Ewa M. Kwiatkowska*, Małgorzata Skórzewska-Amberg**

Technologie informacyjno-komunikacyjne w ochronie zdrowia – problematyka naruszania prywatności

Spis treści

Streszczenie

Artykuł poświęcony jest technologiom informacyjno-komunikacyjnym (ICT) w sektorze ochrony zdrowia. Scharakteryzowano pojęcia prawne dotyczące omawianej problematyki. Podkreślono zagrożenia związane z kwestią ochrony danych wrażliwych, do których należą między innymi informacje dotyczące stanu zdrowia pacjentów. Przeanalizowano stan informatyzacji ochrony zdrowia w Polsce w kontekście zbliżającego się wprowadzenia obowiązku prowadzenia dokumentacji medycznej w postaci elektronicznej.

Słowa kluczowe: Internet rzeczy; ochrona prywatności; ochrona danych osobowych; Elektroniczna Dokumentacja Medyczna; System Informacji Medycznej.

JEL: I18, K14

I. Wprowadzenie

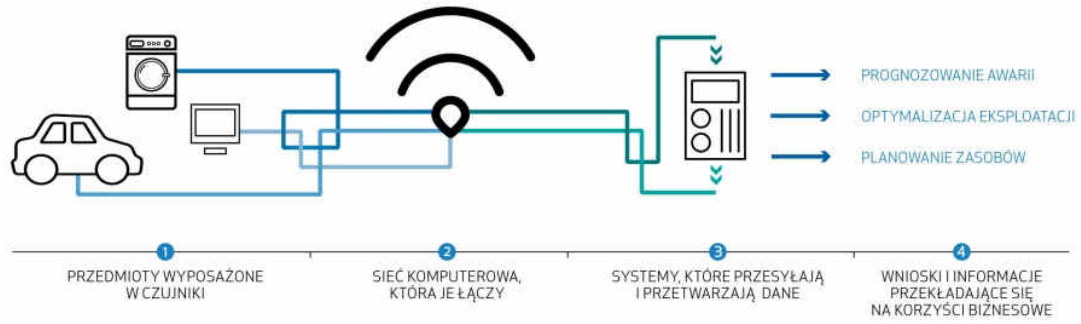
Dzięki szybkiemu rozwojowi i upowszechnieniu Internetu udostępnione zostały praktycznie nieograniczone zasoby informacji, które mogą być szybko przetwarzane i przesyłane. Teksty, obrazy, dźwięki przekazywane w globalnej sieci stały się poszukiwanym towarem, dostępnym w każdym miejscu i czasie. Początek XXI wieku wyznacza nowy etap w rozwoju społecznym – pojawienie się społeczeństwa informacyjnego, definiowanego jako wysoko rozwinięte społeczeństwo,

* Adiunkt w Katedrze Metod Ilościowych i Zastosowań Informatyki Akademii Leona Koźmińskiego; e-mail: ewcia@kozminski.edu.pl.
** Adiunkt w Katedrze Teorii i Filozofii Prawa Akademii Leona Koźmińskiego; e-mail: mskorzewska@kozminski.edu.pl.

w którym zapewniony jest pełen dostęp do usług i informacji przy użyciu technologii informacyjno-komunikacyjnych (ICT) (Bangemann, 1994)[1].

Coraz częściej sieć wykorzystywana jest nie tylko do pozyskiwania, przetwarzana i przesyłania informacji między ludźmi – użytkownikami Internetu, lecz także do pozyskiwania i wymiany danych między urządzeniami podłączonymi do sieci. Wszelkie urządzenia podłączone do sieci, których oprogramowanie umożliwia zdalnie nimi sterowanie tworzą tzw. Internet rzeczy (*Internet of Things*, IoT). Ściślej rzecz ujmując IoT może być traktowany jako pewien podzbiór Internetu, obejmujący komunikujące się ze sobą urządzenia, przestrzeń komunikacji tych urządzeń oraz wszelkie przetwarzane dane (rys. 1).

Rysunek 1. Internet rzeczy



Źródło: SAS Institute.

Rozwój globalnych sieci teleinformatycznych powoduje przeniesienie coraz większej części ludzkiej aktywności do sfery wirtualnej. Wraz z rozpowszechnianiem się Internetu rzeczy, pojawia się coraz więcej tzw. urządzeń inteligentnych (*smart devices*), tj. takich, które działają autonomicznie i, opierając się na algorytmach sztucznej inteligencji, podejmują określone działania. Rozwój technologii powoduje, że coraz częściej urządzenia takie działają „w tle" – poza bieżącą kontrolą człowieka. Zyskujące rosnącą popularność inteligentne domy (*smart homes*) wyposażone są w cały zestaw urządzeń, które w sposób niebywale skuteczny ułatwiają życie – kontrolują temperaturę pomieszczeń, stopień nawilgotnienia powietrza, sterują oświetleniem w zależności od pory dania i roku, włączają urządzenia kuchenne (toster, ekspres do kawy itp.), gdy budzik zaczyna budzić domowników, zamawiają dostawę brakujących artykułów spożywczych (np. inteligentne lodówki). Niestety urządzenia te równie skutecznie mogą być wykorzystywane do permanentnej inwigilacji domowników. Działanie inteligentnych urządzeń oparte jest na przetwarzaniu (przede wszystkim gromadzeniu i analizie) danych pozyskiwanych w sposób ciągły, a dotyczących m.in. zwyczajów domowników (np. rozkład dnia), rodzajów ich aktywności, ulubionych firm, seriali, książek (np. przez zamawianie ebooków), muzyki, aż po dane, które mogą dotyczyć rejestracji obrazu czy dźwięku (alarm, monitoring itp.).

