Ekonomiczne Problemy Usług nr 1/2018 (131), t. 2

ISSN: 1896-382X | www.wnus.edu.pl/epu
DOI: 10.18276/epu.2018.131/2-12 | strony: 127-135

Krzysztof Musiał
ActiveMED Sp. z o. o.
krzysztof.musial@activemed.pl

Mateusz Kuczabski
Akademia Sztuki Wojennej
Wydział Bezpieczeństwa Narodowego
Instytut Studiów Strategicznych
Katedra Bezpieczeństwa Informacyjnego i Komunikacji
mateusz.kuczabski@piastunzoz.pl

Bezpieczeństwo informacyjne w organizacjach ochrony zdrowia

Kod JEL: I 11
Słowa kluczowe: ochrona zdrowia, bezpieczeństwo informacyjne, sieci komputerowe
Streszczenie. Bezpieczeństwo informacyjne w sektorze ochrony zdrowia to wyzwanie najbliższych lat na wszystkich poziomach organizacyjnych. Począwszy od Ministerstwa Zdrowia, aż po pojedyncze gabinety realizujące świadczenia w zakresie ochrony zdrowia. Zmiana sposobu rejestrowania danych, ich rosnąca ilość i zakres wprowadzania do systemów, a także przetwarzanie i przesyłanie wymagają nowych metod i narzędzi zabezpieczania przed wyciekiem i utratą przechowywanych i przetwarzanych informacji. Konieczne staje się budowanie bezpiecznych systemów przechowujących i przetwarzających dane oraz kształtowanie świadomości w tym zakresie zarówno osób zarządzających jednostkami jak i całego personelu, który ma dostęp do przetwarzanych informacji.

Wprowadzenie

Upowszechnianie i rozwój technologii informacyjno-komunikacyjnych w jednostkach ochrony zdrowia spowodował w ostatnich latach gwałtowny wzrost ilości przechowywanych danych w systemach informatycznych. Zarówno na poziomie Ministerstwa Zdrowia, narodowego płatnika jakim jest NFZ, jednostek samorządu terytorialne-

go, jak i świadczeniodawców działających w publicznym systemie ochrony zdrowia oraz w placówkach komercyjnych.

Problem ilości i jakości przechowywanych danych rozpatrywany jest na dwóch poziomach. Poziomie zarządzania centralnego, mogącego kontrolować wielkość i prawidłowość wprowadzanych danych, a co za tym idzie racjonalizować sposoby wydatkowania środków publicznych na krytyczną infrastrukturę państwa – ochronę zdrowia oraz poziomie pojedynczych jednostek sektora zdrowia, które mogą optymalizować zasoby ludzkie i sprzętowe, pozwalając na efektywne zarządzanie.

Ustawa o ochronie danych osobowych z 1997 roku wraz z późniejszymi zmianami, rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych, a także przepisy dotyczące prowadzenia dokumentacji medycznej, narzucają na jednostki ochrony zdrowia określone wymagania dotyczące przechowywania, przetwarzania i udostępniania zbieranych danych (Rozporządzenie UE 2016/679, 2016).

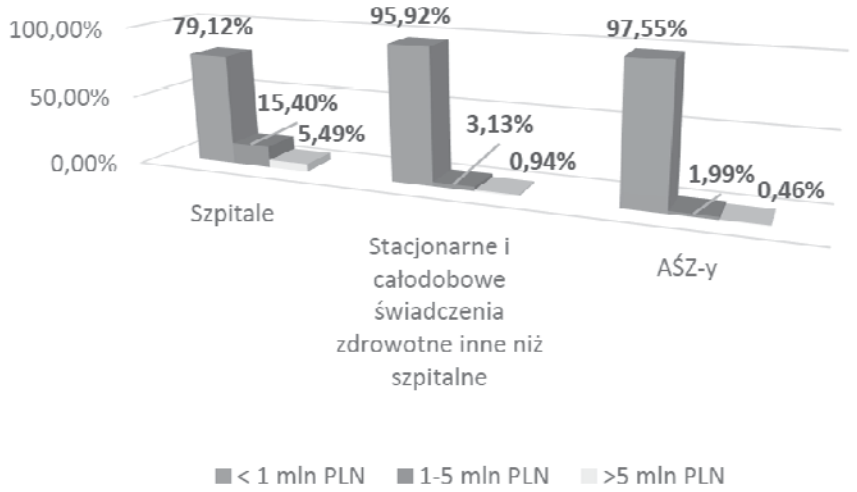
1. Wdrażanie systemów przetwarzania informacji w jednostkach sektora ochrony zdrowia

