DZP
więcej niż prawo

Microsoft

Cyberbezpieczeństwo w sektorze ochrony zdrowia

Warszawa, 5 października 2017 r.

Autorzy:
Lek. Piotr Najbuk, Associate DZP
Paweł Kaźmierczyk, Associate DZP
Wojciech Dziomdziora, Counsel DZP
Piotr Marczuk, Dyrektor ds. Polityki Korporacyjnej, Microsoft

Raport został przygotowany przy wsparciu merytorycznym Microsoft Polska sp. z o.o.

Spis treści

I. Wprowadzenie

Dane pacjentów coraz częściej zapisywane są przez szpitale i inne placówki lecznicze w formie cyfrowej, w ramach elektronicznej dokumentacji medycznej. Wynika to nie tylko ze względów organizacyjnych – łatwy i szybki transfer informacji o stanie zdrowia sprzyja rozwojowi telemedycyny, a dokonywane przez komputer analizy zgromadzonych zbiorów danych mogą wspomagać proces leczenia pacjentów i projektowania polityki zdrowotnej. Dlatego też prowadzenie elektronicznej dokumentacji medycznej ma być prawnie uwarunkowanym standardem. Obowiązek wdrożenia takich systemów (obejmujących m.in. elektroniczne recepty i skierowania), choć wielokrotnie przekładany, ma zacząć funkcjonować najpóźniej do 1 stycznia 2021 r.[1]

Przejście z papierowych kartotek do danych zapisanych w szpitalnych serwerowniach lub w chmurze wiąże się z innymi ryzykami, charakterystycznymi dla wirtualnej rzeczywistości. Awarie, złośliwe oprogramowanie oraz ataki hakerskie wymuszają podjęcie działań zabezpieczających zbiory danych medycznych. Podstawowe zasady bezpieczeństwa wynikają wprost z przepisów prawa, bardziej zaawansowane środki określone są w publikowanych przez stronę publiczną lub organizacje branżowe zaleceniach, rekomendacjach, kodeksach postępowania lub zbiorach dobrych praktyk.

12 maja 2017 r. nieznani hakerzy dokonali masowego cyberataku na firmy i instytucje w całej Europie. W przypadku Wielkiej Brytanii przestępcy skupili się na szpitalach należących do *National Health Service (NHS)*[2].

- **Komputery podmiotów leczniczych zostały zarażone przez tzw. ransomware. Oprogramowanie zostało całkowicie zablokowane, lekarze poszukujący elektronicznej dokumentacji medycznej ujrzeli jedynie komunikat z żądaniem okupu.**

- **Atak nastąpił synchronicznie – dotknięte nim szpitale utraciły dostęp do danych w tym samym momencie, co wywołało dodatkowy chaos.**

- **W wyniku ataku wielu pacjentów musiało zostać przeniesionych do innych placówek, karetki były kierowane do innych szpitali, część planowych zabiegów została odwołana.**

- **Jak podała stacja BBC, National Cyber Security Center, jednostka odpowiedzialna za śledztwo w tej sprawie, podejrzewa, że za atakami stała Korea Północna[3].**

---

1 Ustawa z dnia 20 lipca 2017 r. o zmianie ustawy o systemie informacji w ochronie zdrowia oraz niektórych innych ustaw (Dz.U. z 2017 r. poz. 1524) ponownie wydłużyła termin implementacji nowych rozwiązań teleinformatycznych, który dotychczas zaplanowany był na 1 stycznia 2018 r.

2 http://www.bbc.com/news/health-39899646

3 http://www.bbc.com/news/technology-40297493

II. Ochrona danych pacjenta

1. Dane medyczne – dane wymagające szczególnej ochrony

W sektorze ochrony zdrowia codzienne przetwarzane są olbrzymie ilości danych o stanie zdrowia pacjentów. Są to niezwykle intymne i wrażliwe informacje dotyczące m.in. aktualnych chorób, przebytych operacji, przyjmowanych leków, nałogów. W wielu przypadkach utrata danych lub zablokowanie do nich dostępu dla osób wykonujących zawody medyczne może uniemożliwić lub znacząco skomplikować dalsze udzielanie świadczeń zdrowotnych, co w konsekwencji stanowi poważne zagrożenie dla zdrowia, a w skrajnych przypadkach także życia pacjenta. Równie poważne skutki mogą wyniknąć z wycieku danych i dostania się ich w niepowołane ręce. Dane medyczne mogą zostać np. bezprawnie wykorzystane przez ubezpieczycieli, upublicznione bez zgody mogą uderzać w prywatność osób publicznych oraz zwykłych obywateli, mogą też zostać wykorzystane jako narzędzie szantażu bądź służyć do zdyskredytowania danej osoby.