Internet rzeczy nie stanowi zagrożenia, dopóki pozyskiwane dane, stanowiące już kategorię *big data*, wykorzystywane są wyłącznie pod kontrolą osób, których dotyczą. Jeśli jednak ktokolwiek nieuprawniony (tzn. osoba, która nie jest podmiotem danych, względnie nie otrzymała od

[1] Por. Dyrektywa 98/34/WE Parlamentu Europejskiego i Rady z 22.06.1998 r., *Dz. U. L 204, 21/07/1998 s. 0037 – 0048*, znowelizowana dyrektywą 98/48/WE Parlamentu Europejskiego i Rady z 20.07.1998 r. zmieniającą dyrektywę 98/34/WE ustanawiającą procedurę udzielania informacji w zakresie norm i przepisów technicznych, *Dz. U. L 217, 05/08/1998 s. 0018 – 0026.*

podmiotu danych stosownego upoważnienia do przetwarzania danych) uzyska do nich dostęp, mamy wtedy do czynienia z naruszeniem prawa do prywatności.

Zastosowanie ICT, w tym szczególnie Internetu rzeczy w nauce i przemyśle może kompletnie zmienić codzienne życie i to już w najbliższej przyszłości. Prawdziwa rewolucja ma szansę dokonać się w medycynie i ochronie zdrowia – począwszy od stosowania inteligentnych systemów wspomagających diagnozowanie, przez specjalnie projektowane czujniki monitorujące bieżący stan zdrowia, aż do wysoce wyspecjalizowanych technologii umożliwiających zdalne stosowanie procedur medycznych. Przykładami implementowania Internetu rzeczy w ochronie zdrowia mogą być m.in.: czasowe tatuaże oparte na półprzewodnikach, monitorujących procesy życiowe życia płodowego dziecka oraz jego matki – wraz z oprogramowaniem ostrzegającym przed możliwością przedwczesnego porodu czy smart soczewki dla diabetyków, wyposażone w możliwość transmisji danych, dokonujące pomiaru poziomu cukru (*5 przykładów…*, http). Pionierskim w skali światowej przykładem wykorzystywania najnowszych technologii jest prowadzony od 2017 r. polski projekt NoMED-AF (nieinwazyjny monitoring we wczesnym wykrywaniu migotania przedsionków), którego celem jest próba wykrycia częstości występowania migotania przedsionków, w tym tzw. niemego, tj. bezobjawowego migotania przedsionków. Wykorzystywane w projekcie urządzenie Comarch NoMED-AF składa się z: kamizelki do badania EKG, rejestratora umieszczanego w kamizelce oraz bezobsługowej stacji transmisyjnej, przesyłającej sygnał badania EKG do centrali w Zabrzu. Kamizelki skonstruowane są w taki sposób, aby w jak najmniejszym stopniu utrudniały pacjentom normalne funkcjonowanie, jednocześnie zapewniając wysokiej jakości, prawidłowe, długookresowe, bo trwające do 30 dni badanie pracy serca przez rejestrację sygnału EKG (COMARCH, 2017).

Nie można zapominać o rzeczach wydawałoby się prozaicznych, które mogą znacząco ułatwić życie i pacjenta, i lekarza, takich jak dokumentacja medyczna prowadzona w formie elektronicznej oraz systemy umożliwiające wymianę informacji w czasie rzeczywistym. Dostępność dokumentów w wersji elektronicznej (oraz digitalizacja dokumentów papierowych) jest ważna, jednak kluczową sprawą jest możliwość zapewnienia płynnej, szybkiej i przede wszystkim bezpiecznej wymiany danych między różnymi podmiotami ochrony zdrowia, m.in. szpitalami, ośrodkami zdrowia, lekarzami rodzinnymi – niezależnie od publicznego czy prywatnego źródła ich finansowania. Zagrożenia związane z wdrożeniem i stosowaniem Internetu rzeczy w ochronie zdrowia, w szczególności zaś Elektroniczna Dokumentacja Medyczna oraz analiza stanu informatyzacji ochrony zdrowia w Polsce, są szczególnym przedmiotem analizy w niniejszym artykule.

II. Uwarunkowania prawne technologii informacyjno-komunikacyjnych

Pojęcie ICT obejmuje wszelkie media umożliwiające komunikację (w tym Internet, sieci przewodowe i bezprzewodowe, telefonię stacjonarną, komórkową i satelitarną, technologie komunikacji dźwięku i obrazu, radio, telewizje itp.) oraz zapis informacji (pamięci przenośne, dyski twarde, dyski CD/DVD, taśmy itp.), a także sprzęty umożliwiające przetwarzanie informacji (np. komputery osobiste, serwery, klastry, sieci komputerowe), wraz z oprogramowaniem umożliwiającym przetwarzanie i przesyłanie danych (*Słownik pojęć Strategii Rozwoju Transportu*, 2017).

Polskie prawo posługuje się określeniem „system teleinformatyczny", które to pojęcie definiują: art. 3 ust. 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów

realizujących zadania publiczne (t.j. Dz.U. 2017, poz. 570) oraz art. 2 ust. 3 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (t.j. Dz.U. 2017, poz. 1219), określając system teleinformatyczny jako zespół współpracujących ze sobą urządzeń i oprogramowania zapewniający przetwarzanie (w tym ich przechowywanie, wysyłanie i odbieranie) danych w sieciach telekomunikacyjnych[2].

