Projekt, z dnia 13 marca 2012 r.

ROZPORZĄDZENIE
MINISTRA ZDROWIA [1)]

z dnia.....2012 r.

w sprawie Systemu Ewidencji Zasobów Ochrony Zdrowia

Na podstawie art. 24 ust. 5 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 Ewidencji Zasobów Ochrony Zdrowia, zwanego dalej „systemem";
2) warunki organizacyjno – techniczne gromadzenia, przetwarzania i pobierania danych przetwarzanych w systemie;
3) warunki powszechnego udostępniania danych zgromadzonych 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)]);

[1)] Minister Zdrowia kieruje działem administracji rządowej – zdrowie, na podstawie rozporządzenie 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.

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);

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) rejestr medyczny – rejestr w rozumieniu art. 2 pkt 12 ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia, zwanej dalej „ustawą".

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

1) na poziomie usługodawców:

a) pobierania do systemu z rejestrów medycznych danych o usługodawcach w formacie i o strukturze odpowiadającym warunkom technicznym systemu,

b) wyszukiwania określonych usługodawców na terenie wybranego województwa, powiatu, gminy oraz pobierania danych adresowych usługodawcy,

c) wprowadzania danych i informacji dotyczących szczególnych zadań realizowanych przez usługodawcę,

d) wprowadzania i wyszukiwania informacji o wyrobach medycznych w rozumieniu ustawy z dnia 20 maja 2010 r. o wyrobach medycznych (Dz. U. Nr 107, poz. 679 oraz z 2011 r. Nr 102, poz. 586 i Nr 113, poz. 657) o których mowa w art. 17 ust. 2 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej (Dz. U. Nr 112, poz. 654, Nr 149, poz. 887, Nr 174, poz.1039 i Nr 185, poz.1092);

2) na poziomie płatników w rozumieniu art. 2 pkt 9 lit. a ustawy:

a) dokonania identyfikacji płatnika,

b) pobierania danych o zakresie świadczeń opieki zdrowotnej finansowanych przez płatnika,

c) pobierania danych adresowych płatnika;

3) na poziomie podmiotów, sprawujących nadzór i kontrolę nad działalnością usługodawców, oraz płatników w rozumieniu art. 2 pkt 9 lit. a ustawy:

a) identyfikacji podmiotu sprawującego nadzór i kontrolę nad wybranym:
   - usługodawcą,
   - płatnikiem,
b) wymiany danych drogą elektroniczną z podmiotami sprawującymi nadzór i kontrolę nad płatnikiem lub usługodawcą,
c) przesyłania dokumentów elektronicznych do podmiotu sprawującego nadzór i kontrolę nad płatnikiem lub usługodawcą oraz uzyskania potwierdzenia ich przyjęcia.

2. System w ramach funkcjonalności statystycznej zapewnia w szczególności wczytywanie danych z rejestrów medycznych, wprowadzanie ich przez administratora systemu, weryfikację ich poprawności i jakości, agregację danych oraz dostęp do tych danych gromadzonych w systemie.

3. System w zakresie swojej minimalnej funkcjonalności zapewnia bieżącą aktualizację danych , okresowe i automatyczne wykonywanie kopii bezpieczeństwa.

4. System zapewnia rejestrację wszystkich prób logowania do systemu oraz zdefiniowanie zestawu śledzonych czynności wykonywanych przez użytkowników, o których mowa w § 3 ust. 1 pkt 1, 2 i 3.

§ 4. 1. System zapewnia dostęp do danych zgromadzonych w systemie na zasadzie powszechnej dostępności.

2. Dane, o których mowa w ust. 1, są udostępniane na portalu edukacyjno - informacyjnym, o którym mowa w art. 36 ustawy.

§ 5. 1. System gromadzi, przetwarza i udostępnia dane z rejestrów medycznych za pomocą systemu teleinformatycznego Platforma Udostępniania On–Line Usług i Zasobów Cyfrowych Rejestrów Medycznych.

