

**ROZPORZĄDZENIE
MINISTRA ZDROWIA ¹⁾**

z dnia2012 r.

w sprawie Systemu Statystyki w Ochronie Zdrowia

Na podstawie art. 23 ust. 4 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 Statystyki w Ochronie Zdrowia, zwanego dalej „systemem”;
- 2) warunki organizacyjno-techniczne gromadzenia i pobierania danych przetwarzanych w systemie.

§2. 1. System w zakresie swojej minimalnej funkcjonalności udostępnia usługi związane z tworzeniem statystyk, analiz, raportów i sprawozdań na podstawie gromadzonych danych.

2. Minimalna funkcjonalność systemu zapewnia następujące usługi:

- 1) dostęp do aktualnych wzorów formularzy statystycznych;
- 2) automatyczne pobieranie danych lub ich ręczne wprowadzanie;
- 3) walidację danych;
- 4) wizualizację wypełnionych formularzy statystycznych;
- 5) bieżące zapisywanie formularzy statystycznych;
- 6) archiwizację prowadzonych formularzy statystycznych;
- 7) przygotowywanie i wysyłanie raportów;
- 8) odbieranie formularzy statystycznych;
- 9) weryfikację formularzy statystycznych;

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).

10) tworzenie zbiorów danych ze zgromadzonych danych statystycznych, a następnie dokonywanie na podstawie tych zbiorów obliczeń, opracowań i analiz.

§ 3. 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.

§ 4. Przekazywanie danych do systemu odbywa się drogą elektroniczną w rozumieniu ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. Nr 144, poz. 1204, z późn. zm.²⁾).

§ 5. 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

²⁾ Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2004 r. Nr 96, poz. 959 i Nr 173, poz. 1808, z 2007 r. Nr 50, poz. 331, z 2008 r. Nr 171, poz. 1056 i Nr 216, poz. 1371, z 2009 r. Nr 201, poz. 1540 oraz z 2011 r. Nr 85, poz. 459 i Nr 134, poz. 779.

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.

§ 6. 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.

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

MINISTER ZDROWIA

W porozumieniu:

MINISTER ADMINISTRACJI I CYFRYZACJI

www.inforlex.pl

**Za zgodność pod względem
prawnym i redakcyjnym**

DYREKTOR
Departamentu Prawnego

Władysław Puzon
radca prawny

3

UZASADNIENIE

Projekt rozporządzenia, zwany dalej „projektem”, stanowi wykonanie upoważnienia określonego w art. 23 ust. 4 ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz. U. Nr 113, poz. 657, z późn. zm.), zwanej dalej „ustawą”.

Projekt określa minimalną funkcjonalność oraz warunki organizacyjno-techniczne gromadzenia i pobierania danych przetwarzanych w Systemie Statystyki w Ochronie Zdrowia, zwanym dalej „systemem”, uwzględniając konieczność zapewnienia sprawnego przekazywania danych do systemu w postaci elektronicznej oraz umożliwienia powszechnej dostępności danych zgromadzonych w systemie, przy zachowaniu odpowiedniego poziomu bezpieczeństwa.

System 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 informacyjnego ochrony zdrowia.

System opisany w art. 23 ustawy jest systemem gromadzącym, przetwarzającym i udostępniającym dane statystyczne, zarówno w obszarze określonym przepisami wydanymi na podstawie ustawy z dnia 29 czerwca 1995 r. o statystyce publicznej (Dz. U. Nr 88, poz. 439, z późn. zm.), jak również dane gromadzone w systemach teleinformatycznych obsługujących system informacji w ochronie zdrowia, co pozwoli na analizę wskaźników i zjawisk zachodzących w ochronie zdrowia bez zwiększania obowiązków statystycznych po stronie usługodawców.

System umożliwi realizację zadań wspierających procesy decyzyjne w ochronie zdrowia, w szczególności:

- 1) tworzenie statystyk, analiz, raportów i sprawozdań na podstawie wybranych danych według określonego kryterium, dla potrzeb prowadzonych projektów naukowych i sektorowych strategii branżowych;
- 2) planowanie opieki zdrowotnej – poprzez umożliwienie analiz danych o zdarzeniach medycznych, w tym analiz wykorzystujących zaawansowane metody statystyczne, takie jak: analiza predykcyjna, wykrywanie wzorców, analiza szeregów czasowych, analiza trendu, analiza koszykowa oraz bieżących analiz i raportów;
- 3) wspomaganie zarządzania kryzysowego – poprzez dostarczenie informacji umożliwiającej bieżące monitorowanie i reagowanie na zagrożenia o charakterze epidemiologicznym itp.;

- 4) monitorowanie zachorowalności i chorobowości;
- 5) monitorowanie obrotu lekami i wspomaganie zarządzania gospodarką lekami;
- 6) eksplorację danych gromadzonych w SIM;
- 7) monitorowanie liczby specjalistów medycznych.

Minimalna funkcjonalność systemu umożliwi udostępnianie usług związanych z tworzeniem statystyk, analiz, raportów i sprawozdań na podstawie gromadzonych danych.

W zakresie warunków organizacyjno – technicznych gromadzenia i udostępniania danych w systemie przyjęto, że system musi być zgodny z pełnym katalogiem norm stosowanych do zapewnienia wymiany i bezpieczeństwa danych i informacji w ochronie zdrowia.

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) zapewnienie aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia;
- 3) przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowanie działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy;
- 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 rozporządzenie:

Projekt oddziałuje na:

- 1) ministra właściwego do spraw zdrowia;
- 2) jednostkę podległą ministrowi właściwemu do spraw zdrowia właściwą w zakresie systemów informacyjnych ochrony zdrowia;
- 3) służby statystyki publicznej;
- 4) podmioty wykonujące działalność leczniczą.

Ponadto projekt oddziałuje na podmioty prowadzące bazy danych z zakresu ochrony zdrowia w tym podmioty prowadzące rejestry medyczne.

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, Krajowemu Centrum Bankowania Tkanek i Komórek, Centrum Organizacyjno – Koordynacyjnemu ds. Transplantacji Poltransplant, Zakładowi Epidemiologii i Prewencji Nowotworów Centrum Onkologii 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 lobbingskiej 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 15,1 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

Przepisy rozporządzenia nie będą miały bezpośredniego 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.

d) na ochronę zdrowia ludności

Regulacja umożliwi wsparcie kluczowych procesów decyzyjnych kreatora polityki zdrowotnej państwa, mających na celu poprawę bezpieczeństwa zdrowotnego obywateli oraz wzrost świadomości społecznej na temat systemu ochrony zdrowia.

e) sytuację i rozwój regionalny

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