



MINISTER ZDROWIA

MZ-OZZ-0212-26903-31/MKU/12

P. J. Delawski

Warszawa, 2012-05-30
POLSKA KONFEDERACJA
PRACODAWCÓW PRYWATNYCH
LEWIATAN
04.05.2012
WPŁYNEŁO
Lp.dz.

Wg rozdzielnika

Stosownie do postanowień § 12 ust. 1 uchwały nr 49 Rady Ministrów z dnia 19 marca 2002 r. Regulamin pracy Rady Ministrów (M.P. Nr 13, poz. 221, z późn. zm.), przesyłam w załączeniu projekt *rozporządzenia Ministra Zdrowia w sprawie wymagań dla Systemu Informacji Medycznej* z uprzejmą prośbą o zgłoszenie ewentualnych uwag w terminie do dnia **17 maja 2012 r.**

Proszę o przesłanie uwag także w postaci elektronicznej na adres SIOZ@mz.gov.pl w formacie edytowalnym (doc).

Jednocześnie informuję, że projekt rozporządzenia jest dostępny na stronie internetowej Ministerstwa Zdrowia:

www.mz.gov.pl/wwwmz/index?ma=19814

Z upoważnienia
MINISTRA ZDROWIA
SEKRETARZ STANU

Jakub Szulc

Otrzymują:

1. Minister – Członek Rady Ministrów, Szef Kancelarii Prezesa Rady Ministrów, Przewodniczący Komitetu Stałego Rady Ministrów
2. Wiceprezes Rady Ministrów – Minister Gospodarki
3. Prezes Rządowego Centrum Legislacji (2 egz.)
4. Minister Edukacji Narodowej
5. Minister Finansów
6. Minister Pracy i Polityki Społecznej
7. Minister Transportu, Budownictwa i Gospodarki Morskiej
8. Minister Kultury i Dziedzictwa Narodowego
9. Minister Obrony Narodowej
10. Minister Nauki i Szkolnictwa Wyższego
11. Minister Rolnictwa i Rozwoju Wsi
12. Minister Skarbu Państwa
13. Minister Sprawiedliwości

14. Minister Spraw Wewnętrznych
15. Minister Administracji i Cyfryzacji
16. Minister Spraw Zagranicznych
17. Minister Środowiska
18. Minister Rozwoju Regionalnego
19. Minister Sportu i Turystyki
20. Przewodniczący Komitetu do Spraw Europejskich
21. Szef Agencji Bezpieczeństwa Wewnętrznego
22. Szef Agencji Wywiadu
23. Główny Inspektor Sanitarny
24. Główny Inspektor Farmaceutyczny
25. Prezes Urzędu Ochrony Konkurencji i Konsumentów
26. Prezes Narodowego Funduszu Zdrowia
27. Rzecznik Praw Pacjenta
28. Naczelna Rada Lekarska
29. Naczelna Rada Pielęgniarek i Położnych
30. Naczelna Rada Aptekarska
31. Krajowa Rada Diagnostów Laboratoryjnych
32. Ogólnopolskie Porozumienie Związków Zawodowych
33. Sekretariat Ochrony Zdrowia Komisji Krajowej NSZZ „Solidarność”
34. Ogólnopolski Związek Zawodowy Lekarzy
35. Ogólnopolski Związek Zawodowy Pielęgniarek i Położnych
36. Ogólnopolski Związek Zawodowy Położnych
37. Ogólnopolski Związek Zawodowy Techników Medycznych Radioterapii
38. Ogólnopolski Związek Zawodowy Techników Medycznych „Medyk”
39. Ogólnopolski Związek Zawodowy Techników Medycznych Elektroradiologii
40. Związek Zawodowy Anestezjologów
41. Związek Zawodowy Neonatologów
42. Porozumienie Zielonogórskie – Federacja Związków Pracodawców Ochrony Zdrowia
43. Porozumienie Pracodawców Ochrony Zdrowia
44. Krajowy Sekretariat Ochrony Zdrowia NSZZ „Solidarność 80”
45. Forum Związków Zawodowych
46. Federacja Związków Pracodawców Zakładów Opieki Zdrowotnej
47. Federacja Związków Zawodowych Pracowników Ochrony Zdrowia
48. Prezes Urzędu Zamówień Publicznych
49. Rada Krajowa Federacji Konsumentów
50. Fundacja Stefana Batorego
51. Polska Konfederacja Pracodawców Prywatnych Lewiatan
52. Związek Pracodawców Niepublicznej Opieki Zdrowotnej
53. Związek Pracodawców Ratownictwa Medycznego Samodzielnych Publicznych Zakładów Opieki Zdrowotnej
54. Polskie Stowarzyszenie Dyrektorów Szpitali
55. Stowarzyszenie Menadżerów Opieki Zdrowotnej STOMOZ
56. Prezes Zakładu Ubezpieczeń Społecznych
57. Prezes Kasy Rolniczego Ubezpieczenia Społecznego
58. Państwowy Fundusz Rehabilitacji Osób Niepełnosprawnych
59. Narodowy Instytut Zdrowia Publicznego
60. Pracodawcy Rzeczypospolitej Polskiej
61. Business Centre Club - Związek Pracodawców
62. Ogólnopolskie Stowarzyszenie Szpitali Niepublicznych

