systemu;
5) opracowanie i utrzymywanie systemu z uwzględnieniem wymogów bezpieczeństwa i stosowaniem kryptograficznej ochrony danych zwłaszcza w czasie transmisji;
6) zarządzanie ciągłością działania systemu teleinformatycznego, zwłaszcza w warunkach wystąpienia naruszenia bezpieczeństwa informacji albo zagrożenia jego wystąpienia.

2. Działań, o których mowa w ust. 1, dokonuje się z zachowaniem wymagań zgodnych z normą PN-ISO/IEC 27001:2007 Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji – Wymagania.

§ 8. Przekazanie systemu do eksploatacji administratorowi systemu wymaga opracowania:

1) strategii i zakresu SZBI właściwego dla podmiotu publicznego i zakresu zadań publicznych, które realizuje;
2) zasad postępowania w przypadku wystąpienia naruszenia bezpieczeństwa informacji;
3) zasad postępowania zapobiegającego wystąpieniu naruszenia bezpieczeństwa informacji wraz z oceną ryzyka wystąpienia naruszenia bezpieczeństwa informacji;
4) uzasadnienia ochrony grup informacji;
5) zasad nadzoru nad sporządzaniem i dostępem do dokumentacji SZBI, w zakresie określonym w pkt 1-4.

§ 9. Rozporządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

MINISTER ZDROWIA

W porozumieniu:
MINISTER ADMINISTRACJI I CYFRYZACJI

ność pod względem
m i redakcyjnym

DYREKTOR
Departamentu Prawnego
Władysław
radca prawny

UZASADNIENIE

Projekt rozporządzenia stanowi wykonanie upoważnienia określonego w art. 26 ust. 9 ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz. U. Nr113, poz. 657 i Nr 174, poz. 1039), zwanej dalej „ustawą" i określa minimalną funkcjonalność oraz warunki organizacyjno – techniczne gromadzenia i udostępniania danych w Systemie Monitorowania Zagrożeń.

System Monitorowania Zagrożeń dalej zwany „systemem", określony w art. 26 ustawy jest systemem teleinformatycznym, w rozumieniu art. 2 pkt 3 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. Nr 144, poz. 1204, z późn. zm.). Stanowi on jeden z elementów systemu informacji w ochronie zdrowia.

Projektowane rozporządzenie ma na celu umożliwienie gromadzenia i przetwarzania w jednym miejscu danych w ramach zadań podmiotów prowadzących rejestry zachorowań na choroby zakaźne, podmiotów prowadzących rejestry niepożądanych odczynów poszczepiennych, Prezesa Urzędu Rejestracji Produktów Leczniczych, Wyrobów Medycznych i Produktów Biobójczych i pracowników medycznych. Ponadto system ten umożliwi usługodawcom i innym podmiotom zobowiązanym do składania informacji o zagrożeniach dokonywania zgłoszeń w formie dokumentu elektronicznego.
Gromadzone w systemie dane będą ważnym narzędziem przy podejmowaniu działań w zakresie zapobiegania skutkom niepożądanych zdarzeń medycznych mających wpływ na zdrowie i życie ludzi.

Jednoczesne połączenie Systemu Monitorowania Zagrożeń z danymi gromadzonymi w Systemie Informacji Medycznej spowoduje, że resortowy system wczesnego ostrzegania, umożliwiający uprawnionym podmiotom i organom, umieszczanie i dostęp do informacji o zagrożeniach i niepożądanych zdarzeniach medycznych, stanowiących zagrożenie dla zdrowia lub życia, będzie działał szybko i sprawnie, a co najważniejsze zostanie zrealizowany cel Programu Działań Wspólnotowych w Dziedzinie Zdrowia Publicznego (Decyzja 1786/2002/WE Parlamentu Europejskiego i Rady z dnia 23 września 2002 r.) tj. prowadzenie skoordynowanych działań w zakresie przeciwdziałania skutkom niepożądanych zdarzeń, stanowiących zagrożenie dla zdrowia i życia obywateli.

Zapewnienie przez system realizacji usług, o których mowa w § 3 projektu rozporządzenia następuje poprzez umieszczanie i odbieranie dokumentów elektronicznych w formacie XML w strukturach i formatach umożliwiających komunikację, z wykorzystaniem protokołów komunikacyjnych i szyfrujących.

Dodatkowo w systemie zostaną zapewnione stosowne klasyfikacje i słowniki (ICD-10, TERYT, słownik kodów pocztowych itp.), zapewniające jednolitość i spójność systemu z innymi systemami stanowiącymi części systemu informacji w ochronie zdrowia. W odniesieniu do całego systemu informacji w ochronie zdrowia stosowana będzie zasada maksymalnego wykorzystania słowników, z uwagi na potrzebę ich wykorzystywania do budowy dokumentów strukturalnych w formacie XML.