Przetwarzanie, przechowywanie i udostępnianie dokumentacji medycznej zarówno w formie papierowej, jak i elektronicznej obwarowane jest wieloma przepisami polskimi oraz europejskimi. Przygotowanie jednostki do wdrożenia systemu przetwarzania Elektronicznej Dokumentacji Medycznej musi uwzględniać wiele obszarów zarządzania placówki (*Rekomendacje Centrum Systemów*…, 2017). Pominięcie jednego z obszarów może skutkować poważnymi błędami mogącymi uniemożliwić poprawną realizację takiego wdrożenia. Zakres wdrożenia powinien obejmować przynajmniej:

- modelowanie struktury organizacyjnej jednostki,
- przygotowanie i wdrożenie polityki bezpieczeństwa,
- przygotowanie i wdrożenie infrastruktury sieciowej,
- dobór urządzeń i sprzętu informatycznego,
- dobór serwerów i stacji roboczych,
- dobór oprogramowania,
- utrzymanie i zabezpieczenie infrastruktury teleinformatycznej,
- zasady dostępu do urządzeń i danych,
- metody archiwizacji i reguł postepowania w przypadku naruszeń polityki bezpieczeństwa.

2. Finansowanie

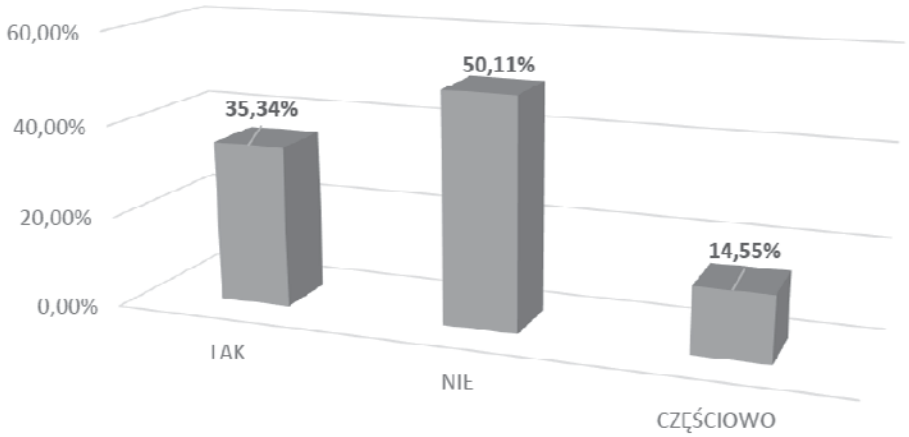
Jednym z podstawowych problemów wspomnianego wdrożenia systemów jest brak dostatecznego finansowania w jednostkach służby zdrowia. Na podstawie badania przeprowadzonego w 2016 roku przez CSIOZ koszt wdrożenia systemów HIS w ankietowanych jednostkach jest wysoki. „79% szpitali, 96% stacjonarnych całodobowych świadczeń zdrowotnych innych niż szpitalne oraz 97% AŚZ-ów szacuje, iż na ten cel potrzebuje poniżej 1 miliona złotych, 15% szpitali, 3% stacjonarnych całodobowych świadczeń zdrowotnych innych niż szpitalne oraz 2% AŚZ-ów pomiędzy 1–5 milionów złotych, a 5% szpitali, 1% stacjonarnych całodobowych świadczeń zdrowotnych innych niż szpitalne oraz 0,5% AŚZ-ów powyżej 5 milionów złotych" (*Badanie stopnia przygotowania*…, 2016).



Rysunek 1. Szacowana wartość dostosowania się podmiotu do obowiązków właściwych na podstawie ustawy z 28 kwietnia 2011 roku o systemie informacji w ochronie zdrowia

Źródło: *Badanie stopnia przygotowania*… (2016).