63. Zarząd Główny Związku Zawodowego Techników Farmaceutycznych RP
64. Główny Urząd Statystyczny
65. Generalny Inspektor Ochrony Danych Osobowych
66. Agencja Oceny Technologii Medycznych w Warszawie
67. Centrum Monitorowania Jakości w Ochronie Zdrowia w Krakowie
68. Unia Metropolii Polskich
69. Unia Miasteczek Polskich
70. Unia Uzdrawisk Polskich
71. Związek Powiatów Polskich
72. Związek Miast Polskich
73. Związek Gmin Wiejskich RP
74. Federacja Związków Gmin i Powiatów RP
75. Komisja Wspólna Rządu i Samorządu Terytorialnego
76. Koalicja na Rzecz Pacjentów „Mam prawo do Zdrowia”
77. Konwent Marszałków RP
78. Instytut Praw Pacjenta i Edukacji Zdrowotnej
79. Federacja Pacjentów Polskich
80. Polska Izba Ubezpieczeń
81. Polskie Towarzystwo Informatyczne
82. Polska Izba Informatyki i Telekomunikacji
83. Polska Izba Komunikacji Elektronicznej
84. Polskie Towarzystwo Społeczeństwa Informacyjnego
85. Krajowa Izba Gospodarcza
86. Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji
87. Koalicja na Rzecz Rozwoju Społeczeństwa Informacyjnego

Do wiadomości:

1. Pan Bartosz Arłukowicz – Minister Zdrowia
2. Pan Jakub Szulc – Sekretarz Stanu
3. Pani Agnieszka Pachciarz - Podsekretarz Stanu
4. Pan Marek Haber - Podsekretarz Stanu
5. Pan Cezary Rzemek - Podsekretarz Stanu
6. Pan Aleksander Sopliński – Podsekretarz Stanu

**ROZPORZĄDZENIE
MINISTRA ZDROWIA¹⁾**
z dnia2012 r.

w sprawie wymagań dla Systemu Informacji Medycznej

Na podstawie art. 13 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:

Rozdział 1
Przepisy ogólne

§ 1. Rozporządzenie określa:

- 1) format elektronicznej dokumentacji medycznej udostępnianej przez usługodawców w Systemie Informacji Medycznej, zwanym dalej „SIM”, warunki organizacyjno-techniczne jej przetwarzania, udostępniania, autoryzacji oraz zabezpieczenia przed utratą;
- 2) warunki organizacyjno-techniczne zamieszczania i pobierania z SIM dokumentów elektronicznych niezbędnych do prowadzenia diagnostyki, ciągłości leczenia oraz zaopatrzenia usługobiorców w produkty lecznicze i wyroby medyczne, zgodnie z zakresem zadań wykonywanych przez usługodawców;
- 3) warunki organizacyjno-techniczne realizacji dostępu i pobierania danych przetwarzanych w SIM.

