Dr Artur Romaszewski
Uniwersytet Jagielloński - Collegium Medicum
Wydział Nauk o Zdrowiu, Zakład Medycznych Systemów Informacyjnych
artur.romaszewski@uj.edu.pl

Mgr Krzysztof Gajda
Uniwersytet Jagielloński - Collegium Medicum
Wydział Nauk o Zdrowiu, Zakład Medycznych Systemów Informacyjnych
krzysztof.gajda@uj.edu.pl

Mgr Mariusz Kielar
Uniwersytet Jagielloński - Collegium Medicum
Wydział Nauk o Zdrowiu, Zakład Medycznych Systemów Informacyjnych
mariusz.kielar@uj.edu.pl

Dr hab. Wojciech Trąbka
Krakowska Akademia im. Andrzeja Frycza Modrzewskiego
Wydział Lekarski i Nauk o Zdrowiu, Katedra Bioinformatyki i Zdrowia Publicznego
wojciech.trabka@uj.edu.pl

NOWE TECHNOLOGIE - PROPONOWANE ROZWIĄZANIA INSTYTUCJONALNE I PROGRAMOWE W OCHRONIE DANYCH MEDYCZNYCH

Wprowadzenie

W artykule omówiono wpływ niektórych nowych rozwiązań technologicznych na problem bezpieczeństwa i poufności danych medycznych oraz przedstawiono możliwe rozwiązania instytucjonalne i programowe wspierające instytucje opieki zdrowotnej w zapewnieniu, zgodnie z nowymi regulacjami, odpowiedniego poziomu zabezpieczenia danych medycznych.

Urządzenia monitorujące parametry życiowe pacjentów i wiele innych rozwiązań telemedycznych generują ogromne ilości danych medycznych podlegających ochronie. Tajemnice przedsiębiorstwa oraz tajemnica telekomunikacyjna mogą stanowić pewien system zabezpieczeń. W artykule omówiono zasady budowy systemów informatycznych: *privacy by design* i *privacy by default* , nowe rozporządzenie *e-privacy* oraz kodeksy postepowania, jako elementy służące poprawie bezpieczeństwa danych medycznych. Przedstawiono także rolę oceny ryzyk oraz audytu oprogramowania w jednostkach opieki zdrowotnej w aspekcie bezpieczeństwa danych osobowych.

1. Urządzenia medyczne – Internet rzeczy a system bezpieczeństwa danych

System bezpieczeństwa danych w ochronie zdrowia musi uwzględniać bezpieczeństwo wszelkiego rodzaju urządzeń niezbędnych do funkcjonowania nowoczesnych podmiotów ochrony zdrowia i często skomunikowanych ze sobą za pośrednictwem sieci *Wi-Fi*. Tego typu systemy często wchodzą w skład tzw. Internetu rzeczy (przedmiotów). Pod tym pojęciem należy rozumieć rozwiązania służące do zdobywania informacji, przetwarzania informacji i automatycznego dzielenia się informacjami pochodzącymi z różnych zasobów (z sensorów, z urządzeń, które nosimy ze sobą oraz z maszyn)[1].

W ochronie zdrowia przykłady urządzeń wspierających procesy leczenia pacjenta i jednocześnie wymieniających się danymi są liczne. Wśród nich można wskazać systemy zdalnego systemu monitorowania parametrów życiowych pacjenta z wykorzystaniem medycznego sprzętu pomiarowego i transmisji danych przez Internet (audio lub wideo). Są to m.in. systemy służące do monitorowania parametrów życiowych: ciśnienia tętniczego, częstości pracy serca, saturacji tlenem, temperatury ciała, pojemności wydechowej (pojemność płuc) i poziomu glukozy we krwi. Zebrane dane przekazywane są lekarzowi.

Ciekawym rozwiązaniem może być zastosowanie silikonowych mikroczujników zamontowanych w tabletkach pozwalających na monitorowanie przyjmowania przez pacjentów przepisanych leków. Nowe rozwiązania to również wszczepianie programowalnego bionanochipa (*programable-bio-nano-chip*), który może wykrywać choroby serca lub markery nowotworowe z próbki śliny pacjenta. Wszczepienie takiego chipa do ciała pacjenta mogłoby zapewnić system wczesnego powiadamiania o tych chorobach, na długo przed odkryciem jakichkolwiek symptomów przez pacjenta[2].

Większość z tych skomplikowanych urządzeń jednocześnie przetwarza dane osobowe i komunikuje się z serwerami wykorzystywanymi nie tylko przez lekarza, ale również przez producenta lub dystrybutora. Pojawia się problem odpowiedzi na pytanie o ich właściwego administratora danych.

W przypadku Internetu rzeczy mamy do czynienia z wyraźnym rozróżnieniem według następujących kryteriów:

[1] K. Chylińska, *Zastępca Europejskiego Inspektora Ochrony Danych Osobowych: Nowe technologie – Internet rzeczy*, http://blog.e-odo.pl/2015/10/17/nowe-technologie-internet-rzeczy/ (dostęp 04.2018).

[2] E. Kwiatkowska, *Rozwój Internetu rzeczy – szanse i zagrożenia*, http://www.wz.uw.edu.pl/pracownicyFiles/id26574-6.0_Rozw%C3%B3j_internetu_rzeczy_-_szanse_i_zagro%C5%BCenia%5B1%5D.pdf (dostęp 04.2018).

- kto stworzył system;
- kto stworzył urządzenia;
- kto zarządza informacją;
- kto jest użytkownikiem.