W celu zapewnienia ochrony danych przetwarzanych w systemie przed ich nieuprawnionym dostępem i ujawnieniem, administrator systemu jest zobowiązany do opracowania, wdrażania, nadzorowania, utrzymywania oraz w uzasadnionych przypadkach modyfikowania systemu zarządzania bezpieczeństwem informacji.

Na SZBI składa się szereg procesów, którym towarzyszą polityki, standardy, procedury, wytyczne itd. Należy pamiętać, że budowanie systemu zarządzania bezpieczeństwem informacji nie polega na jednorazowym wdrożeniu. Wynikiem regularnych przeglądów oraz reakcją na niezgodności lub dezaktualizację powinny być działania modyfikujące podejmowane przez administratora systemu, mające na celu wyeliminowanie wszelkich zidentyfikowanych niezgodności oraz niedoskonałości, a tym samym zapewniające ciągłe ulepszanie SZBI. Zakres modyfikacji SZBI będzie zależny od wyników przeglądu i zmian otoczenia. Na bieżąco weryfikowane będą wszystkie aspekty związane z definiowaniem, osiąganiem i utrzymywaniem poufności, integralności, dostępności, niezaprzeczalności, rozłączalności autentyczności, ciągłości i niezawodności informacji i systemów, w których są one przetwarzane.

Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności poprzez zapewnienie warunków organizacyjno-technicznych umożliwiających realizację następujących działań:

1) zapewnienie odpowiedniego (adekwatnego do charakteru przetwarzanych danych i występujących zagrożeń) poziomu bezpieczeństwa w systemach teleinformatycznych poprzez zapewnienie ochrony przetwarzanych informacji

przed ich kradzieżą, nieuprawnionym dostępem, ujawnieniami, uszkodzeniami lub zakłóceniami;

2) przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowanie działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy;
3) aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia;
4) podjęcie działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji. W przypadku zmiany zadań tych osób powinna nastąpić natychmiastowa zmiana ich uprawnień.

Projekt rozporządzenia nie podlega notyfikacji w rozumieniu rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. Nr 239, poz. 2039 oraz z 2004 r. Nr 65, poz. 597).

Projekt nie jest objęty prawem Unii Europejskiej.

Ocena Skutków Regulacji

1. Podmioty, na które oddziałuje projektowane rozporządzenie

Projekt oddziałuje na podmioty związane z usługami ochrony zdrowia. W szczególności w zakresie oddzialywania Systemu Monitorowania Zagrożeń, są to podmioty prowadzące rejestry zachorowań na choroby zakaźne i dodatnich wyników badań laboratoryjnych, podmioty prowadzące rejestry niepożądanych odczynów poszczepiennych, pracownicy medyczni pracujący w ramach monitorowania zagrożeń, służby sanitarne i podmioty związane z rejestracją leków, Prezesa Urzędu Rejestracji Produktów Leczniczych, Wyrobów Medycznych i Produktów Biobójczych oraz Ministra Zdrowia.

2. Konsultacje społeczne

Projekt został przesłany do zaopiniowania: Naczelnej Radzie Lekarskiej, Naczelnej Radzie Pielęgniarek i Położnych, Naczelnej Radzie Aptekarskiej, Krajowej Radzie Diagnostów Laboratoryjnych, Ogólnopolskiemu Porozumieniu Związków Zawodowych, Sekretariatowi Ochrony Zdrowia Komisji Krajowej NSZZ „Solidarność", Federacji Związków Zawodowych Pracowników Ochrony Zdrowia, Ogólnopolskiemu Związkowi Zawodowemu Lekarzy, Ogólnopolskiemu Związkowi Zawodowemu Pielęgniarek i Położnych, Krajowemu Sekretariatowi Ochrony Zdrowia NSZZ „Solidarność 80", Forum Związków Zawodowych, Unii Metropolii Polskich, Związkowi Powiatów Polskich, Związkowi Miast Polskich, Związkowi Gmin Wiejskich RP, Unii Miasteczek Polskich, Konwentowi Marszałków RP, Federacji Związków Gmin i Powiatów RP, Komisji Wspólnej Rządu i Samorządu Terytorialnego, Polskiemu Towarzystwu Informatycznemu, Polskiej Izbie Informatyki i Telekomunikacji, Polskiemu Towarzystwu Społeczeństwa Informacyjnego, Krajowej Izbie Gospodarczej Elektroniki i Telekomunikacji, Krajowej Izbie Gospodarczej, Polskiej Izbie Komunikacji Elektronicznej, Koalicji na rzecz Rozwoju Społeczeństwa Informacyjnego, PKPP „Lewiatan", Business Centre Club i Generalnemu Inspektorowi Ochrony Danych Osobowych.