§ 2. Użyte w rozporządzeniu określenia 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. zm²⁾);
- 2) centralne repozytorium wzorów dokumentów elektronicznych – miejsce, o którym mowa w art. 19b ust. 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji

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.

działalności podmiotów realizujących zadania publiczne (Dz. U. Nr 64 poz. 565, z późn. zm³⁾);

- 3) elektroniczny dokument SIM – elektroniczny dokument zawierający dane identyfikacyjne usługobiorcy, informacje dotyczące usług medycznych oraz informacje o elektronicznej dokumentacji medycznej związanej z usługami medycznymi, przetwarzany w systemie informatycznym usługodawcy i przekazywany do SIM;
- 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.

Rozdział 2

Format elektronicznej dokumentacji medycznej oraz warunki organizacyjno – techniczne jej przetwarzania, autoryzacji i zabezpieczenia

§ 3. 1. Elektroniczna dokumentacja medyczna udostępniana przez usługodawców w SIM zawiera:

- 1) dokumenty elektroniczne w formacie XML, których zakres odpowiada danym gromadzonym w dokumentacji medycznej określonym przepisami ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz. U. z 2012 r. poz. 159);
- 2) pliki multimedialne będące wynikiem diagnostyki obrazowej.

2. Elektroniczna dokumentacja medyczna jest udostępniana w SIM w formacie XML oraz w zakresie wymiany i interpretacji danych medycznych związanych z diagnostyką obrazową w standardzie DICOM.

3. Administrator SIM określa strukturę logiczną elektronicznej dokumentacji medycznej udostępnianej przez usługodawców w SIM.

4. Struktura logiczna elektronicznej dokumentacji medycznej, o której mowa w ust. 3, umieszczana jest w centralnym repozytorium wzorów dokumentów elektronicznych, na

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.

portalu edukacyjno - informacyjnym, o którym mowa w art. 36 ustawy oraz w Biuletynie Informacji Publicznej ministra właściwego do spraw zdrowia.

5. Elektroniczna dokumentacja medyczna udostępniana przez usługodawców w SIM jest zbudowana w formie hierarchicznych struktur danych w odniesieniu do wszystkich rodzajów zdarzeń medycznych i plików multimedialnych będących wynikiem diagnostyki obrazowej.

§ 4. 1. Udostępnianie elektronicznej dokumentacji medycznej odbywa się w sposób umożliwiający identyfikację i autoryzację uprawnionych osób przy użyciu bezpiecznego podpisu elektronicznego albo danymi potwierdzonymi profilem zaufanym ePUAP.

2. Udostępnianie uprawnionym podmiotom elektronicznej dokumentacji medycznej następuje przez elektroniczną transmisję danych w formie komunikatów.

3. Komunikaty, o których mowa w ust. 2, są zgodne ze wzorcami struktury logicznej elektronicznych komunikatów opisanych za pomocą formatu XML/XSD i standardu wymiany i interpretacji danych medycznych związanych z diagnostyką obrazową DICOM.

4. Udostępnianie elektronicznej dokumentacji medycznej odbywa się w trybie świadczenia usługi drogą elektroniczną w rozumieniu przepisów ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. Nr 144, poz. 1204, z późn. zm⁴⁾).

§ 5. 1. Proces przygotowania i przesyłania komunikatów, o których mowa w § 4 ust. 2, obejmuje:

- 1) przesłanie przez zamawiającego do SIM zapotrzebowania na elektroniczną dokumentację medyczną;
- 2) przyjęcie przez SIM elektronicznego zapotrzebowania na elektroniczną dokumentację medyczną;
- 3) weryfikację uprawnień zamawiającego;
- 4) w przypadku pozytywnej weryfikacji uprawnień zamawiającego, przesłanie przez SIM zapotrzebowania na elektroniczną dokumentację medyczną do usługodawcy, do którego skierowano zapotrzebowanie;
- 5) przygotowanie treści komunikatu przez pracownika medycznego usługodawcy udostępniającego elektroniczną dokumentację medyczną;

⁴⁾ 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.

- 6) podpisanie przez pracownika medycznego usługodawcy udostępniającego elektroniczną dokumentację medyczną komunikatu przy użyciu bezpiecznego podpisu elektronicznego albo danymi potwierdzonymi profilem zaufanym ePUAP;
- 7) wysłanie do zamawiającego komunikatu przez usługodawcę udostępniającego elektroniczną dokumentację medyczną;
- 8) odebranie przez zamawiającego komunikatu;
- 9) potwierdzenie odebrania komunikatu przez zamawiającego w SIM i w systemie teleinformatycznym usługodawcy udostępniającego elektroniczną dokumentację medyczną.