Grupa Robocza Artykułu 29 będąca ciałem doradczym dla instytucji Unii Europejskiej[3] wydała opinię[4] poświęconą technologii Internetu rzeczy. W dokumencie tym przyznano, że dane wygenerowane przez urządzenia tworzące Internet rzeczy mogą stanowić dane osobowe. Producenci tego typu urządzeń i oprogramowania, co do zasady, mogą zostać uznani za administratorów danych osobowych. Wobec tego będą na nich nałożone obowiązki wynikające z unijnych i krajowych przepisów o ochronie danych osobowych. Natomiast użytkownicy Internetu Rzeczy powinni być informowani o tym, kto przetwarza ich dane. Powinni również wyrazić zgodę na takie przetwarzanie, kiedy wymagają tego przepisy.

W przedmiotowej opinii zwraca się również uwagę na problemy technologiczne urządzeń. Większość czujników obecnych dziś na rynku nie jest w stanie wykorzystać zaszyfrowane łącze do komunikacji, ponieważ wymagania obliczeniowe mają wpływ na wydajność urządzenia ograniczoną przez baterie o małej mocy.

W opinii zwraca się szczególną uwagę na to, by osoby, których czynności zdrowotne są monitorowane, musiały wyrazić na to zgodę. Wskazuje się, że urządzenia rejestrujące np. *Quantified Self*[5] rejestrują głównie dane dotyczące dobrostanu jednostki. Te dane niekoniecznie stanowią dane dotyczące zdrowia jako takie, ale mogą szybko dostarczyć informacji na temat zdrowia jednostki z uwagi na ich rejestrację w czasie rzeczywistym. Umożliwia to wyciągnięcie wniosków na temat jego zmienności w danym okresie. Administratorzy danych powinni przewidywać tę możliwą zmianę kwalifikacji i podjąć odpowiednie działania.

Ataki hakerskie na urządzenia wykorzystywane w diagnostyce oraz w urządzeniach do podtrzymywania życia umożliwiają nie tylko kradzież zebranych danych i ewentualną ich sprzedaż, ale również sterowanie takimi maszynami. Będzie to szczególnym zagrożeniem dla zaawansowanych urządzeń, którym powierzone jest bezpieczeństwo ludzi. Należy zatem

[3] Powołana na mocy Dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 2 października 1995 r.
[4] *Opinia 8/2014 w sprawie ostatnich postępów w dziedzinie Internetu Przedmiotów (WP 223) Grupy Roboczej art. 29*, https://giodo.gov.pl/pl/1520203/8646.
[5] Znany również jako *lifelogging*, to specyficzny ruch Gary Wolfa i Kevina Kelly'ego z magazynu „Wired", który rozpoczął się w 2007 r. i próbuje włączyć technologię do gromadzenia danych dotyczących aspektów codziennego życia danej osoby. Ludzie zbierają dane dotyczące spożywanej żywności, jakości otaczającego powietrza, nastroju, przewodnictwa skóry jako wskaźnika pobudzenia, pulsoksymetrii dla poziomu tlenu we krwi i wydajności, zarówno umysłowej, jak i fizycznej. Wolf opisał ilościowe „ja" jako „samoświadomość poprzez samośledzenie za pomocą technologii".

zaopatrzyć je w zabezpieczenia uniemożliwiające włamanie i zapewnić szyfrowanie przepływających danych. Kwestią budzącą wątpliwości prawne jest również to, kto ma mieć prawa do danych wygenerowanych przez czujniki, skoro mogą one stanowić atrakcyjny produkt na rynku. Prawa do takich danych rościć może zarówno użytkownik Internetu Rzeczy, właściciel platformy zbierającej dane, jak i producent urządzenia[6].

2. Tajemnica przedsiębiorstwa

Przez tajemnicę przedsiębiorstwa rozumie się „nieujawnione do wiadomości publicznej informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, co, do których przedsiębiorca podjął niezbędne działania w celu zachowania ich poufności[7].” Wiąże ona zarówno pracowników, osoby świadczące usługi na postawie umów cywilnoprawnych jak i instytucje sprawujące kontrolę. Nowa definicja tajemnicy przedsiębiorstwa została zamieszczona w przepisach prawa UE[8] co w niedługim czasie spowoduje zmiany przedstawione powyżej definicji. Zgodnie z nowym brzmieniem przez tajemnicę przedsiębiorstwa należy rozumieć informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, które jako całość lub w szczególnym zestawieniu i zbiorze ich elementów nie są powszechnie znane osobom zwykle zajmującym się tym rodzajem informacji albo nie są łatwo dostępne dla takich osób, o ile uprawniony do korzystania z informacji lub rozporządzania nimi podjął, przy zachowaniu należytej staranności, działania w celu utrzymania ich w poufności[9].

Wyjawienie tajemnicy prowadzić może również do odpowiedzialności karnej naruszyciela w sytuacji, gdy takie wyjawienie wyrządza poważną szkodę przedsiębiorcy, a naruszyciel wyjawia informację wbrew ciążącemu na nim w stosunku do przedsiębiorcy obowiązkowi. Odpowiedzialności karnej podlega także osoba, która uzyskała bezprawnie

[6] D. Koseła, *Internet Rzeczy – rewolucja technologiczna i nowe wyzwania dla prawników*, http://bpcc.org.pl/pl/publikacje/internet-rzeczy-rewolucja-technologiczna-i-nowe-wyzwania-dla-prawnikow (dostęp 04.2018).
[7] Art. 11 ust 4. Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 9 lutego 2018 r. w sprawie ogłoszenia jednolitego tekstu ustawy o zwalczaniu nieuczciwej konkurencji Dz.U. 2018 poz. 419.
[8] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/943 z dnia 8 czerwca 2016 r. w sprawie ochrony niejawnego know-how i niejawnych informacji handlowych (tajemnic przedsiębiorstwa) przed ich bezprawnym pozyskiwaniem, wykorzystywaniem i ujawnianiem (Dz. Urz. UE L 157 z 15.06.2016, s. 1).
[9] 9 czerwca 2018 roku upływa termin wdrożenia w Polsce dyrektywy UE 2016/943 w sprawie ochrony niejawnego know-how i niejawnych informacji handlowych (tajemnic przedsiębiorstwa) przed ich bezprawnym pozyskiwaniem, wykorzystywaniem i ujawnianiem.

informację stanowiącą tajemnicę przedsiębiorstwa i ujawniła ją innej osobie lub wykorzystała we własnej działalności gospodarczej.