Przestrzeń, w której przesyłane są dane i komunikaty między systemami teleinformatycznymi, określana jest mianem cyberprzestrzeni (Maurer, 2011). Definicja legalna cyberprzestrzeni znajduje się w art. 1b ustawy z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (t.j. Dz.U. 2016, poz. 851 ze zm.), który określa cyberprzestrzeń jako przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne wraz z powiązaniami między nimi oraz relacjami z użytkownikami.

Prywatność można określić jako sferę zastrzeżoną do wyłącznej dyspozycji konkretnego człowieka. Prawo do prywatności obejmuje m.in.: prawo do ochrony wizerunku, czci, miru domowego czy prawo do tajemnicy komunikowania się. Zakres prawa do prywatności jest pojęciem trudnym do zdefiniowania, gdyż każdorazowo uzależniony będzie od decyzji jednostki. To co dla jednych jest naruszeniem prywatności (np. upublicznienie wizerunku), dla innych będzie działaniem neutralnym czy wręcz pożądanym (np. dla celebryty).

Przyznane w art. 8 Europejskiej Konwencji Praw Człowieka prawo do ochrony prawnej przeciwko ingerencjom w prywatność oraz zobowiązanie do pozytywnej ochrony życia prywatnego i rodzinnego, mieszkania i korespondencji, według Europejskiego Trybunału Praw Człowieka i Europejskiej Komisji Praw Człowieka oznaczają dla jednostki m.in.: możliwość nieskrępowanego nawiązywania kontaktów z innymi ludźmi według swojego wyboru, możliwość decydowania o zakresie ujawniania dotyczącej jej informacji, uniemożliwienie przejęcia przez osoby nieuprawnione wiadomości przekazywanych za pomocą wszelkich sposobów komunikowania się i zagwarantowanie dotarcia informacji do adresata (Hofmański, 1997).

Konstytucja Rzeczpospolitej Polskiej w art. 47 stanowi o ochronie życia prywatnego, która obejmuje także autonomię informacyjną (art. 51 Konstytucji), oznaczającą prawo do samodzielnego decydowania o ujawnieniu innym informacji dotyczących swojej osoby, a także prawo do sprawowania kontroli nad takimi informacjami, jeżeli znajdują się w posiadaniu innych podmiotów[3]. W wyroku z dnia 12 listopada 2002 r. Trybunał Konstytucyjny podkreślił, że istota autonomii informacyjnej każdego człowieka sprowadza się do pozostawienia każdemu swobody w określeniu sfery dostępności dla innych wiedzy o sobie[4].

O zakresie przetwarzanych informacji i kręgu osób, którym są one udostępniane decyduje ten, którego dane dotyczą. Większość ludzi nie zdaje sobie jednak sprawy z tego, jak wiele danych o sobie ujawnia, i jak dużym zagrożeniem dla prywatności może stać się niekontrolowane udostępnienie zbyt wielu takich danych.

[2] Przetwarzanie odbywa się za pomocą właściwego dla danego rodzaju sieci urządzenia końcowego przeznaczonego do podłączenia bezpośrednio lub pośrednio do zakończeń sieci (telekomunikacyjne urządzenie końcowe, art. 2 pkt 43 ustawy z 16.07.2004 r. – Prawo telekomunikacyjne (Dz.U. z 2016 r., poz. 1489, ze zm.).

[3] Por. wyr. TK z 19.02.2002 r., K3/01 (OTK ZU Nr 1/A/2002, poz. 3).

[4] Wyr.TK z 12.11.2002 r., SK40/01 (OTK ZU 2002 r. Nr 6, poz. 81).

III. Elektroniczna Dokumentacja Medyczna – uregulowania prawne

Z technicznego punktu widzenia Elektroniczna Dokumentacja Medyczna (EDM) jest to baza danych, w której jest zapisana i przechowywana całość lub część indywidualnej (dotyczącej konkretnego pacjenta) i zbiorczej (dotyczącej grup pacjentów) dokumentacji medycznej. Aby Elektroniczna Dokumentacja Medyczna zapewniała pełną funkcjonalność, musi być ona częścią systemu wymiany danych umożliwiającego dostęp do dokumentacji w dowolnym miejscu i czasie przez wszystkie upoważnione do tego osoby, w tym pacjenta, którego dokumentacja ta dotyczy.

Definicja legalna EDM zawarta jest w art. 2 pkt 6 ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (t.j. Dz.U. 2016, poz. 1535), który określa ją jako dokument elektroniczny umożliwiający usługobiorcy uzyskanie świadczenia opieki zdrowotnej od świadczeniodawcy określonego w art. 5 pkt 41 ustawy z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych[5] (t.j. Dz.U. 2016, poz. 1793 ze zm.), ogólnodostępnej apteki lub punktu aptecznego oraz wytworzoną w postaci elektronicznej indywidualną dokumentację medyczną (z wyłączeniem skierowań)[6]. Sposób prowadzenia i udostępniania dokumentacji medycznej regulowany jest przez ustawę o systemie informacji w ochronie zdrowia oraz ustawę z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (t.j. Dz.U. 2017, poz. 1318). Zgodnie z art. 56 ustawy o systemie informacji w ochronie zdrowia od 1 stycznia 2018 r. forma elektroniczna będzie jedyną formą prowadzenia dokumentacji medycznej.

Gromadzenie i przetwarzanie danych o pacjentach nierozerwalnie związane jest z koniecznością zapewnienia ochrony prywatności pacjentów, których dane są przetwarzane. W przypadku pacjentów można próbować wyróżnić dwie kategorie przetwarzanych danych: „zwykłe" dane osobowe oraz tzw. wrażliwe dane osobowe.