Pomocne okazują się tutaj środki z funduszy unijnych w ramach projektów e-Zdrowia, z których skorzystało wiele jednostek świadczących usługi w publicznym systemie ochrony zdrowia. Od 2007 roku część z nich, w tym publiczne zakłady opieki zdrowotnej, uzyskała finansowanie pozwalające na wdrożenie informatycznych systemów HIS klasy EDM. Zgodnie z deklaracjami ankietowanymi w 2016 roku systemy Elektronicznej Dokumentacji Medycznej obejmującej przynajmniej podstawowe elementy miało do 50% ankietowanych.



Rysunek 2. Czy podmiot leczniczy ma rozwiązania informatyczne umożliwiające prowadzenie dokumentacji medycznej w postaci elektronicznej (w rozumieniu ustawy o SIOZ, czyli w postaci dokumentów elektronicznych)?

Źródło: *Badanie stopnia przygotowania*… (2016).

3. Polityka bezpieczeństwa

Ustawa o ochronie danych osobowych z 29 sierpnia 1997 roku nałożyła na administratora danych obowiązek opracowania i wdrożenia Polityki Bezpieczeństwa oraz Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych. Należy tu zwrócić uwagę, że w przypadku podmiotów realizujących świadczenia zdrowotne, poza danymi osobowymi przetwarzane są również dane wrażliwe (dane dotyczące zdrowia) podlegające szczególnej ochronie (Świtała, 2016). Zgodnie z par. 6 dane wrażliwe o stanie zdrowia są przetwarzane w systemach teleinformatycznych o poziomie bezpieczeństwa podwyższonym lub wysokim – w przypadku połączenia rozwiązań służących do przetwarzania danych z publiczną siecią telekomunikacyjną. Szczegółowy katalog i opis środków bezpieczeństwa stosowany na poszczególnych poziomach określa załącznik do omawianego rozporządzenia (Rozporządzenie UE 2016/679, 2016).

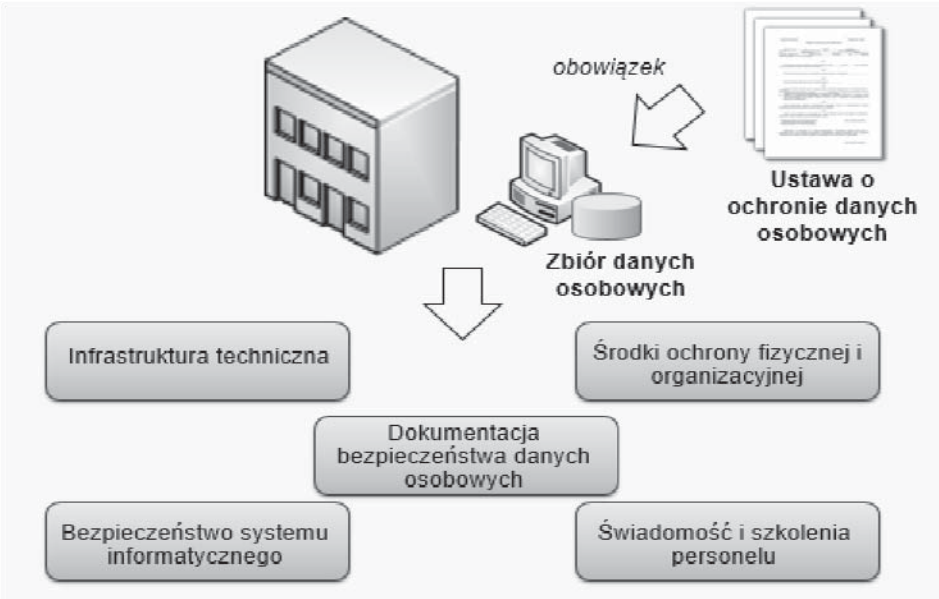
Zgodnie z wymogami ustawy przygotowano wytyczne dla usługodawców realizujących świadczenia w zakresie ochrony zdrowia przez prezesa CSIOZ (*Rekomendacje Centrum Systemów*…, 2017). Podstawowe elementy obejmujące zakres krytycznych składowych z uwagi na bezpieczeństwo budowy takich systemów stanowią:

- bezpieczeństwo fizyczne i środowiskowe,
- bezpieczeństwo sieciowe,
- bezpieczeństwo systemów klasy EDM,
- kontrola dostępu,
- stosowanie podpisu elektronicznego,
- audytowalność i niezaprzeczalność danych zdarzeń w systemie,

– archiwizacja danych medycznych,
– zarządzanie incydentami związanymi z bezpieczeństwem informacji,
– zarządzanie ciągłością działania.