Najpopularniejszymi regulacjami tajemnicy przedsiębiorstwa są regulaminy wewnętrzne, umowy zachowania poufności i klauzule konkurencyjne. Zwykle przy podjęciu pracy wraz z umową pracownik podpisuje regulamin, który wyraźnie określa zasady w firmie - również dotyczące postępowania z informacjami. Zapisy w regulaminie obligują pracownika do ich stosowania. Poza nimi przedsiębiorcy decydują się na przedkładanie innych form zabezpieczenia tajemnicy przedsiębiorstwa[10].

Problem tajemnicy informacji dotyczących danych pacjentów znajduje się w wielu regulacjach odnoszących się do obszarów ochrony zdrowia, regulowanych oddzielnymi aktami prawnymi np. zdrowie psychiczne, medycyna pracy.

Ponadto w ochronie zdrowia funkcjonują tajemnice związane z funkcjonowaniem konkretnych instytucji. Przykładem jest tajemnica EWUŚ[11]. Dane o stanie zdrowia są również chronione tajemnicą statystyczną, tajemnicą pracowników socjalnych oraz innymi tajemnicami związanymi z innymi działalnościami, które mogą na podstawie przepisów prawa przetwarzać dane o stanie zdrowia.

3. Tajemnica telekomunikacyjna

Istnieją obszary, na które bezpośrednio nie mają wpływu osoby odpowiedzialne za zapewnienie bezpieczeństwa danych w instytucji ochrony zdrowia. Każdy dokument elektroniczny, w tym zawierający dane o stanie zdrowia pacjenta, który zostaje przekazywany do innych podmiotów za pośrednictwem sieci teleinformatycznych może być kontrolowany przez podmiot, który go stworzył tylko do momentu, kiedy znajduje się w jego systemie. Jeżeli przekazuje się go do innych podmiotów np. za pośrednictwem e-mail to w czasie ich wysyłania proces może kontrolować tylko operator sieci i inne instytucje upoważnione do tego prawem. Podmioty te objęte są tajemnicą telekomunikacyjną.

Obejmuje ona swym zakresem m.in:

1) dane dotyczące użytkownika;

2) treść indywidualnych komunikatów;

[10] *Tajemnica przedsiębiorstwa a zakaz konkurencji*, https://poradnikprzedsiebiorcy.pl/-tajemnica-przedsiebiorstwa-a-zakaz-konkurencji (dostęp 04.2018).

[11] § 3. 3 pkt 2 b Rozporządzenie Ministra Zdrowia z dnia 20 grudnia 2012 r. w sprawie warunków występowania o sporządzenie dokumentu elektronicznego potwierdzającego prawo do świadczeń opieki zdrowotnej Dz.U. 2012 poz. 1500.

3) dane transmisyjne, które oznaczają dane przetwarzane dla celów przekazywania komunikatów w sieciach telekomunikacyjnych, w tym dane lokalizacyjne, które oznaczają wszelkie dane przetwarzane w sieci telekomunikacyjnej wskazujące położenie geograficzne urządzenia końcowego użytkownika publicznie dostępnych usług telekomunikacyjnych.

Do zachowania tajemnicy telekomunikacyjnej są zobowiązane podmioty uczestniczące w wykonywaniu działalności telekomunikacyjnej w sieciach publicznych oraz podmioty z nim współpracujące. Podmioty, o których mowa powyżej, są zobowiązane również do zachowania należytej staranności, w zakresie uzasadnionym względami technicznymi lub ekonomicznymi, przy zabezpieczaniu urządzeń telekomunikacyjnych, sieci telekomunikacyjnych oraz zbiorów danych przed ujawnieniem tajemnicy telekomunikacyjnej. Jeżeli osoba korzystając z urządzenia radiowego lub końcowego, zapoznała się z komunikatem dla niej nieprzeznaczonym, posiada ona także obowiązek zachowania tajemnicy telekomunikacyjnej[12].

4. Tajemnica związana z kontrola podmiotu

Tajemnicą zostały również objęte podmioty dopuszczone prawnie do kontroli danych osobowych w podmiocie, w tym w podmiocie leczniczym. Minister Zdrowia w ramach przewidzianej prawem kontroli wykonuje ją za pośrednictwem osób objętych tajemnicą zawodową. Ograniczony w stosunku do danych objętych tajemnicami prawnie chronionymi został Prezes Urzędu Ochrony Danych Osobowych. Wprowadzono możliwość zastrzeżenia informacji, dokumentów lub ich części zawierających tajemnicę przedsiębiorstwa dostarczanych Prezesowi Urzędu przez stronę postępowania w sprawie naruszenia przepisów o ochronie danych osobowych. W takim przypadku strona jest obowiązana przedstawić Prezesowi Urzędu również wersję dokumentu niezawierającą informacji objętych zastrzeżeniem.