2. 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.

3. Struktury i formaty, o których mowa w ust. 2, 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.

4. Dokumenty elektroniczne, o których mowa w ust. 2, podpisuje się bezpiecznym podpisem elektronicznym, podpisem osobistym albo z wykorzystaniem profilu zaufanego ePUAP.

5. Wzory dokumentów elektronicznych, o których mowa w ust. 2, są przechowywane 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.

6. 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.** 1. 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, są zabezpieczane i przechowywane 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. Przepisy dotyczące podpisu osobistego stosuje się od dnia 1 lipca 2013 r.

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

MINISTER ZDROWIA

Za zgodność pod względem prawnym i redakcyjnym
DYREKTOR
Departamentu Prawnego
Radca prawny

UZASADNIENIE

Projekt rozporządzenia stanowi wykonanie upoważnienia określonego w art. 24 ust. 5 ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz. U. Nr 113, poz. 657 i Nr 174, poz. 1039), zwanej dalej „ustawą".

System Ewidencji Zasobów Ochrony Zdrowia 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.

W obecnym stanie prawnym funkcjonuje kilka różnych rejestrów obejmujących podmioty biorące udział w procesie udzielania świadczeń opieki zdrowotnej. Podmioty sprawujące nadzór i kontrolę nad ich działalnością nie są w ogóle ewidencjonowane lub są ewidencjonowane w sposób szczątkowy.

System ma na celu gromadzenie i przetwarzanie danych dotyczących podmiotów udzielających świadczeń opieki zdrowotnej (usługodawców) oraz podmiotów sprawujących nadzór i kontrolę nad ich działalnością we wszystkich aspektach prowadzonej działalności, a także płatników. Obecnie dane dotyczące usługodawców są gromadzone w rejestrach medycznych prowadzonych przez podmioty odpowiedzialne za ich prowadzenie na podstawie odrębnych przepisów.

Obecnie zbiory danych dotyczące usługodawców są prowadzone przez:

1) wojewodę właściwego dla siedziby albo miejsca zamieszkania podmiotu leczniczego - w odniesieniu do podmiotów leczniczych na podstawie ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej (Dz. U. Nr 112, poz. 654, z późn. zm.);
2) wojewodów i Ministra Zdrowia na podstawie przepisów ustawy z dnia 8 września 2006 r. o Państwowym Ratownictwie Medycznym (Dz. U. Nr 191, poz. 1410, z późn. zm.);
3) Naczelną Radę Lekarską na podstawie przepisów ustawy z dnia 2 grudnia 2009 r. o izbach lekarskich (Dz. U. Nr 219, poz. 1708, z późn. zm.) w odniesieniu do Centralnego Rejestru Lekarzy i Lekarzy Dentystów Rzeczypospolitej Polskiej;

4) Okręgowe rady lekarskie i Wojskową Radę Lekarską na podstawie przepisów ustawy z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty (Dz. U. z 2011 r. Nr 227, poz. 1634, z późn. zm.) w odniesieniu do indywidualnych praktyk zawodowych lekarzy i lekarzy dentystów;

5) Naczelną Radę Pielęgniarek i Położnych na podstawie przepisów ustawy z dnia 1 lipca 2011 r. o samorządzie pielęgniarek i położnych (Dz. U. z 2011 r. Nr 174, poz. 1038) w odniesieniu do Centralnego Rejestru Pielęgniarek i Położnych;

6) Okręgowe rady pielęgniarek i położnych na podstawie przepisów ustawy z dnia 1 lipca 2011 r. o samorządzie pielęgniarek i położnych w odniesieniu do rejestru obywateli państw członkowskich Unii Europejskiej wykonujących na terenie tej izby czasowo i okazjonalnie zawód pielęgniarki, położnej;