Art. 6 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. 2016, poz. 922) definiuje dane osobowe jako wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Zatem „danymi osobowymi są wszelkie informacje dotyczące zidentyfikowanej lub dającej się zidentyfikować osoby, a nie tylko takie informacje, które same służą identyfikacji" (Barta, Fajgielski i Markiewicz, 2015, s. 344). Polskie prawo posługuje się określeniem danych osobowych zarówno w odniesieniu do danych bezpośrednio służących identyfikacji osoby (danych personalnych), jak i danych prywatnych rozumianych jako dane dotyczące życia prywatnego osoby, np. stan cywilny, stan zdrowia. Możliwość jakiegokolwiek przetwarzania danych osobowych (gromadzenia, usuwania, przesyłania, modyfikowania itp.) uzależniona jest od zgody podmiotu danych (osoby, której dane dotyczą).

Dane tzw. wrażliwe są to dane, określone w art. 27 ust. 1 ustawy, dotyczące szczególnych kategorii informacji, których ujawnienie mogłoby narazić podmiot danych na szkodę. Do kategorii danych wrażliwych należą m.in. dane o stanie zdrowia, kodzie genetycznym i nałogach, a więc

[5] Świadczeniodawcą jest podmiot wykonujący działalność leczniczą w rozumieniu przepisów o działalności leczniczej, inna osoba fizyczna – posiadająca fachowe uprawnienia do udzielania świadczeń zdrowotnych i udzielająca ich w ramach wykonywanej działalności gospodarczej, podmiot realizujący czynności z zakresu zaopatrzenia w wyroby medyczne.

[6] Sposób wytwarzania takiej dokumentacji regulowany jest w: rozporządzeniu Ministra Zdrowia z 9.11.2015 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania (Dz.U. z. 2015 r., poz. 2069), rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z 25.02. 2016 r. w sprawie rodzajów, zakresu i wzorów oraz sposobu przetwarzania dokumentacji medycznej w podmiotach leczniczych utworzonych przez ministra właściwego do spraw wewnętrznych (Dz.U. z 2016 r., poz. 249) oraz rozporządzeniu Ministra Sprawiedliwości z 26.02.2016 r. w sprawie rodzajów i zakresu dokumentacji medycznej prowadzonej w podmiotach leczniczych dla osób pozbawionych wolności oraz sposobu jej przetwarzania (Dz.U. z 2016 r., poz. 258).

takie, które stanowią integralną część informacji przechowywanych w dokumentacji medycznej pacjenta. Przetwarzanie danych wrażliwych jest co do zasady zabronione, jednak ustawa przewiduje wyjątki określone w art. 27 ust. 2. Należy do nich przetwarzanie prowadzone w celu ochrony stanu zdrowia, świadczenia usług medycznych lub leczenia pacjentów przez osoby trudniące się zawodowo leczeniem lub świadczeniem innych usług medycznych, zarządzania udzielaniem usług medycznych, jeśli tylko zapewnione są pełne gwarancje ochrony danych osobowych (art. 27 ust. 2 pkt 7 ustawy).

Dokumentacja medyczna, która zawiera dane identyfikujące pacjenta wraz z opisem stanu zdrowia pacjenta oraz udzielonych mu świadczeń zdrowotnych (art. 25 ustawy o prawach pacjenta) podlega zatem szczególnej ochronie, ze względu na przetwarzanie nie tylko „zwykłych" danych osobowych, lecz także danych wrażliwych.

IV. System Informacji Medycznej

System Informacji Medycznej (SIM), zgodnie z definicją zawartą w art. 10 ustawy o systemie informacji w ochronie zdrowia, jest to system teleinformatyczny, który umożliwia przetwarzanie danych dotyczących świadczeń zdrowotnych. Informacje te udostępniane są przez systemy teleinformatyczne usługodawców zapewniających świadczenia zdrowotne. Upraszczając można powiedzieć, że system informacji medycznej zapewnia udostępnianie i przetwarzanie Elektronicznej Dokumentacji Medycznej.

Każdy system informatyczny, w którym przetwarzane są dane, aby był systemem wiarygodnym dla użytkowników wymaga zapewnienia co najmniej czterech podstawowych cech: poufności, integralności, uwierzytelnienia i niezaprzeczalności. Poufność ma gwarantować, że dostęp do danych jest możliwy wyłącznie dla osoby uprawnionej; uwierzytelnienie, że tożsamość osób uzyskujących dostęp do systemu i dokonujących w nim jakichkolwiek czynności jest potwierdzona, niezaprzeczalność zaś oznacza, że nikt, kto dokonał jakiejś czynności w systemie nie może temu zaprzeczyć. Bezwzględnie jedną z najbardziej fundamentalnych cech funkcji bezpieczeństwa gwarantujących wiarygodność danych w systemie informatycznym jest integralność, która gwarantuje nienaruszalność przetwarzanych danych, tzn. zapewnia, że dane nie zostały w żadnym momencie zmienione w sposób nieuprawniony, a jeśli została podjęta próba ingerencji w ich treść, to fakt ten zostanie natychmiast wykryty.

Systemy teleinformatyczne, w których prowadzona jest Elektroniczna Dokumentacja Medyczna muszą spełniać warunki, określone w rozporządzeniu Ministra Zdrowia z dnia 9 listopada 2015 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania (Dz.U. 2015, poz. 2069). Paragraf 80 tego rozporządzenia[7] wymaga od systemu teleinformatycznego zapewnienia m.in.: zabezpieczenia dokumentacji przed jej uszkodzeniem lub utratą, integralności treści dokumentacji, stałego i autoryzowanego dostępu do dokumentacji dla osób uprawnionych oraz zabezpieczenia przed dostępem osób nieuprawnionych. Kolejne przepisy tego rozporządzenia (§§ 82, 83 i 86)[8] określają warunki utrwalania, udostępniania i zabezpieczania

[7] Odpowiednio: § 61 rozporządzenia Ministra Spraw Wewnętrznych i Administracji w sprawie rodzajów, zakresu i wzorów oraz sposobu przetwarzania dokumentacji medycznej w podmiotach leczniczych utworzonych przez ministra właściwego do spraw wewnętrznych oraz § 51 rozporządzenia Ministra Sprawiedliwości w sprawie rodzajów i zakresu dokumentacji medycznej prowadzonej w podmiotach leczniczych dla osób pozbawionych wolności oraz sposobu jej przetwarzania.