5. Zasady *privacy by design* oraz *privacy by default*

Z powyższym zagadnieniem wiążą się dwie zasady bezpieczeństwa przetwarzania danych osobowych zawarte w RODO - *privacy by design* (zasada prywatności w fazie projektowania) oraz *privacy by default* (zasadą prywatności w ustawieniach domyślnych). Pierwsza zasada oznacza, że ochrona danych, ma być wbudowywana na etapie projektowania

[12] Ustawa z 16.07.2004 r. – Prawo telekomunikacyjne (Dz.U. Nr 171, poz. 1800 ze zm.)

systemu (procedur, dokumentacji oraz sprzętu) do przetwarzania danych osobowych oraz samego procesu przetwarzania (*by design*). Tym samym zobowiązuje ona administratora danych do zapewnienia już na etapie projektowania systemu, aplikacji lub procesu oraz na etapie wykorzystywania ich do przetwarzania danych wprowadzania do nich odpowiednich środków technicznych i organizacyjnych, które zapewnią właściwą ochronę danych osobowych. W praktyce zasada ta oznacza przewidywanie i przeciwdziałanie możliwym problemom w zakresie ochrony danych jeszcze na etapie przygotowania konkretnych rozwiązań systemowych, z obowiązkiem udokumentowania swojego wyboru. W tym celu trzeba mieć na uwadze poniższe kryteria:

1. minimalizacja – ilość zbieranych danych jest ograniczona do niezbędnego minimum;
2. ukrywanie - dane i zależności między nimi nie są widoczne dla osób mających do nich dostęp (dodatkowe działanie w celu dostępu do danych);
3. separowanie - przetwarzanie danych rozdzielonych, rozproszonych w poszczególnych zbiorach;
4. agregowanie - dane przetwarzane w możliwie najwyższym stopniu agregowania[13].

Druga zasada wymaga, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia konkretnego celu przetwarzania. Innymi słowy, ochrona danych ma być aktywna domyślnie (*by default*) bez konieczności podejmowania działań przez osoby, których przetwarzane dane dotyczą. Zastosowane środki powinny gwarantować domyślność ustawień umożliwiających ochronę przetwarzanych danych osobowych. W praktyce zgodnie z tą zasadą udostępnienie danych osobowych niesprecyzowanej liczbie innych osób przez użytkownika aplikacji, systemu, programu, czy usługi jest możliwe wyłącznie za pomocą zmiany domyślnych ustawień przez użytkownika.

6. Kodeksy postępowania, jako możliwy wybór sytemu zabezpieczenia danych

Wraz z nowymi prawami i obowiązkami wprowadzanymi przez RODO w zakresie bezpieczeństwa przetwarzania danych osobowych, jednym z kluczowych aspektów jest dopuszczenie przyjmowania kodeksów postępowania przez zrzeszenia i inne podmioty reprezentujące określone kategorie administratorów lub podmioty przetwarzające (np. branża medyczna). Zapisy w nich zawarte są wyrazem polityki samoregulacji w danej branży,

[13] A. Wolanin, *Privacy by design - nowa zasada planowania przetwarzania*, https://www.rodokompas.ostrowski-legal.net/single-post/2018/01/22/privacybydesign (dostęp 04.2018).

aczkolwiek ze względu na formalne zatwierdzenie przez organ nadzorczy mają status prawny. Zatem w praktyce przestrzeganie np. przez placówkę medyczną zapisów takich dokumentów oznacza wywiązywanie się z obowiązków nałożonych przez RODO.

W praktyce zarządzający placówkami medycznymi otrzymują dokument umożliwiający dokonanie optymalnego wyboru w obszarze zabezpieczenia danych zgodnie z postanowieniami RODO. Wskazuje się w nim, w jaki techniczny i organizacyjny sposób dobrać zabezpieczenia w zależności od możliwości finansowych danego podmiotu. Mogą go stosować wszystkie podmioty wykonujące działalność leczniczą - bez znaczenia na formę prawną, strukturę właścicielską i organ założycielski oraz sposób udzielania świadczeń zdrowotnych (finansowanych ze środków publicznych, komercyjnie).

7. Rozporządzenie *e-Privacy*

RODO to jedyny akt prawny, który wpłynie na ochronę prywatności wszystkich osób, których dane są przetwarzane. Rozporządzenie *e-Privacy* ma uzupełnić przepisy RODO, a jednocześnie być wobec niego regulacją szczególną, w przypadku, gdy dane pozyskiwane w związku ze świadczeniem usług łączności są danymi osobowymi. Rozporządzenie chroni nie tylko prywatność osób fizycznych (jak w przypadku RODO), ale jego przepisy stosuje się również do osób prawnych.

Rozporządzenie *e-Privacy* ma zwiększyć prywatność osób i podmiotów świadczących usługi (w tym medyczne) przed monitorowaniem wykorzystywanych przez te podmioty wszelkiego rodzaju urządzeń końcowych np. smartfony, laptopy. Ma się to odbyć poprzez:

- zwiększenie wymogów, co do pozyskiwania zgody użytkownika końcowego na wykorzystywanie informacji o jego urządzeniu lub informacji znajdujących się na urządzeniu (np. w zakresie zgód na gromadzenie informacji za pomocą plików *cookies*), także w przypadku wykorzystywania ich w celu marketingu;
- podniesienie poziomu przejrzystości w odniesieniu do plików *cookies*;
- skorelowanie przepisów *e-Privacy* z przepisami RODO;
- objęcie ochroną również metadanych, takich jak informacje o lokalizacji, długości rozmowy, odwiedzanych stronach www;
- obowiązek wyświetlania numeru (lub specjalnego prefiksu) w przypadku marketingu telefonicznego;

- wprowadzenie kar administracyjnych za naruszenie przepisów rozporządzenia do 20 mln EUR lub do 4% rocznego obrotu[14].

Rozporządzenie obejmuje ochroną (np. obowiązkiem zachowania poufności) dane pochodzące z usług łączności elektronicznej. Chodzi nie tylko o informacje pozyskiwane w związku ze świadczeniem tradycyjnych usług łączności, ale też informacje pozyskiwane z nowymi, opartymi na Internecie usługami umożliwiającymi komunikację jak np. usługi telefonii internetowej (VoIP), komunikatory internetowe, usługi poczty elektronicznej przez Internet (tzw. usługi OTT, *Over-the-Top communications services*).