W celu zapewnienia bezpieczeństwa jednostki, konieczne jest podjęcie działań w każdym z wymienionych elementów. W zależności od wybranego rodzaju oprogramowania (model klasyczny, outsourcing-kolokacja, IAAS, PAAS, SAAS) zabezpieczenie poszczególnych elementów może należeć bezpośrednio do jednostki ochrony zdrowia lub usługodawcy realizującego konkrety zakres usług.

Poza wyżej wymienionymi, istotnym elementem bezpieczeństwa informacyjnego jest budowanie świadomości personelu w jednostce, który ma dostęp do danych osobowych (Strategia cyberbezpieczeństwa, 2016). Uświadomienie ryzyka związanego z nieuprawnionym przekazywaniem danych osobom, które bezpośrednio mają do nich dostęp, może w znaczącym stopniu ograniczyć występowanie takich incydentów.



Rysunek 3. Elementy organizacyjne i prawne konieczne do poprawnego wdrożenia polityki bezpieczeństwa w organizacji

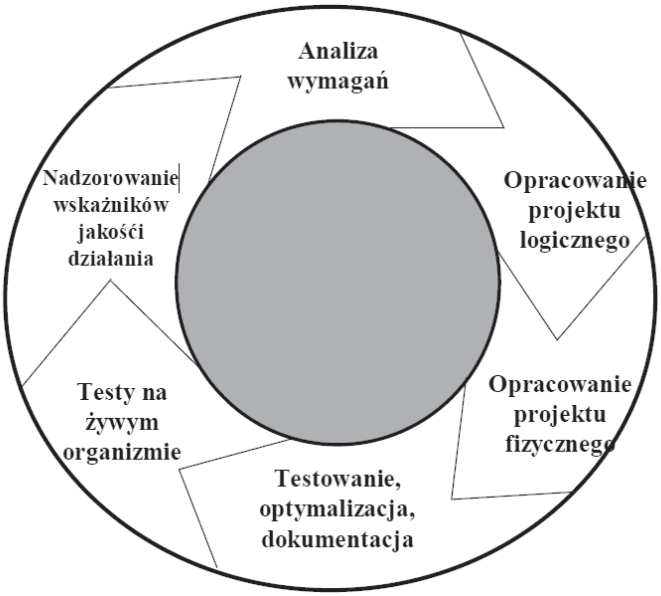
Źródło: opracowanie własne na podstawie: „ABC bezpieczeństwa danych osobowych przetwarzanych przy użyciu systemów informatycznych", www.giodo.gov.pl.

4. Wdrożenie infrastruktury sieciowej i sprzętowej

Mnogość i złożoność rozwiązań sieciowych i serwerowych sprawia, że doborem odpowiedniego sprzętu muszą zająć się eksperci. Z doświadczeń własnych wynika, że nawet jednostki dysponujące swoimi działami IT i zatrudnionymi tam informatykami nie są w stanie samodzielnie dobrać sprzętu do potrzeb w ramach konkretnego rozwią-

zania. Potencjalni dostawcy konkurują cenami – a rozpiętość cen urządzeń sieciowych i serwerów jest bardzo duża – nie zapewniając optymalnych rozwiązań i jakości. Konieczność wyboru określonych modułów, funkcji może być kluczowa z punktu widzenia bezpieczeństwa i funkcjonalności projektowanego systemu. Odpowiedni projekt infrastruktury sieciowej, dobór konkretnego rozwiązania czy technologii może uprościć zarządzanie taką infrastrukturą bądź ją bardzo utrudnić, czy wręcz uniemożliwić działanie. Z tego powodu, na uwagę zasługuje rozwiązanie polegające na projektowaniu za pomocą metody *top-down* firmy Cisco (Oppenheimer, 2007). Zakłada ono cztery podstawowe fazy przygotowania do uruchomienia sieci teleinformatycznej:

Część I – Określenie potrzeb i celów klienta.
Część II – Projekt logiczny.
Cześć III – Projekt fizyczny.
Część IV – Testy, dokumentacja i konserwacja.



Rysunek 4. Poszczególne elementy przy projektowaniu sieci metodą *top-down*

Źródło: opracowanie własne.