[8] Odpowiednio: §§ 63, 64 i 67 rozporządzenia Ministra Spraw Wewnętrznych i Administracji w sprawie rodzajów, zakresu i wzorów oraz sposobu przetwarzania dokumentacji medycznej w podmiotach leczniczych utworzonych przez ministra właściwego do spraw wewnętrznych oraz

Elektronicznej Dokumentacji Medycznej (integralność, poufność, uwierzytelnienie, niezaprzeczalność). Format Elektronicznej Dokumentacji Medycznej przetwarzanej i udostępnianej w Systemie Informacji Medycznej, warunki organizacyjno-techniczne jej przetwarzania, udostępniania, autoryzacji i zabezpieczenia uregulowane są w rozporządzeniu Ministra Zdrowia z dnia 28 marca 2013 r. w sprawie wymagań dla Systemu Informacji Medycznej (Dz.U. 2013, poz. 463).

W ostatnich latach rozwijany jest projekt *Elektronicznej Platformy Gromadzenia, Analizy i Udostępniania zasobów cyfrowych o Zdarzeniach Medycznych* (Platforma P1). Platforma P1 projektowana jest jako zespół systemów informatycznych, mających na celu usprawnienie procesów planowania i realizacji świadczeń zdrowotnych, monitorowanie ich realizacji, zapewnienie dostępu do informacji o udzielanych świadczeniach oraz publikowanie informacji w obszarze ochrony zdrowia (CSIOZ, http). Celem wdrażanych rozwiązań jest umożliwienie tworzenia, gromadzenia i analizy informacji o zdarzeniach medycznych[9]. Platforma P1 ma zarządzać m.in. dostępem do Elektronicznej Dokumentacji Medycznej, systemu e-skierowań oraz systemu e-recept.

V. Elektroniczna Dokumentacja Medyczna w praktyce

Od grudnia 2015 r. możliwe jest świadczenie usług medycznych na odległość. Dotychczas nie rozwiązano jednak problemów związanych z ochroną danych medycznych, będących specjalną kategorią danych osobowych (tzw. dane wrażliwe). Ośrodki opieki zdrowotnej powinny je właściwie zabezpieczać, archiwizować, a także zapewnić bezpieczne ich przekazywanie drogą elektroniczną. Prowadzenie pełnej dokumentacji medycznej w formie elektronicznej niezbędne jest do świadczenia usług telemedycznych (Kucharczyk, 2016). Jednak w dalszym ciągu dokumentacja medyczna w Polsce jest prowadzona głównie w formie papierowej. Niewiele ośrodków medycznych prowadzi ją w formie elektronicznej, choć prowadzenie dokumentacji medycznej w formie innej niż elektroniczna (tzn. w formie papierowej), zgodnie z art. 56 ustawy o systemie informacji w ochronie zdrowia możliwe jest jedynie do 31 grudnia 2017 r. Pierwotnym terminem wprowadzenia wyłącznie formy elektronicznej prowadzenia dokumentacji medycznej był 1 sierpnia 2014 r. Termin ten przesunięto do dnia 1 sierpnia 2017 r. Obecnie obowiązujący termin 1 stycznia 2018 r. wprowadzono nowelizacją z 9 października 2015 r. (Dz.U. 2015, poz. 1991). Niestety zapowiedzi Ministerstwa Zdrowia wskazują, że termin wprowadzenia obowiązku prowadzenia dokumentacji medycznej wyłącznie w formie elektronicznej zostanie najprawdopodobniej przesunięty raz jeszcze – ze względu na brak wystarczającego przygotowania podmiotów ochrony zdrowia do tej zmiany. Ostatecznie, wprowadzenie w życie tego obowiązku ma zagwarantować zwiększenie sprawności, polepszenie i przyspieszenie dostępu do danych medycznych świadczeniodawcom, jak i świadczeniobiorcom (NIK, 2016). Jednakże dostęp z każdego miejsca do danych medycznych, będących danymi wrażliwymi, wymaga odpowiedniego zabezpieczenia tej dokumentacji, tak aby dane pacjentów nie były ujawniane w sposób niezgodny z prawem. Warto przy tym podkreślić, że dokumentacja medyczna prowadzona w tradycyjnej, papierowej formie

§§ 53,54 i 57 rozporządzenia Ministra Sprawiedliwości w sprawie rodzajów i zakresu dokumentacji medycznej prowadzonej w podmiotach leczniczych dla osób pozbawionych wolności oraz sposobu jej przetwarzania.