2. Zamawiającym, o którym mowa w ust. 1, może być uprawniony usługodawca, pracownik medyczny oraz usługobiorca.

§ 6. 1. W przypadku zakończenia działalności przez podmiot wykonujący działalność leczniczą, w rozumieniu 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), elektroniczna dokumentacja medyczna przekazywana jest do SIM.

2. Jeżeli zadania podmiotu, o którym mowa w ust. 1, przejmuje inny podmiot, podmiot ten przejmuje elektroniczną dokumentację medyczną.

3. Elektroniczna dokumentacja medyczna, o której mowa w ust. 1, udostępniana jest przez SIM uprawnionym podmiotom w sposób określony w § 4.

§ 7. Ochrona danych zawartych w elektronicznej dokumentacji medycznej udostępnianej w SIM polega w szczególności na:

- 1) odmowie dostępu do danych w przypadku braku lub niepełnej identyfikacji zamawiającego, o którym mowa w § 5 ust. 2;
- 2) odmowie dostępu do danych w sytuacji braku zgody usługobiorcy na ich udostępnienie, z zastrzeżeniem art. 35 ust. 4 ustawy;
- 3) zastosowaniu środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną;
- 4) zabezpieczeniu danych przed ich udostępnieniem osobom nieupoważnionym, przed nieuprawnioną zmianą oraz utratą, uszkodzeniem lub zniszczeniem tych danych;

5) zachowaniu integralności i wiarygodności danych.

Rozdział 3

Realizacja dostępu i pobierania danych przetwarzanych w SIM oraz warunki organizacyjno - techniczne zamieszczania i pobierania z SIM dokumentów elektronicznych niezbędnych do prowadzenia diagnostyki, ciągłości leczenia oraz zaopatrzenia usługobiorców w produkty lecznicze i wyroby medyczne

§ 8. 1. Usługodawcy przetwarzają elektroniczne dokumenty SIM w zakresie danych, o których mowa w art. 10 ust. 2 ustawy.

2. Przesyłanie elektronicznych dokumentów SIM polega na:

- 1) opracowaniu treści komunikatu zawierającego elektroniczne dokumenty SIM przez podmiot zobowiązany do przekazywania informacji do SIM;
- 2) podpisaniu komunikatu, o którym mowa w pkt 1, przy użyciu bezpiecznego podpisu elektronicznego albo danymi potwierdzonymi profilem zaufanym ePUAP;
- 3) wysłaniu komunikatu, o którym mowa w pkt 1, przez podmiot zobowiązany do przekazywania informacji do SIM;
- 4) odebraniu komunikatu, o którym mowa w pkt 1, weryfikację prawidłowości i wysłanie potwierdzenia jego otrzymania lub wykazu stwierdzonych w nim błędów lub braków do podmiotów zobowiązanych do przekazywania informacji do SIM.

3. Struktury logiczne komunikatu, o którym mowa w ust. 2, zawierającego elektroniczne dokumenty SIM w formacie XML/XSD oraz zasady weryfikacji komunikatów, umieszczone 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.

4. Komunikat, o którym mowa w ust. 2, przekazywany jest do SIM przez usługodawców na bieżąco, co najmniej raz dziennie.

5. W zakresie danych, o których mowa w art. 14 ust. 4 ustawy, przekazywanie komunikatu, o którym mowa w ust. 2, dokonuje się na bieżąco, co najmniej raz dziennie.

6. Komunikat, o którym mowa w ust. 2, jest gromadzony i przetwarzany przez SIM oraz udostępniany:

- 1) usługobiorcom;
- 2) usługodawcom i pracownikom medycznym, w zakresie wykonywanych przez nich zadań i posiadanych uprawnień;
- 3) płatnikom;
- 4) podmiotom, o których mowa w art. 12 ust. 5 i ust. 7-8 ustawy.