Za dane pochodzące z łączności elektronicznej uznaje się wszelkie informacje dotyczące przesyłanych lub przekazywanych treści (treści łączności elektronicznej) oraz informacje dotyczące użytkowników końcowych, w tym dane służące do śledzenia i zidentyfikowania źródła i miejsca docelowego łączności, lokalizacji, daty i godziny oraz rodzaju łączności.

Ochroną objęto również metadane, jako mogące ujawniać pośrednio szczególnie chronione informacje, takie jak zwyczaje, codzienne aktywności, relacje towarzyskie. Do metadanych zalicza się m.in. wybierane numery, odwiedzane strony internetowe, lokalizację, godzinę, datę i czas trwania połączenia.

Rozporządzenie dotyczy danych w zakresie w jakim sieci łączności są udostępniane nieokreślonej grupie użytkowników (np. publiczne hot spoty). Nie ma ono natomiast zastosowania do sieci firmowych, dostępnych dla użytkowników wyłącznie jednej organizacji.

Rozporządzenie ma również zastosowanie do komunikatów przesyłanych w trybie maszyna-maszyna, jeśli dochodzi do przekazywania sygnału w ramach sieci. Ma to w szczególności zastosowanie do rozwiązań opartych na Internecie Rzeczy (*Internet of Things, IoT*). Unijny prawodawca dopuszcza możliwość szczególnego uregulowania odpowiednich środków bezpieczeństwa w tym zakresie w odrębnych aktach prawnych.

8. Ocena ryzyk i szacowanie bezpieczeństwa w systemach informatycznych ochrony zdrowia

Jednym z istotnych czynników dotyczących bezpieczeństwa informacji i danych w systemach informatycznych jest szacowanie możliwych sfer ryzyka. Administrator danych (w

[14] Rozporządzenie e-Privacy. *Większa ochrona użytkowników urządzeń końcowych (komputerów, telefonów, smartfonów, czy tabletów) przed nadmierną ingerencją w sferę ich prywatności*, https://www2.deloitte.com/pl/pl/pages/doradztwo-prawne/articles/alerty-prawne/rozporzadzenie-eprivacy-przewodnik.html (dostęp 04.2018).

jednostkach opieki zdrowotnej to kierownik podmiotu leczniczego) jest odpowiedzialny za zapewnienie bezpieczeństwa danych przechowywanych nie tylko w systemie informatycznym, ale również w innej formie. System informatyczny jest bezpieczny, jeśli jego użytkownik może na nim polegać, a zainstalowane oprogramowanie działa zgodnie ze swoją specyfikacją[15]. Jednak nawet najbardziej rozwinięte oprogramowanie z bardzo zaawansowanymi elementami zapewniającymi bezpieczeństwo narażone jest na błąd ludzki, ponieważ najsłabszym ogniwem systemów informatycznych jest człowiek. Rozumienie bezpieczeństwa informacji w systemach informatycznych opiera się na trzech podstawowych parametrach, które w skrócie nazywane są CIA (*Confidentiality* - poufność, *Integrity* - integralność, *Availability* – dostępność)[16].

Poufność - dane i usługi powinny być dostępne tylko dla osób, procesów lub innych usług, które mają do nich uprawnienia. Dostępu do kont i danych chronią nazwy użytkowników, hasła, hasła jednorazowe, szyfrowane łącza itp. W bardziej złożonych scenariuszach pojawia się wielostopniowe uwierzytelnianie. Dwa terminy ściśle związane z poufnością, to również uwierzytelnianie, czyli potwierdzenie tożsamości oraz autoryzacja, czyli potwierdzenie uprawnień.

Integralność – dane i usługi powinny być nienaruszone przez podmioty (osoby, procesy, usługi), które nie mają do nich uprawnień. Wszelkie próby (udane oraz nieudane) takich operacji powinny być wykryte i zanotowane. Do tego celu warto wykonywać audyt oprogramowania oraz szacowanie ryzyka, a także monitorowanie zachowań.

Dostępność - cecha ta w zasadzie dotyczy jednego, ale dość ważnego warunku: ktokolwiek jest uprawniony powinien mieć możliwość wykorzystania zasobów w całości praw, jakie posiada. Zapewnienie tej cechy leży głównie po stronie administratora systemu informatycznego.

Bezpieczeństwo nie jest stanem nadanym raz, zatem nie da się wprowadzić takiej konfiguracji systemu, aby można było powiedzieć, że od tej pory jest bezpiecznie. Bezpieczeństwo jest procesem ciągłym, w którym wykonuje się określony zespół czynności, w którym bierze udział nie tylko administrator systemów informatycznych, ale również pracownicy. Podstawowe zagrożenia bezpieczeństwa można podzielić na dwa rodzaje:

1. celowe (chęć zysku, uznania, zemsta),

[15] S. Garfinkel, PRACTICAL UNIX AND INTERNET SECURITY, II e., O'Reilly, 2003
[16] A. Białas, *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, Wydawnictwa Naukowo-Techniczne, Warszawa 2006.

2. przypadkowe (nieświadomość użytkownika, zaniedbania, naiwność, wady sprzętu i oprogramowania).

Najtrudniej zapewnić bezpieczeństwo wynikające z zagrożeń przypadkowych, ponieważ osoby odpowiedzialne nie są w stanie dokładnie przewidzieć, czego można oczekiwać od użytkowników systemów, ale również od czynników zewnętrznych np. zalanie, pożar. W związku z tym niezwykle, ważne jest wykonywanie audytu bezpieczeństw i ocena ryzyk.