[9] Art. 2 pkt 18 ustawy o systemie informacji w ochronie zdrowia definiuje zdarzenie medyczne przetwarzane w systemie informacji jako czynność w ramach świadczenia zdrowotnego (działanie służące profilaktyce, zachowaniu, ratowaniu, przywracaniu lub poprawie zdrowia oraz inne działanie medyczne wynikające z procesu leczenia) lub świadczenia zdrowotnego rzeczowego (związane z procesem leczenia leki, środki spożywcze specjalnego przeznaczenia żywieniowego i wyroby medyczne), o których mowa w art. 5 odpowiednio pkt 40 i 37 ustawy z dnia 27.08.2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych.

również musi być zabezpieczana. Kontrola przeprowadzona przez NIK wykazała, że blisko 46% spośród kontrolowanych świadczeniodawców nie przestrzega procedur dotyczących zabezpieczenia dokumentacji medycznej pacjentów. Dokumentacja ta mogła ulec zniszczeniu, uszkodzeniu lub zagubieniu. Możliwy był również dostęp do niej nieuprawnionych osób trzecich. Kontrola wykazała także zagrożenia wynikające z braku szczegółowych regulacji prawnych dotyczących prawidłowego udostępniania dokumentacji medycznej. Te podmioty, które prowadziły dokumentację medyczną w postaci elektronicznej wyeliminowały pewne uchybienia związane z dokumentacją. Siłą rzeczy wpisy były czytelne i kompletne. Jednak stan zaawansowania przygotowań podmiotów do wprowadzenia obowiązku prowadzenia dokumentacji medycznej pacjentów wyłącznie w formie elektronicznej nie zapewnia, w ocenie NIK, realności spełnienia tego obowiązku do końca 2017 r. (NIK, 2016).

VI. Informatyzacja ochrony zdrowia

Centrum Systemów Informacyjnych Ochrony Zdrowia (CSIOZ), na przełomie lipca i sierpnia 2016 r., przeprowadziło badanie ankietowe podmiotów opieki zdrowotnej dotyczące stopnia zaawansowania prac mających na celu dostosowanie tych podmiotów do prowadzenia i wymiany dokumentacji medycznej pacjentów w postaci elektronicznej oraz rozwoju usług telemedycznych. Celem ankiety była ocena poziomu implementacji rozwiązań informatycznych w jednostkach wykonujących działalność leczniczą. W tabeli 1 przedstawiono wybrane wskaźniki, dotyczące poziomu informatyzacji, w tym szczególnie bezpieczeństwa teleinformatycznego szpitali i zakładów udzielających ambulatoryjnych świadczeń zdrowotnych (AŚZ), dla których to podmiotów badanie ankietowe uznano za reprezentatywne.

Przytoczone w tabeli 1 wyniki pokazują, że podmioty lecznicze nie są przygotowane w wystarczającym stopniu do prowadzenia dokumentacji medycznej w formie elektronicznej. Technologie informacyjno-komunikacyjne nie są wykorzystywane w większości placówek ochrony zdrowia. Chociaż prawie wszystkie ankietowane szpitale (blisko 98%) deklarują posiadanie i bieżące aktualizowanie strony www, to tylko niecałe 46% tych placówek udostępnia pacjentom możliwość e-rejestracji, a już jedynie 41% dysponuje rozwiązaniami informatycznymi umożliwiającymi prowadzenie EDM. Jeśli chodzi o zakłady udzielające ambulatoryjnych świadczeń zdrowotnych, to poziom informatyzacji jest jeszcze niższy. Tylko niespełna 60% tych podmiotów posiada stronę www, 35% ma rozwiązania informatyczne pozwalające na prowadzenie dokumentacji medycznej w formie elektronicznej, a usługę e-rejestracji umożliwia tylko ok. 20%. Możliwość posiadania internetowego konta pacjenta istnieje w blisko 37% szpitali i około 5% AŚZ-ów. W obu typach placówek tylko po ok. 15% umożliwia pacjentom dostęp do wyników ich badań online. Dokumentację medyczną w formie elektronicznej, dostępną właściwie z każdego miejsca i w każdym momencie, zapewnia zaledwie 7% szpitali i blisko 3% AŚZ-ów. Z punktu widzenia zapewnienia kontynuacji leczenia i zmniejszenia kosztów świadczenia usług opieki zdrowotnej, ważnym udogodnieniem jest zapewnienie możliwości wymiany pomiędzy placówkami ochrony zdrowia np. wyników badań pacjentów. Niestety niewiele podmiotów deklaruje występowanie takiej funkcjonalności – jest to tylko blisko 24% szpitali i blisko 15% AŚZ-ów. Co więcej, większość podmiotów ochrony zdrowia (ponad 90% AŚZ-ów i ponad 72% szpitali) deklaruje brak stosowania jakichkolwiek (międzynarodowych lub krajowych) standardów EDM. Placówki ochrony zdrowia nie są kompatybilne. Podmioty

wypełniają dokumenty medyczne jak chcą, w nieustalony między sobą sposób. Powyższe statystyki pokazują, że jedynie niewielka liczba placówek ochrony zdrowia jest przygotowana do informatyzacji. Poziom zaawansowania implementacji rozwiązań informatycznych jest bardzo niski. A nawet jeśli konkretne podmioty są zinformatyzowane to trudno im się miedzy sobą komunikować. Widać przykłady informatyzacji pionowej, natomiast brak jest harmonizacji, co z punktu widzenia zapewnienia koordynowanej opieki medycznej nie jest sytuacją pożądaną.