§ 9. SIM w zakresie warunków organizacyjno – technicznych zamieszczania w nim dokumentów elektronicznych niezbędnych do prowadzenia diagnostyki, ciągłości leczenia oraz zaopatrzenia usługobiorców w produkty lecznicze i wyroby medyczne i ich pobierania z SIM, zgodnie z zakresem zadań wykonywanych przez usługodawców oraz warunków organizacyjno – technicznych realizacji dostępu i pobierania danych przetwarzanych w SIM zapewnia zgodność z normami, których przedmiotem są zasady gromadzenia i wymiany informacji w ochronie zdrowia:

- 1) PN-EN 13606-1:2009 Informatyka w ochronie zdrowia - Przesyłanie elektronicznych dokumentacji zdrowotnej - Część 1: Model referencyjny,
- 2) PN-EN 13606-4:2009 Informatyka w ochronie zdrowia - Przesyłanie elektronicznych dokumentów zdrowotnych - Część 4: Bezpieczeństwo,
- 3) PN-EN ISO 13606-5:2010 Informatyka w ochronie zdrowia - Przesyłanie elektronicznej dokumentacji zdrowotnej - Część 5: Specyfikacja interfejsu,
- 4) ISO 18308:2011 Informatyka w ochronie zdrowia - Wymagania dla architektury elektronicznej dokumentacji medycznej,
- 5) PN-ENV 13608-1:2003 (U) Informatyka w ochronie zdrowia - Bezpieczeństwo przesyłanych danych w opiece zdrowotnej - Część 1: Pojęcia i terminologia,
- 6) PN-ENV 13608-2:2003 (U) Informatyka w ochronie zdrowia - Bezpieczeństwo przesyłanych danych w opiece zdrowotnej - Część 2: Bezpieczne obiekty danych,
- 7) PN-ENV 13608-3:2003 (U) Informatyka w ochronie zdrowia - Bezpieczeństwo przesyłania danych w opiece zdrowotnej - Część 3: Bezpieczne kanały przesyłania danych,
- 8) ISO/TS 22600-1:2006 Informatyka w ochronie zdrowia – Zarządzanie przywilejami i kontrola dostępu – Część 1: Ogólny opis i polityka zarządzania,
- 9) ISO/TS 22600-2:2006 Informatyka w ochronie zdrowia – Zarządzanie przywilejami i kontrola dostępu – Część 2: Modele formalne,

- 10) ISO/TS 22600-3:2009 Informatyka w ochronie zdrowia Zarządzanie przywilejami i kontrola dostępu – Część 3: Wdrożenia,
 - 11) Inicjatywa Zarządzania Procesami Biznesowymi: Notacja Modelowania Procesów Biznesowych, wersja 1.0. Maj 2004,
 - 12) Koalicja na rzecz Zarządzania Przepływu Pracy: Interfejs Wymiany Definicji Procesów Przepływu Pracy - XML Język Definicji Procesów, WfMC-TC-1025, wersja 1.0, Październik 2002
- albo normami i wersjami je zastępującymi.

Rozdział 4

Ochrona danych przetwarzanych w SIM

§ 10. Minimalne wymagania dla SIM związane z bezpieczeństwem przetwarzania i udostępniania danych w postaci elektronicznej uwzględniają:

- 1) dostęp usługobiorcy do informacji podlegających ochronie prawnej, przechowywanych w SIM;
- 2) wdrożenie mechanizmów umożliwiających audyt wymiany danych związanych z elektronicznym dokumentem SIM;
- 3) uwierzytelnianie i identyfikację podmiotów podejmujących próby dostępu do elektronicznego dokumentu SIM do danych przetwarzanych i udostępnianych w SIM;
- 4) wdrożenie mechanizmów pozyskiwania, rejestracji i śledzenia stanu zgody wyrażonej przez usługobiorcę na dostęp do całości lub części danych przetwarzanych w SIM, z uwzględnieniem celu pozyskania dostępu do tych danych;
- 5) określanie, modyfikację i odwoływanie praw dostępu do całości lub części danych przetwarzanych w SIM.

§ 11. Dane przetwarzane w SIM i dane zawarte w elektronicznej dokumentacji medycznej podlegają ochronie na poziomie wysokim, o którym mowa w przepisach wydanych na

podstawie art. 39a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.⁵⁾).

§ 12. 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”, zgodnie z wymaganiami normy „PN-ISO/IEC 27001:2007 Technika informatyczna - Techniki bezpieczeństwa -Systemy zarządzania bezpieczeństwem informacji – Wymagania” albo normą lub wersją ją zastępującą.