7) Okręgowe rady pielęgniarek i położnych na podstawie przepisów ustawy z dnia 15 lipca 2011 r. o zawodach pielęgniarek i położnych (Dz. U. z 2011 r. Nr 174, poz. 1039 i Nr 291, poz. 1707) w odniesieniu do praktyk zawodowych pielęgniarek i położnych;

8) wojewódzkich inspektorów farmaceutycznych na podstawie przepisów ustawy z dnia 6 września 2001 r. - Prawo farmaceutyczne (Dz. U. z 2008 r. Nr 45, poz. 271, z późn. zm.) w odniesieniu do aptek ogólnodostępnych, punktów aptecznych oraz aptek szpitalnych i zakładowych;

9) Krajową Radę Diagnostów Laboratoryjnych na podstawie przepisów ustawy z dnia 27 lipca 2001 r. o diagnostyce laboratoryjnej (Dz. U. z 2004 r. Nr 144, poz. 1529, z późn. zm.) w odniesieniu do danych objętych ewidencją laboratoriów.

Nie istnieje natomiast wspólna baza danych dotycząca zarówno usługodawców, płatników oraz podmiotów sprawujących nadzór i kontrolę nad działalnością usługodawców i płatników. Znamienną cechą tego stanu rzeczy jest brak otwartości i interoperacyjności poszczególnych rejestrów, co uniemożliwia wymianę danych pomiędzy poszczególnymi rejestrami i scalanie ich w jedną bazę danych.

W zakresie przepisów dotyczących określenia minimalnej funkcjonalności systemu przyjęto podział w oparciu o usługi dedykowane dla usługodawców, płatników oraz podmiotów sprawujących nadzór i kontrolę nad działalnością usługodawców oraz płatników. Wśród usług wymieniono m. in. pobieranie do systemu z rejestrów

medycznych danych o usługodawcach w formacie i strukturze odpowiadającym warunkom technicznym systemu, jak również dokonywanie identyfikacji właściwych podmiotów wraz z pobieraniem i przesyłaniem danych (np. adresowych usługodawców).

W celu umożliwienia powszechnego dostępu do danych zgromadzonych w systemie, umożliwiono prezentację informacji zawartych w systemie za pośrednictwem portalu edukacyjno – informacyjnego, o którym mowa w art. 36 ustawy.

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 jest realizowane 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 prowadzące bazy danych z zakresu ochrony zdrowia.

Ponadto projekt oddziałuje na wytwórców systemów teleinformatycznych i na podmioty prowadzące rejestry medyczne.

Dotyczy to w szczególności:

1) usługobiorców;

2) usługodawców;

3) płatników w rozumieniu art. 2 pkt 9 lit. a ustawy;

4) podmiotów sprawujących nadzór i kontrolę nad działalnością usługodawców i płatników.

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.

Wyniki konsultacji społecznych zostaną omówione po ich zakończeniu.

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 3,4 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. Oznacza to konieczność zwiększenia budżetu państwa w części 46 – Zdrowie w 2014 roku o wyżej wymienioną kwotę. 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

Przepisy projektu rozporządzenia nie będą miały wpływu na rynek pracy.

c) konkurencyjność gospodarki i przedsiębiorczość w tym na funkcjonowanie przedsiębiorstw

Projektowana regulacja nie będzie miała bezpośredniego wpływu na konkurencyjność gospodarki i przedsiębiorczość, pośrednio natomiast wpłynie na funkcjonowanie przedsiębiorstw, m.in. poprzez pobudzenie konkurencyjności wewnętrznej w obszarze ochrony zdrowia.

d) na ochronę zdrowia ludności

Projekt zakłada usprawnienie przepływu informacji pomiędzy podmiotami, na które regulacja ma wpływ, co z kolei doprowadzi do zapewnienia niemalże w czasie rzeczywistym dostępu do danych o stanie zdrowia leczonego.

e) na sytuację i rozwój regionalny

Projektowana regulacja nie będzie miała wpływu na sytuację i rozwój regionalny.