Wspomniany sposób projektowania, bez względu na rodzaj wykorzystywanego połączenia – czy będzie to połączenie kablowe czy bezprzewodowe gwarantuje, że zaprojektowana sieć będzie wydajna, zarządzalna i skalowalna, co z kolei pozwala na bezproblemową pracę przez długie lata.

Drugim, nie mniej ważnym elementem, jest infrastruktura serwerowa. Wybór odpowiedniej technologii wdrożenia systemu jest zagadnieniem kluczowym dla poprawnej i bezpiecznej pracy całego systemu. Technologie uwierzytelniania, autoryzacji,

autentykacji systemów pozwalają na bezpieczną pracę złożonych systemów. Metody uwierzytelniania serwerów RADIUS, czy też jednokrotnego logowania (SSO – *Single Sign On*) pozwalają na bezpieczną, ale też wygodną pracę dla użytkowników całego systemu. Dzięki takim rozwiązaniom nie jest konieczne zapamiętywanie kilku haseł do logowania do każdego systemu. Jeden login i hasło dają użytkownikowi dostęp do wszystkich systemów – przy czym do każdego zgodnie z jego listą ACL (*Access Control List*)

5. Dobór oprogramowania

Elementarnym problemem jednostki jest taki wybór systemu, który zapewni poprawne funkcjonowanie w określonych warunkach organizacyjno-prawnych. Obecnie brakuje doradców w zakresie wsparcia jednostek w doborze właściwego rodzaju oprogramowania i wyboru jego funkcjonalności, obejmującej jak największy obszar działalności konkretnej organizacji. Z uwagi na liczbę i jakość funkcjonujących systemów na polskim rynku, dobór systemu jest trudnym zadaniem. System pracujący w tzw. chmurze bardzo dobrze sprawdza się dla pojedynczego gabinetu, który samodzielnie nie jest w stanie realizować bieżących aktualizacji, weryfikacji czy archiwizacji, a dzięki zastosowaniu tej technologii, są one wykonywane regularnie i poprawnie. Jednostki korzystające w swojej działalności z rozwiązań wielostanowiskowych, które decydują się na zastosowanie technologii tzw. chmury, potencjalnie mogą być narażone, w przypadku braku dostępu do internetu (awaria łączy, lokalnego routera dostępowego), na przerwę w pracy dla kilkudziesięciu specjalistów.

Należy podkreślić, że jednym z podstawowych argumentów wdrażania systemów HIS jest lepsza organizacja pracy, która ma podnosić wydajność całej jednostki, co w dobie starzejącego się społeczeństwa i ograniczonych środków na finansowanie służby zdrowia staje się kluczowym zagadnieniem dla przetrwania jednostki w warunkach bieżącej i przyszłej sytuacji rynkowej oraz zapewnienia wysokiego poziomu świadczonych usług. Równie istotnym argumentem jest wpieranie decyzji medycznych dzięki budowanej bazie wiedzy i umiejętnego wykorzystania przechowywanych informacji. Dzięki coraz częściej pojawiającym się funkcjonalnościom, które wspomagają decyzje lekarzy na podstawie zgromadzonych informacji – leczenie pacjenta może być bardziej efektywne i mniej kosztochłonne. Niestety, w tym zakresie odnotowuje się często brak zrozumienia i niechęć personelu medycznego do wdrażanych rozwiązań. Problemem jest także brak na rynku specjalistów przygotowanych do wykonywania wdrożeń, które wymagają częstej i różnorodnej komunikacji pomiędzy systemami, umożliwiającej opracowanie jak najdokładniejszych baz danych, wspomagających decyzje lekarzy. Próbą rozwiązania mogą okazać się działające obecnie tzw. Regionalne Platformy Gromadzenia, Analizy i Udostępniania Zasobów Cyfrowych o Zdarzeniach Medycznych, które choć w ograniczonym zakresie, to jednak zbierają dane o zdarzeniach medycznych od części jednostek sektora ochrony zdrowia. Przykładem takiej platformy

jest m.in. Podkarpacki System Informacji Medycznej (PSIM) uruchomiony w 2014 roku (www.psim.podkarpackie.pl). Wspomniane platformy były tworzone z założeniem ich integracji z powstającym systemem centralnym w ramach Krajowej Platformy P1, ale wdrożenie to jest przesuwane w czasie. Zintegrowanie wszystkich systemów pozwoliłoby na pełną wymianę informacji pomiędzy jednostkami ochrony zdrowia, takimi jak szpitale, ambulatoria, laboratoria, apteki a nawet lecznice weterynaryjne.