Wagę problemu oceny ryzyk oraz oceny bezpieczeństwa danych najlepiej ilustrują dwa poniższe przykłady nieprawidłowości, które wystąpiły tak w polskim, jak i brytyjskim systemie opieki zdrowotnej.

Dane osobowe (pacjentów i pracowników) zgromadzone na serwerach SP ZOZ w Kole przechowywane były na niezabezpieczonych hasłem serwerach. W rezultacie nastąpił wyciek danych osobowych dotyczących personelu oraz około 50 tysięcy pacjentów zarejestrowanych w latach 2003-2007.

W przypadku brytyjskim doszło w 2017 roku do największego ataku na brytyjską ochronę zdrowia. Wszystko wskazuje na to, że atak był możliwy tylko, dlatego, że nie wdrożono aktualizacji do systemu, którą jego producent opracował i udostępnił. Wydarzenia te miały miejsce, mimo, że ICO (odpowiednik polskiego Urzędu Ochrony Danych) nakładał surowe kary na podmioty, które nie wykonywały zalecanych przez urząd uaktualnień. Kilka lat wcześniej upubliczniona została informacja o luce w zabezpieczeniach protokołu OpenSSL, nazwanej „*Heartbleed*". Protokoły OpenSSL wykorzystywane są w celu zabezpieczenia internetowej komunikacji pomiędzy serwerami a komputerami podłączonymi do sieci. Wadliwe zabezpieczenia zostały wykorzystane przez grupę *Anonymous*, wskutek czego uzyskano dostęp do kilkunastu skrzynek mailowych pracowników. Znajdowało się w nich ponad 30 tysięcy maili – część z nich zawierała dane wrażliwe pracowników. Na urząd miasta Gloucester, nałożona została kara w wysokości 100 tysięcy funtów brytyjskich. Trzeba również dodać, że wykrycie przez urząd luki było niemal natychmiastowe; dopiero późniejsze zaniedbania zaowocowały udanym atakiem grupy *Anonymous*.

9. Audyt oprogramowania

Audyt oprogramowania to ocena przedsiębiorstwa pod względem zarządzania licencjami oraz legalnością posiadanego oprogramowania. Audyt przeprowadzany jest na wszystkich stacjach roboczych i serwerach oraz pozwala na dostarczenie szczegółowych informacji o zainstalowanych na nich aplikacjach oraz plikach przechowywanych na dyskach, które

mogłyby być sprzeczne z wytycznymi przedsiębiorstwa oraz obowiązującym prawem. Audyt oprogramowania powinien dać odpowiedź na trzy podstawowe pytania, czy oprogramowanie jest potrzebne, czy jest legalne oraz czy wersje są aktualne.

Celem przeprowadzenia audytu oprogramowania jest wprowadzenie porządku w oprogramowaniu, tak, aby osoba odpowiedzialna za oprogramowanie w firmie miała pewność, że każdy zainstalowany w firmie program jest używany zgodnie z licencją, że ilość programów odpowiada rzeczywistemu zapotrzebowaniu oraz że programy są optymalnie wykorzystywane przez użytkowników. Celem uporządkowania procesów audytu zaleca się przeprowadzanie go w odpowiednich etapach (patrz: Rysunek 1). W początkowych etapach klasyfikacja oprogramowania zgodnie z jej wykorzystywaniem oraz miejscem zainstalowania, następnie charakterystyka oprogramowania i zarządzanie licencjami. Od audytu oczekiwać trzeba również, między innymi:

- przeprowadzenia inwentaryzacji oprogramowania,
- zestawienia zainstalowanego oprogramowania z nabytymi licencjami,
- zarządzania polisami bezpieczeństwa i procedury,
- rozwinięcia planu ewidencyjnego z uwzględnieniem odpowiedniej dokumentacji.

Audyt oprogramowania może być związany z audytem sprzętu, a najlepszym momentem na wykonanie takich audytów jest tak zwany audyt zerowy, czyli pierwszy dokonany w firmach spis oprogramowania wraz ze spisem sprzętu. Podstawowe korzyści płynące z audytu to między innymi:

- korzyści finansowe wynikające ze świadomego wykorzystania posiadanego oprogramowania i korzystania z optymalnych opcji zakupowych,
- optymalizacja planów inwestycyjnych związanych z oprogramowaniem (kupowanie wyłącznie tego, co jest naprawdę potrzebne)
- aktualizowanie tylko tych licencji, które naprawdę są używane (co daje wymierne korzyści finansowe dla całej firmy),
- redukcja kosztów pomocy technicznej wynikająca ze standaryzacji oraz usunięcia zbędnych i przestarzałych składników infrastruktury.

Szczegółowo przykładowe etapy inwentaryzacji oprogramowania prezentuje Rysunek 1.

Sam audyt oprogramowania nie jest tym samym, czym audyt bezpieczeństwa danych przechowywanych w systemach informatycznych, a nieodłącznym elementem jest identyfikacja ryzyka i analiza zagrożeń dla bezpieczeństwa danych zdrowotnych. Głównym

celem identyfikacji ryzyka jest określenie możliwych zagrożeń wynikających z dwóch podstawowych obszarów:

1. błędy ludzkie - wynikają one z niestosowania się pracowników podmiotu leczniczego do założeń polityki bezpieczeństwa lub źle opracowanej polityki.
2. błędy zewnętrzne – niezależne od ludzi bądź źle oszacowanych ryzyk. Obejmują one na przykład ryzyko zalania serwera lub jednostek, pożar, kradzież komputerów przez złe zabezpieczenia pomieszczeń.

Rysunek 1. Przykład inwentaryzacji oprogramowania

Źródło: Opracowanie własne.