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, przeprowadza nie rzadziej niż raz do roku audyt SZBI, w celu kontroli stopnia przestrzegania wymagań SZBI.

4. Audyt SZBI jest prowadzony przez audytora wewnętrznego.

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

§ 13. 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 oraz do informacji przetwarzanych przez ten system;
- 3) dobór, szkolenie i sprawdzanie personelu obsługującego system;
- 4) zabezpieczenie fizyczne obiektów i urządzeń systemu;

⁵⁾ Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2002 r. Nr 153, poz. 1271, z 2004 r. Nr 25, poz. 219 i Nr 33, poz. 285, z 2006 r. Nr 104, poz. 708 i 711, z 2007 r. Nr 165, poz. 1170 i Nr 176, poz. 1238, z 2010 r. Nr 41, poz. 233, Nr 182, poz. 1228 i Nr 229, poz. 1497 oraz z 2011 r. Nr 230, poz. 1371.

- 5) opracowywanie i utrzymywanie systemu z uwzględnieniem wymogów bezpieczeństwa i stosowaniem kryptograficznej ochrony danych zwłaszcza w czasie transmisji;
- 6) zarządzanie ciągłością działania systemu, zwłaszcza w warunkach wystąpienia naruszenia bezpieczeństwa informacji albo zagrożenia jego wystąpienia.

§ 14. Przekazanie systemu do eksploatacji administratorowi systemu SIM 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.

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

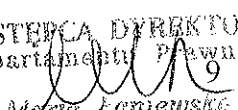
MINISTER ZDROWIA

W porozumieniu:

MINISTER ADMINISTRACJI I CYFRYZACJI


ZASTĘPCA DYREKTORA
Departamentu Organizacji Ochrony
Zdrowia
Marcin Kędziński

**Za zgodność pod względem
prawnym i redakcyjnym**


ZASTĘPCA DYREKTORA
Departamentu Prawnego
Maria Łoniewska
radca prawny
60.04.10v

UZASADNIENIE

Projekt rozporządzenia, zwany dalej „projektem”, stanowi wykonanie upoważnienia określonego w art. 13 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”.

W obecnym stanie prawnym kwestie związane ze sposobem prowadzenia dokumentacji medycznej, w tym elektronicznej dokumentacji medycznej, zostały uregulowane w rozporządzeniu Ministra Zdrowia z dnia 21 grudnia 2010 r. w sprawie rodzajów i zakresu dokumentacji medycznej oraz sposobu jej przetwarzania (Dz. U. Nr 252, poz. 1697).

Zakładana w ustawie powszechność prowadzenia dokumentacji medycznej w postaci elektronicznej wymaga wielu przedsięwzięć o charakterze technicznym i organizacyjnym, pozwalającym na wprowadzenie na obszarze Polski właściwych warunków do wytworzenia systemu pozwalającego nie tylko na gromadzenie danych w postaci elektronicznej, jak również udostępniania ich w czasie rzeczywistym, oraz wielokrotnego ich wykorzystywania.

Obecnie system gromadzenia danych z dokumentacji medycznej oparty jest głównie na formie pisemnej, co znacznie ogranicza dostępność do poszczególnych części dokumentacji, zwłaszcza w przypadku konieczności pozyskania danych związanych z kontynuacją leczenia.

W projekcie przyjęto, że elektroniczna dokumentacja medyczna udostępniana przez usługodawców w Systemie Informacji Medycznej, zwanym dalej „SIM”, zawierać będzie dokumenty elektroniczne w formacie XML, oraz pliki multimedialne będące wynikiem diagnostyki obrazowej. Elektroniczna dokumentacja medyczna zbudowana będzie w formie hierarchicznych struktur danych w odniesieniu do wszystkich rodzajów zdarzeń medycznych i plików multimedialnych będących wynikiem diagnostyki obrazowej.

SIM 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.), którego zadaniem jest gromadzenie, analiza i udostępnianie zasobów cyfrowych zawierających dane i informacje związane z udzielonymi, udzielanymi lub planowanymi świadczeniami opieki zdrowotnej.