Podsumowanie

Systemy ochrony zdrowia przetwarzają i przechowują bardzo rozległą informację o stanie zdrowia pacjentów. Bezpieczeństwo przetwarzanych informacji stanowi wyzwanie na najbliższe lata na wszystkich poziomach zarządzania w systemie ochrony zdrowia. Brak specjalistów d.s. bezpieczeństwa, wykorzystywanie przestarzałych technologii, luki w zabezpieczeniach, brak świadomości użytkowników systemów informatycznych to rzeczywistość sporej części podmiotów przetwarzających dane medyczne. Dopóki sytuacja nie ulegnie drastycznej poprawie bezpieczeństwo informacyjne w całym obszarze będzie zagrożone, a dane pacjentów już są zagrożone. Wycieki takich informacji niestety się zdarzają (www.zaufanatrzeciastrona.pl, 2017).

Bibliografia

ABC bezpieczeństwa danych osobowych przetwarzanych przy użyciu systemów informatycznych (2007). Wydawnictwo sejmowe. Pobrane z: www.giodo.gov.pl.

Badanie stopnia przygotowania podmiotów wykonujących działalność leczniczą do obowiązków wynikających z ustawy z 28 kwietnia 2011 roku o systemie informacji w ochronie zdrowia (2016). CSIOZ. Pobrane z: https://www.csioz.gov.pl/aktualnosci/szczegoly/wyniki-ii-edycji-badania-ankietowego-dotyczacego-stopnia-informatyzacji-podmiotow-wykonujacych-dz/.

Oppenheimer, P. (2007). *Cisco. Projektowanie sieci metodą Top-Down.* Warszawa: Wydawnictwo Naukowe PWN.

Podkarpacki System Informacji Medycznej (2014). Pobrane z: https://psim.podkarpackie.pl/strona-glowna.

Rekomendacje Centrum Systemów Informacyjnych Ochrony Zdrowia w zakresie bezpieczeństwa oraz rozwiązań technologicznych stosowanych podczas przetwarzania dokumentacji medycznej w postaci elektronicznej (2017). CSIOZ 2017. Pobrane z: www.csioz.gov.pl.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 roku. Pobrane z: http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32016R0679.

Świtała, K. (2016). *Obowiązki prawne podmiotów przetwarzających dane medyczne w kontekście wdrażania rozwiązań e-zdrowia w Polsce*. *Roczniki. Kolegium Analiz Ekonomicznych, 42*, 407–421.

Wytyczne, zasady i rekomendacje dla usługodawców w zakresie budowy i stosowania systemu bezpiecznego przetwarzania elektronicznej dokumentacji medycznej (2014), cz. 1–6. CSIOZ. Pobrane z: https://csioz.gov.pl/aktualnosci/archiwum/szczegoly/zaktualizowane-wytyczne-i-rekomendacje-w-zakresie-bezpiecznego-przetwarzania-edm/.

Wyciek danych wrażliwych (2017). Pobrane z: https://zaufanatrzeciastrona.pl/post/wyciek-danych-wrazliwych-50-tysiecy-pacjentow-polskiego-szpitala/.

Założenia strategii cyberbezpieczeństwa dla Rzeczypospolitej Polskiej (2016). Pobrane z: http://www.konsultacje.gov.pl/sites/default/files/file-attachments/3903/.

INFORMATION SECURITY IN HEALTHCARE INSTITUTION

Keywords: healthcare, information security, computer networks

Summary. Information security in the healthcare sector is the main challenge at all levels of organizations in upcoming years. Starting with Health Ministries to single offices providing health services. Change the way of registration of data and its increasing amount, the scope of entering data into the system, and also processing and data transmission demand new methods and tools to protect from leaks and loosing proceeded and stored information. It is becoming to be necessary to build safe systems dealing with storing and preceding data and create public awareness in this filed among both management of healthcare institutions and all medical staff who have access to proceed information.

Translated by Mateusz Kuczabski

Cytowanie

Musiał, K., Kuczabski, M. (2018). Bezpieczeństwo informacyjne w organizacjach ochrony zdrowia. *Ekonomiczne Problemy Usług*, *2* (131/2), 127–135. DOI: 10.18276/epu.2018.131/2-12.