W związku z tym, podmioty lecznicze przetwarzające informacje dotyczące stanu zdrowia, w tym informacje o stanie zdrowia indywidualnych osób, powinny mieć spisaną politykę bezpieczeństwa informacji, zaakceptowaną przez kierownictwo, opublikowaną, ale również podaną do wiadomości wszystkim pracownikom i ewentualnym stronom zewnętrznym. Ponieważ polityka bezpieczeństwa jest procesem ciągłym powinna być poddawana przeglądowi przynajmniej raz na rok. Częstotliwość aktualizacji polityki jest uzależniona od wielkości podmiotu leczniczego, natomiast aktualizacja tego dokumentu jest konieczna po wystąpieniu incydentu dotyczącego bezpieczeństwa danych[17].

[17] ISO/IEC 27002: 2013; Information technology -- Security techniques -- Code of practice for information security controls

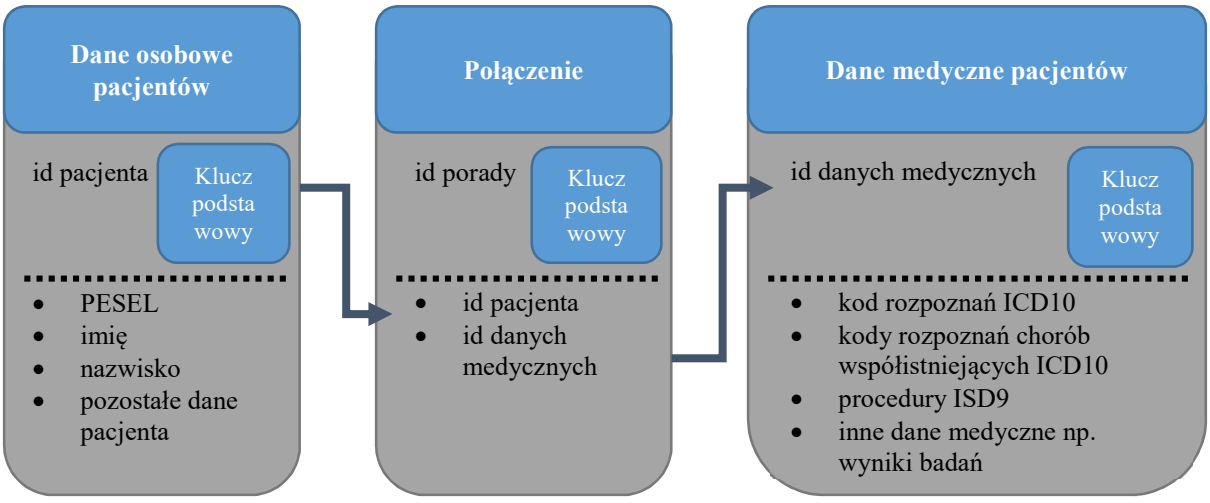
Elementy analizy ryzyka i zarządzania nim powinny obejmować wiele aspektów, miedzy innymi:

- identyfikacja aktywów (w tym celu przeprowadza się opisany wyżej audyt oprogramowania), zagrożeń i słabych punktów;
- ocenę wpływu na funkcjonowanie podmiotu;
- prawdopodobieństwo zagrożenia i ocena podatności systemu;
- określenie poziomu ryzyka lub wielu ryzyk naruszeń bezpieczeństwa;
- zestawienie aktualnych kontroli z poprzednimi i identyfikacja nadmiarowych obszarów ryzyka;
- mapowanie decyzji podjętych na podstawie przeprowadzonych kontroli.

Jednym z zalecanych sposobów zapobiegania skutkom nieuprawnionego dostępu jest takie projektowanie aplikacji, aby zapewnić separacje danych (patrz: **Błąd! Nie można odnaleźć źródła odwołania.**)[18]. Dane medyczne pacjenta powinny być wydzielone fizycznie, ale też logicznie od danych osobowych (demograficznych) pacjentów. Dzięki temu dane medyczne są niezależne od danych osobowych pacjentów.

Strukturę separacji danych w podmiotach leczniczych przestawia **Błąd! Nie można odnaleźć źródła odwołania.**.

Rysunek 2. Separacja danych w podmiotach leczniczych



Źródło: Opracowanie własne.

[18] Ibidem.

Wnioski

Dane wygenerowane przez urządzenia tworzące Internet rzeczy mogą stanowić dane osobowe. Producenci tego typu urządzeń i oprogramowania, co do zasady, mogą zostać uznani za administratorów danych osobowych. Wobec tego będą na nich nałożone obowiązki wynikające z unijnych i krajowych przepisów o ochronie danych osobowych. Natomiast użytkownicy Internetu rzeczy powinni być informowani o tym, kto przetwarza ich dane. Powinni również wyrazić zgodę na takie przetwarzanie, kiedy wymagają tego przepisy.

Zasada *Privacy by design* (zasada prywatności w fazie projektowania) oraz *privacy by default* (zasadą prywatności w ustawieniach domyślnych) wymagają przewidywania i przeciwdziałania możliwym problemom w zakresie ochrony danych, jeszcze na etapie przygotowania konkretnych rozwiązań systemowych, z obowiązkiem udokumentowania swojego wyboru.

Kodeks postepowania to dokument umożliwiający dokonanie optymalnego wyboru w obszarze zabezpieczenia danych zgodnie z postanowieniami RODO. Wskazuje się w nim, w jaki techniczny i organizacyjny sposób dobrać zabezpieczenia, w zależności od specyfiki instytucji i możliwości finansowych danego podmiotu. W praktyce zarządzający placówkami medycznymi otrzymują rodzaj praktycznej instrukcji ułatwiającej tworzenie systemu ochrony danych osobowych.

Rozporządzenie *e-Privacy* ma zwiększyć prywatność osób i podmiotów świadczących usługi (w tym medyczne) przed monitorowaniem wykorzystywanych przez te podmioty wszelkiego rodzaju urządzeń końcowych np. smartfony, laptopy.