Przyjęto, że udostępnianie elektronicznej dokumentacji medycznej odbywać się będzie w sposób umożliwiający identyfikację i autoryzację uprawnionych podmiotów przy użyciu bezpiecznego podpisu elektronicznego albo danymi potwierdzonymi profilem zaufanym ePUAP.

SIM umożliwia wymianę pomiędzy usługodawcami dokumentacji medycznej prowadzonej w postaci elektronicznej oraz dostarcza narzędzia do elektronicznego rozliczenia usługodawców i płatników.

SIM umożliwia wymianę danych i informacji pomiędzy:

- 1) **usługodawcami** – w zakresie wymiany drogą elektroniczną dokumentacji medycznej, automatycznego dostępu do dokumentów elektronicznych związanych z kontynuacją leczenia (e-skierowanie, e-recepta, e-zlecenie) oraz dostępu usługodawców do informacji o stanie zdrowia usługobiorcy lub stosowanych poprzednio metodach leczenia. Pozwoli to na przyspieszenie wymiany informacji, ograniczy koszty związane np. z powtarzaniem badań diagnostycznych w celu ustalenia stanu zdrowia usługobiorcy badań. Możliwy zakres wymiany danych usługobiorców zostanie uprzednio zdefiniowany w systemie przez usługobiorcę;
- 2) **usługobiorcami a usługodawcami** - umawianie się na wizyty on - line, monitorowanie statusu na liście osób oczekujących na udzielenie świadczenia finansowanego ze środków publicznych w trybie on-line, elektroniczne powiadamiania o terminie udzielenia świadczenia, wyeliminowanie możliwości kilkukrotnego wpisywania się przez świadczeniobiorców na listę oczekujących na to samo świadczenie u kilku świadczeniodawców;
- 3) **usługobiorcami a SIM** – poprzez udostępnienie usługobiorcy dostępu do własnego konta zawierającego informacje o planowanych, udzielanych i udzielonych świadczeniach opieki zdrowotnej oraz usługach medycznych;
- 4) **usługodawcą a SIM** – poprzez umożliwienie wygenerowania z systemu raportów statystycznych;
- 5) **usługodawcami a płatnikiem** – poprzez generowanie raportów niezbędnych do rozliczenia udzielonych świadczeń medycznych oraz faktur elektronicznych przy wykorzystaniu funkcjonalności Systemu RUM - NFZ;

6) **SIM a rejestrami medycznymi** – w zakresie udostępniania danych statystycznych, danych o zachorowaniach, planowanych, udzielanych i udzielonych świadczeniach opieki zdrowotnej, usługach medycznych i innych danych niezbędnych do określenia zapotrzebowania na świadczenia zdrowotne lub usługi medyczne oraz zarządzania zasobami i finansami systemu ochrony zdrowia – ta funkcja SIM znacznie zmniejszy obowiązki informacyjne, statystyczne i rozliczeniowe usługodawców oraz zapewni kompleksowość danych o funkcjonowaniu systemu;

7) **SIM a organami administracji publicznej i jednostkami samorządu terytorialnego** poprzez dostęp do danych służących optymalizacji celów i metod zarządzania ochroną zdrowia.

Osiągnięcie funkcjonalności SIM wymaga określenia szeregu warunków organizacyjnych i technicznych umożliwiających funkcjonowanie całego systemu i powiązania go z pozostałymi elementami systemu informacji w ochronie zdrowia.

Wprowadzenie opisu danych zawartych w SIM pozwoli na ujednoczenie zasad gromadzenia danych u poszczególnych usługodawców i umożliwi bezpieczną wymianę pomiędzy podmiotami uprawnionymi do dostępu do tych danych.

Obecnie obowiązujące przepisy nie zawierają tak kompleksowych regulacji w obszarze gromadzenia, przetwarzania i udostępniania danych medycznych.

Skutkuje to tym, że wdrożenie omawianego projektu wpłynie nie tylko na wprowadzenie nowej jakości w prowadzeniu dokumentacji medycznej, ale także będzie stanowiło podstawę prawną dla podejmowanych w sposób autonomiczny działań przez poszczególnych usługodawców czy płatników.

W projekcie określono w sposób szczegółowy zasady dostępu do danych gromadzonych w SIM oraz zasady bezpieczeństwa tych danych.