Tabela 1. Poziom informatyzacji podmiotów opieki zdrowotnej (w %)

Działanie	Szpitale	Zakłady udzielające ambulatoryjnych świadczeń zdrowotnych (AŚZ)
Posiadanie i aktualizowanie strony www	97,71	59,68
Posiadanie rozwiązań informatycznych pozwalających na prowadzenie EDM	41,31	35,02
E-rejestracja	45,58	20,48
Internetowe konto pacjenta	36,89	5,37
Dostęp dla pacjentów do wyników badań online	15,55	15,04
Dostęp dla pacjentów do dokumentacji medycznej online	7,01	2,82
Usługi elektroniczne dedykowane innym podmiotom (np. wymiana wyników)	23,78	14,78
Stosowanie międzynarodowych lub krajowych standardów EDM	27,74	9,38
Posiadanie opracowanej i wdrożonej wewnętrznej polityki bezpieczeństwa teleinformatycznego	82,01	56,30
Identyfikacja incydentów związanych z nieuprawionym dostępem do jednostkowych danych medycznych w ciągu roku	0,91	0,20
Wystąpienie istotnych awarii systemów informatycznych skutkujących utratą jednostkowych danych medycznych w ciągu roku	3,05	0,80
Stosowanie jakiejkolwiek metody autoryzacji EDM	91,31	82,97
Posiadanie systemu informatycznego służącego do długoterminowego przechowywania EDM zapewniającego jej integralność i wiarygodność	54,27	39,66
Posiadanie modułu archiwum przez system teleinformatyczny do prowadzenia dokumentacji medycznej w formie elektronicznej	27,13	19,18
Wykonywanie kopii bezpieczeństwa EDM na zewnętrznym nośniku danych	45,45	33,63
Posiadanie repozytorium EDM	27,90	10,47

Źródło: opracowanie własne na podstawie: CSIOZ, 2016.

Jeśli chodzi o wdrożenie wewnętrznej polityki bezpieczeństwa teleinformatycznego, to w przypadku szpitali sytuacja przedstawia się dużo lepiej, niż w przypadku zakładów udzielających świadczeń zdrowotnych ambulatoryjnie. Ponad 82% szpitali, ale już tylko ponad 56% AŚZ-ów, deklaruje posiadanie i wdrożenie takiej polityki. Oznacza to, że przetwarzanie dokumentacji medycznej w systemach informatycznych zapewnia podstawowe atrybuty bezpieczeństwa, czyli poufność danych, ich dostępność i integralność (CSIOZ, 2016a). W ciągu roku, mimo braku implementacji takich rozwiązań we wszystkich podmiotach udzielających świadczeń opieki zdrowotnej, zaobserwowano jedynie odosobnione incydenty polegające na nieuprawnionym dostępie do jednostkowych danych medycznych. Incydenty te polegały na próbach skanowania portów, a także infekowania złośliwym oprogramowaniem (*ransomware*), najczęściej z wykorzystaniem e-maili. Wystąpiły one w niecałym 1% szpitali i 0,2% AŚZ-ów. Praktycznie brak było również istotnych awarii systemów informatycznych, skutkujących utratą jednostkowych danych medycznych. Wystąpiły one jedynie w blisko 1% ankietowanych AŚZ-ów i w ponad 3% szpitali. Awarie te spowodowane były m.in. uszkodzeniami dysku twardego lub baz danych, czy awarią sprzętową serwera bazy danych (CSIOZ, 2016).

Ankietowane przez CSIOZ placówki ochrony zdrowia deklarują w większości przypadków (ponad 91% szpitali i blisko 83% AŚZ-ów) stosowanie autoryzacji dokumentów medycznych występujących w formie elektronicznej. Najczęściej podmioty (odpowiednio 64% wskazań szpitali i 45% AŚZ-ów w stosunku do wszystkich używanych metod) deklarują dokonywanie autoryzacji elektronicznych dokumentów medycznych jedynie przez uwierzytelnienie użytkownika w lokalnym systemie informatycznym. Szpitale wskazywały również jako metodę autoryzacji: uwierzytelnienie użytkownika w lokalnym systemie informatycznym za pomocą indywidualnego certyfikatu pracownika oraz hasła, jak również kwalifikowany podpis elektroniczny. W jednostkowych przypadkach wymieniano również: podpis elektroniczny potwierdzony profilem zaufanym ePUAP, indywidualne certyfikaty wydawane z lokalnego/regionalnego centrum certyfikacji czy uwierzytelnienie użytkownika w systemie bankowości elektronicznej. W przypadku AŚZ-ów, jako drugą najczęściej wykorzystywaną metodę autoryzacji, wskazywano podpis elektroniczny potwierdzony zaufanym profilem ePUAP (CSIOZ, 2016). Zdecydowana większość placówek prowadzi rekordy w systemie, ale trudno jest uznać to za dokumentację medyczną prowadzoną zgodnie z wymogami ustawowymi (Parlamentarny zespół ds. Cyfryzacji Szpitali i Placówek Medycznych, posiedzenie z 1 grudnia 2016).

W momencie wprowadzenia obowiązku prowadzenia dokumentacji medycznej pacjentów wyłącznie w postaci elektronicznej placówki ochrony zdrowia będą musiały posiadać rozwiązania informatyczne pozwalające na przechowywanie dokumentacji medycznej w sposób zapewniający jej integralność i wiarygodność. Zgodnie z wynikami przeprowadzonej przez CSIOZ ankiety, tylko ok. 54% szpitali i jedynie blisko 40% AŚZ-ów deklaruje posiadanie takich rozwiązań. Tylko ok. 27% szpitali i 19% AŚZ-ów posiada system teleinformatyczny do prowadzenia elektronicznej dokumentacji medycznej wyposażony w moduł archiwum dla tejże dokumentacji. Wśród ankietowanych, w ponad 43% szpitali i ponad 33% AŚZ-ów wykonywana jest na zewnętrznych nośnikach kopia bezpieczeństwa elektronicznej dokumentacji medycznej. Jeśli chodzi o przechowywanie dokumentacji medycznej w sposób pozwalający na jej przeszukiwanie, czyli posiadanie przez placówki ochrony zdrowia repozytorium elektronicznej dokumentacji medycznej, to tylko blisko 28% szpitali i ponad 10% AŚZ-ów deklaruje implementowanie takich rozwiązań.