Bezpieczeństwo nie jest stanem nadanym raz, zatem nie da się wprowadzić takiej konfiguracji systemu, aby można było powiedzieć, że od tej pory jest bezpiecznie. Bezpieczeństwo jest procesem ciągłym, w którym wykonuje się określony zespół czynności, w którym bierze udział nie tylko administrator systemów informatycznych, ale również pracownicy. Ocena ryzyk i audyt oprogramowania są istotnymi elementami tego procesu.

Literatura

[1] Białas A., *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, Wydawnictwa Naukowo-Techniczne, Warszawa 2006.
[2] Chylińska K., *Zastępca Europejskiego Inspektora Ochrony Danych Osobowych: Nowe technologie – Internet rzeczy,* http://blog.e-odo.pl/2015/10/17/nowe-technologie-internet-rzeczy/.

[3] Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 2 października 1995 r.
[4] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/943 z dnia 8 czerwca 2016 r. w sprawie ochrony niejawnego know-how i niejawnych informacji handlowych (tajemnic przedsiębiorstwa) przed ich bezprawnym pozyskiwaniem, wykorzystywaniem i ujawnianiem (Dz. Urz. UE L 157 z 15.06.2016, s. 1).
[5] ISO/IEC 27002: 2013; Information technology -- Security techniques -- Code of practice for information security controls.
[6] Koseła D., *Internet Rzeczy – rewolucja technologiczna i nowe wyzwania dla prawników*, http://bpcc.org.pl/pl/publikacje/internet-rzeczy-rewolucja-technologiczna-i-nowe-wyzwania-dla-prawnikow.
[7] Kwiatkowska E., *Rozwój Internetu rzeczy – szanse i zagrożenia*, http://www.wz.uw.edu.pl/pracownicyFiles/id26574-6.0_Rozw%C3%B3j_internetu_rzeczy_-_szanse_i_zagro%C5%BCenia%5B1%5D.pdf.
[8] Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 9 lutego 2018 r. w sprawie ogłoszenia jednolitego tekstu ustawy o zwalczaniu nieuczciwej konkurencji Dz.U. 2018 poz. 419.
[9] *Opinia 8/2014 w sprawie ostatnich postępów w dziedzinie Internetu Przedmiotów (WP 223) Grupy Roboczej art. 29*, https://giodo.gov.pl/pl/1520203/8646.
[10] Rozporządzenie e-Privacy. *Większa ochrona użytkowników urządzeń końcowych (komputerów, telefonów, smartfonów, czy tabletów) przed nadmierną ingerencją w sferę ich prywatności*, https://www2.deloitte.com/pl/pl/pages/doradztwo-prawne/articles/alerty-prawne/rozporzadzenie-eprivacy-przewodnik.html.
[11] Rozporządzenie Ministra Zdrowia z dnia 20 grudnia 2012 r. w sprawie warunków występowania o sporządzenie dokumentu elektronicznego potwierdzającego prawo do świadczeń opieki zdrowotnej Dz.U. 2012 poz. 1500.
[12] Garfinkel S., PRACTICAL UNIX AND INTERNET SECURITY, II e., O'Reilly, 2003.
[13] *Tajemnica przedsiębiorstwa a zakaz konkurencji*, https://poradnikprzedsiebiorcy.pl/-tajemnica-przedsiebiorstwa-a-zakaz-konkurencji.
[14] Ustawa z 16.07.2004 r. – Prawo telekomunikacyjne (Dz.U. Nr 171, poz. 1800 ze zm.).
[15] Wolanin A., *Privacy by design - nowa zasada planowania przetwarzania*, https://www.rodokompas.ostrowski-legal.net/single-post/2018/01/22/privacybydesign.

Streszczenie

W artykule omówiono wpływ niektórych nowych rozwiązań technologicznych na problem bezpieczeństwa i poufności danych medycznych oraz przedstawiono możliwe rozwiązania instytucjonalne i programowe wspierające instytucje opieki zdrowotnej w zapewnieniu, zgodnie z nowymi regulacjami, odpowiedniego poziomu zabezpieczenia danych medycznych.

Dane wygenerowane przez urządzenia tworzące Internet Rzeczy mogą stanowić dane osobowe. Producenci tego typu urządzeń i oprogramowania, co do zasady mogą zostać uznani za administratorów danych osobowych. Wobec tego będą na nich nałożone obowiązki wynikające z unijnych i krajowych przepisów o ochronie danych osobowych.

Privacy by design (zasada prywatności w fazie projektowania) oraz *privacy by default* (zasadą prywatności w ustawieniach domyślnych) wymagają przewidywania i przeciwdziałania możliwym problemom w zakresie ochrony danych jeszcze na etapie przygotowania konkretnych rozwiązań systemowych.

Kodeks postepowania to dokument umożliwiający dokonanie optymalnego wyboru w obszarze zabezpieczenia danych zgodnie z postanowieniami RODO. W praktyce zarządzający placówkami medycznymi otrzymują rodzaj praktycznej instrukcji ułatwiającej tworzenie systemu ochrony danych osobowych.

Rozporządzenie *e-Privacy* ma zwiększyć prywatność osób i podmiotów świadczących usługi (w tym medyczne) przed monitorowaniem wykorzystywanych przez te podmioty wszelkiego rodzaju urządzeń końcowych np. smartfony, laptopy.

Bezpieczeństwo jest procesem ciągłym, w którym wykonuje się określony zespół czynności, w którym bierze udział nie tylko administrator systemów informatycznych, ale również pracownicy. Ocena ryzyk i audyt oprogramowania są istotnymi elementami tego procesu.

Słowa kluczowe

Internet rzeczy, ocena ryzyk, *e-Privacy*, audyt oprogramowania, RODO, kodeksy postępowania