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, zwanego dalej „SZBI”.

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.

W związku z delegacją ustawową, która nakłada obowiązek zapewnienia ochrony danych i informacji dotyczących stanu zdrowia usługobiorców, w treści rozporządzenia, szczególną uwagę zwraca się na system zarządzania bezpieczeństwem informacji, ze szczególnym uwzględnieniem polityki bezpieczeństwa i Polskich Norm z zakresu bezpieczeństwa informacji.

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).

Ocena Skutków Regulacji

1. Podmioty, na które oddziałuje rozporządzenie:

Projekt oddziałuje na podmioty prowadzące bazy danych z zakresu ochrony zdrowia oraz wytwarzające dokumentację medyczną.

Ponadto projekt oddziałuje na wytwórców systemów teleinformatycznych i na podmioty prowadzące rejestry medyczne, pozostające w związku z systemem SIM.

Dotyczy to w szczególności:

- 1) usługobiorców (ok. 38 mln osób);
- 2) usługodawców (ok. 85 tys. podmiotów);
- 3) płatników (obecnie 25 podmiotów);
- 4) podmioty wykonujące działalność leczniczą, o których mowa w art. 19 ust. 2 ustawy (ok. 19 tys. podmiotów);
- 5) organów administracji rządowej i samorządowej w zakresie zadań z zakresu ochrony zdrowia przypisanych im przepisami odrębnymi (ok. 2,8 tys. podmiotów).

2. Konsultacje społeczne:

Projekt został przesłany m.in. 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

Spółczeństwa 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 lobbingsowej 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 wdrożenia projektu rozporządzenia pokrywane będą z projektów „Platforma Udostępniania On-Line Usług i Zasobów Cyfrowych Rejestrów Medycznych”(P2) i „Elektroniczna Platforma Gromadzenia Analizy i Udostępniania Zasobów Cyfrowych o Zdarzeniach medycznych”(P1).

Zgodnie z postanowieniami porozumienia o dofinansowanie (porozumienie nr POIG.07.01.00-00-008/09-00 zawarte 22.06.2009 r., z późn. zm.) całkowity koszt realizacji Projektu P2 wznosi 53 263 tys. zł. Kwota wydatków kwalifikowanych wynosi 50 763 tys. zł., z czego ze środków europejskich zostanie pokryta kwota 43 148,55 tys. zł. (stanowiąca 85%) oraz z budżetu państwa, z części 46 - Zdrowie, której dysponentem jest minister właściwy do spraw zdrowia – kwota 7 614,45 tys. zł. (stanowiąca 15%).

Zgodnie z postanowieniami porozumienia o dofinansowanie (porozumienie nr POIG.07.01.00-00-007/09-00 zawarte 22.06.2009 r., z późn. zm.) 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%).

Skutki finansowe dla budżetu państwa wynikające z niniejszej regulacji są częścią kosztów Platform P1 i P2. Koszty związane z projektowaną regulacją będą odnosiły się do wielu projektów i rozwiązań technicznych, których konieczność wytworzenia wynika bezpośrednio z ustawy. Regulacja ma charakter stricte techniczny i odnosi się m.in. do sposobów i zasad

udostępniania i wymiany pomiędzy usługodawcami danych zawartych w elektronicznej dokumentacji medycznej dalej zwaną „EDM”. Koszty związane z wytworzeniem mechanizmów umożliwiających wymianę danych z EDM będą pokrywane ze środków przeznaczonych na wytworzenia Platformy P1.

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 będzie miało wpływ na rynek pracy, w szczególności na zwiększenie poziomu zatrudnienia pracowników pionu IT, wytwórców oprogramowania oraz dostawców sprzętu IT.

c) konkurencyjność gospodarki i przedsiębiorczość w tym na funkcjonowanie przedsiębiorstw

Projektowana regulacja będzie miała pośredni wpływ na konkurencyjność gospodarki i przedsiębiorczość poprzez rozwój nowych technologii informacyjnych i komunikacyjnych.

d) na ochronę zdrowia ludności

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

e) sytuację i rozwój regionalny

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

4. Zgodność regulacji z prawem Unii Europejskiej

Projekt jest zgodny z prawem Unii Europejskiej.