Projekt rozporządzenia – stosownie do przepisów ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. Nr 169, poz. 1414, z późn. zm.) – został udostępniony w Biuletynie Informacji Publicznej Ministra Zdrowia oraz – stosownie do postanowień uchwały Nr 49 Rady Ministrów z dnia 19

marca 2002 r. Regulamin pracy Rady Ministrów (M. P. Nr 13, poz. 221, z późn. zm.) - w Biuletynie Informacji Publicznej Rządowego Centrum Legislacji.

3. Wpływ projektu na:

a) sektor finansów publicznych, w tym budżet państwa i budżety jednostek samorządu terytorialnego

Koszty związane z zaprojektowaniem, wytworzeniem i wdrożeniem do eksploatacji systemu zostaną sfinansowane ze środków przeznaczonych na realizację projektu „Elektroniczna Platforma Gromadzenia Analizy i Udostępniania Zasobów Cyfrowych o Zdarzeniach Medycznych"(P1), w zakresie infrastruktury techniczno-systemowej i bazodanowej dostarczanej dla wszystkich elementów systemu P1, w tym także dla systemów dziedzinowych.

Zgodnie z postanowieniami porozumienia o dofinansowanie (porozumienie nr POIG.07.01.00-00-007/09-00 zawarte 22.06.2009 r.) całkowity koszt realizacji Projektu P1 wynosi 712 640 tys. zł. Kwota całkowitych wydatków kwalifikowalnych wynosi 676 840 tys. zł, z czego ze środków europejskich zostanie pokryta kwota 575 314 tys. zł (stanowiąca 85%) oraz z budżetu państwa, z części 46 - Zdrowie, której dysponentem jest minister właściwy do spraw zdrowia - kwota 101 526 tys. zł (stanowiąca 15%). Planuje się, że zaprojektowanie, wytworzenie i wdrożenie oprogramowania związanego z obsługą procesów biznesowych zostanie sfinansowane w 2014 r., w kwocie 4,5 mln zł, z budżetu państwa, z części 46 - Zdrowie, której dysponentem jest minister właściwy do spraw zdrowia w zakresie przewidzianym w projekcie Planu Informatyzacji Państwa na lata 2011-2015. Jako podstawę obliczeń zaprojektowania, wytworzenia i wdrożenia ww. oprogramowania przyjęto identyczny model szacowania jaki został zastosowany do oszacowania projektu P1, w ramach studium wykonalności projektu (w oparciu o metodę COCOMO II). Dla każdego z wykorzystywanych podsystemów oszacowano, jaki procent kosztów całkowitych stanowi wytworzenie samych funkcjonalności biznesowych; niniejsze kwoty przyjęto w dalszym szacowaniu. Następnie ustalono relacje złożoności nowych systemów zwymiarowanych wcześniej przy pomocy modelu. Pozwoliło to następnie przy pomocy prostej proporcjonalności na obliczenie nakładów finansowych wymaganych dla każdej z nich.

Koszty związane z dostosowaniem prowadzonych obecnie przez świadczeniodawców systemów zarządzania bezpieczeństwem informacji do określonego w projektowanym rozporządzeniu SZBI zostaną sfinansowane z budżetów tych podmiotów i zależne będą od aktualnego stanu infrastruktury teleinformacyjnej i polityki bezpieczeństwa konkretnego podmiotu. Należy podkreślić, iż w obecnym stanie prawnym SZBI powinny już obecnie funkcjonować we wszystkich podmiotach przetwarzających informacje podlegające ochronie. Szacunkowe koszty pierwszego audytu wewnętrznego w zakresie bezpieczeństwa informacji nie przekroczą kwoty 50 tys. zł. Koszty roczne kolejnych audytów będą niższe od przedmiotowej kwoty o 15-20 tys. zł w zależności od ilości etatów przeznaczonych dla osób zajmujących się bezpieczeństwem informacji. Obecnie w poszczególnych podmiotach przeznacza się 1-1,5 etatu dla ww. osób.

b) rynek pracy

Projektowane rozporządzenie nie będzie miało wpływu na rynek pracy.

c) konkurencyjność wewnętrzną gospodarki i przedsiębiorczość w tym na funkcjonowanie przedsiębiorstw

Projektowana regulacja nie będzie miała bezpośredniego wpływu na konkurencyjność gospodarki i przedsiębiorczość.

d) na ochronę zdrowia ludności

Projektowana regulacja wpłynie na poprawę efektywności w zakresie zapobiegania skutkom niepożądanych zdarzeń mających wpływ na zdrowie i życie ludzi.

e) sytuację i rozwój regionalny

Projektowane rozporządzenie nie będzie miało wpływu na sytuację i rozwój regionalny.