VII. Podsumowanie

Implementowanie technologii informacyjno-komunikacyjnych w sektorze ochrony zdrowia w Polsce jest koniecznością. Obowiązek ten wynika nie tylko z przepisów prawa, które wcześniej czy później będzie m.in. obligowało świadczeniodawców do prowadzenia dokumentacji medycznej jedynie w formie elektronicznej. Jest on również immanentnie związany z postępem technicznym. Wprowadzane są nowe, coraz bardziej innowacyjne metody leczenia pacjentów. Z początku rozwiązania pionierskie mogą z czasem stać się rozwiązaniami wprowadzanymi w codziennej praktyce lekarskiej.

Implementacja Internetu Rzeczy w ochronie zdrowia wymaga przekonania świadczeniodawców do stosowania rozwiązań pozwalających na usprawnienie świadczenia usług z zakresu opieki zdrowotnej, ale również świadczeniobiorców, którzy muszą być przekonani, że ich dane medyczne nie będą wykorzystywane niezgodnie z przeznaczeniem lub wręcz na szkodę pacjenta, np. przez wykorzystywanie ich przez firmy ubezpieczeniowe w celu zwiększenia składki. Wraz z wdrażaniem urządzeń technicznych monitorujących np. stan zdrowia pacjentów pozostających we własnych domach, bezpieczeństwo świadczeniobiorców wzrasta. Jednak w tym samym czasie ich prywatność może być zagrożona. Dane z urządzeń monitorujących na odległość stan zdrowia pacjentów mogą stać się np. celem ataków hakerskich. Zagrożenia mogą dotyczyć nie tylko stricte prywatności, lecz także przybierać nawet groźniejsze formy, np. przez uzyskanie możliwości kontrolowania rozrusznika serca oraz implantów bazujących na wykorzystaniu IoT.

Rozwój technologii i medycyny, a także zmiany demograficzne (starzenie się społeczeństw) powodują, że technologie informacyjno-komunikacyjne są w coraz większym zakresie wykorzystywane, również w sektorze opieki zdrowotnej. Zapewnienie prywatności pacjentom i zagwarantowanie bezpieczeństwa ich danych medycznych jest niezbędne. Zdarzają się i będą się zdarzać incydenty polegające na włamaniach do baz zawierających dane pacjentów. Należy jednak w taki sposób zabezpieczać te dane oraz tak tworzyć i egzekwować prawo, aby były to jednostkowe, mało znaczące przypadki.

Bibliografia

5 przykładów wykorzystania Internetu Rzeczy w medycynie. Pozyskano z: https://apollogic.com/pl/2016/07/5--przykladow-internetu-rzeczy-ktore-moga-polepszyc-zdrowie/ (15.05.2017).

Bangemann, M. (1994). *Bangemann's Report*. Pozyskano z: http://ec.europa.eu/archives/ISPO/infosoc/backg/bangeman.html (1.06.2017).

Barta, J., Fajgielski, P. i Markiewicz, R. (2015). *Ochrona danych osobowych. Komentarz*, Warszawa: Wolters Kluwer Polska.

CSIOZ (2016). *Wyniki II edycji badania ankietowego 2016 r. „Badanie stopnia przygotowania podmiotów wykonujących działalność leczniczą do obowiązków wynikających z ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia"*, Warszawa.

CSIOZ (2016a). *Wyjaśnienia do artykułu dotyczącego zabezpieczenia danych medycznych pacjentów, gromadzonych w postaci elektronicznej*. Pozyskano z: https://www.csioz.gov.pl/aktualnosci/szczegoly/wyjasnienia-do-artykulu-dotyczacego-zabezpieczania-danych-medycznych-pacjentow-gromadzonych-w-p/ (9.06.2017).

CSIOZ, *Projekt P1*. Pozyskano z: https://www.csioz.gov.pl/projekty/realizowane/projekt-p1/ (9.06.2017).

COMARCH (2017). *NOMED*. Pozyskano z: http://www.comarch.pl/healthcare/produkty/zdalna-opieka-medyczna/zdalna-opieka-kardiologiczna/nomed/ (28.04.2017).

Hofmański, P. (1997). *Komentarz do wybranych przepisów Europejskiej Konwencji o ochronie Praw Człowieka i Podstawowych Wolności*. W: *Standardy prawne Rady Europy*, *Teksty i Komentarze*, T. III. Warszawa: Oficyna Naukowa.

Kucharczyk, B. (2016). Siedem barier rozwoju telemedycyny, *Rzeczpospolita*, 15 listopada.

Maurer, T. (2011). *Cyber Norm Emergence at the United Nations – an Analysis of the Acivities at the UN Regarding Cyber-Security*. W: *Science, Technology, and Public Policy Program Explorations in Cyber International Relations Project*, *Discussion Paper #211-11 Explorations in Cyber International Relations Discussion Paper Series*, Harvard Kennedy School, Belfer Center for Science and International Affairs.

NIK. (2016). *Informacja o wynikach kontroli Tworzenie i udostępnianie dokumentacji medycznej*. Warszawa.

SAS Institute. *Co to jest Internet Rzeczy*. Pozyskano z https://www.sas.com/pl_pl/insights/internet-of-things.html?gclid=CNH8gNLLodQCFUW1GAodoBwFWA (08.06.2017).

Słownik pojęć Strategii Rozwoju Transportu (Załącznik do Strategii Rozwoju Transportu do 2020 roku z perspektywą do 2030 roku). Pozyskano z http://mib.gov.pl/media/3510/Slownik_pojec_SRT.pdf (9.06.2017).