Dostępne dane wskazują, że szpitale i inne placówki medyczne oraz podmioty publiczne przetwarzające dane medyczne coraz częściej stają się celem ataków hakerskich. Przeprowadzone w Stanach Zjednoczonych badania wskazują, że co dziesiąty podmiot leczniczy doświadcza próby włamania każdego dnia[4]. Nie jest to zaskakujące – dane medyczne to cenny łup dla cyberprzestępców, a podmioty wykonujące działalność leczniczą niejednokrotnie nie posiadają dostatecznej świadomości, wiedzy eksperckiej, możliwości organizacyjnych ani środków na wdrożenie procedur i rozwiązań z zakresu cyberbezpieczeństwa. Branża medyczna, pomimo rosnącej liczby cyber ataków, wciąż wydaje się być zapóźniona w porównaniu z sektorem finansowym[5], również przetwarzającym olbrzymie ilości danych wrażliwych i poufnych. Banki posiadają osobne działy IT/cyberbiezpieczeństwa zatrudniające niejednokrotnie kilkudziesięciu profesjonalistów, a także angażują zewnętrze firmy specjalizujące się w zapewnianiu wysokiego poziomu cyberbezpieczeństwa.

Cyberprzestępcom zależy przede wszystkim na uzyskaniu dostępu do danych, które mogą być nastepnie nielegalnie odsprzedane dalej lub wykorzystane np. do szantażu. Za atakami na sektor ochrony zdrowia mogą stać także obce państwa, którym zależy na destabilizacji społecznej (np. paraliż cywilnej służby zdrowia) i zmniejszeniu potencjału obronnego przeciwników (np. paraliż sieci szpitali wojskowych). Z podobnych względów atak hakerski na szpitale może być formą zamachu terrorystycznego.

[4] Healthcare Cybersecurity Survey, KPMG 2015

[5] por. http://www.independent.co.uk/news/business/news/healthcare-is-now-top-industry-for-cyberattacks-says-ibm-a6994526.html

Dotychczasowe badania potwierdzają, że wszelkie incydenty w tym obszarze mogą mieć bardzo duży wpływ na społeczeństwo[6]. Dlatego też sektor ochrony zdrowia oceniany jest jako sektor krytyczny, który powinien podlegać szczególnej ochronie. Wymaga to m.in. dostosowanych do realiów cyberprzestrzeni norm prawnych wyznaczających standardy ochrony oraz wprowadzania skutecznych strategii zarządzania ryzykiem w oparciu o dogłębną analizę możliwości lepszego przygotowania sektora do obrony przed cyber zagrożeniami. Standardy te mogą mieć różny charakter – od wiążących norm prawnych, poprzez samoregulację, aż po zalecane do stosowania przykłady dobrych praktyk. Do najbardziej znanych standardów w zakresie cyberbezpieczeństwa stosowanych przez wiele organizacji w różnych krajach należą Ramy Bezpieczeństwa Cybernetycznego[7], opracowane przez amerykański Krajowy Instytut Standaryzacji i Technologii *(National Institute of Standards and Technology – NIST).* Są to optymalne praktyki, które mogłyby z powodzeniem zostać zaadaptowane przez sektor ochrony zdrowia także w Polsce.

2. Bezpieczeństwo danych medycznych – perspektywa Unii Europejskiej

Systemy ochrony zdrowia w Unii Europejskiej są ze sobą połączone. Dyrektywa w sprawie stosowania praw pacjentów w **transgranicznej** opiece zdrowotnej zapewnia każdemu obywatelowi Wspólnoty swobodę wyboru miejsca leczenia. Wiąże się to z koniecznością transferu danych medycznych związanych z procesem udzielania świadczeń. Dlatego też problemy w tym zakresie jednego państwa członkowskiego już nie są ograniczone wyłącznie do niego - mogą mieć skutki transgraniczne.

Do wyznaczenia wspólnych, minimalnych standardów w tym zakresie zmierza Unia Europejska. Wśród najważniejszych inicjatyw z tego zakresu należy wymienić rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (**ogólne rozporządzenie o ochronie danych, tzw. RODO**), którego normy zaczną obowiązywać od 25 maja 2018 r. wyznacza ono nowy, wyższy standard ochrony danych dotyczących osób fizycznych, w tym danych dotyczących stanu zdrowia. Od 1 lipca 2016 r. stosuje się już przepisy rozporządzenia Parlamentu Europejskiego i Rady (UE) Nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (tzw. **eIDAS**), które określają m.in. poziomy bezpieczeństwa systemów identyfikacji elektronicznej.

Poszerzenie współpracy państw członkowskich w kwestii cyberbezpieczeństwa jest także celem dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii **(tzw. dyrektywa NIS).**

---

[6] Security and Resilience in eHealth - Security Challenges and Risks, ENISA 2015 [3] http://www.bbc.com/news/technology-40297493

[7] https://www.nist.gov/cyberframework

3. Czy polskie placówki są gotowe na wyzwania w zakresie cyberbezpieczeństwa? Dotychczasowe doświadczenia

Zaprezentowane przez Najwyższą Izbę Kontroli wyniki kontroli P/15/061 „Tworzenie i udostępnianie dokumentacji medycznej", której głównym celem było ocenienie rzetelności i zgodności z prawem tworzenia i udostępniania dokumentacji medycznej pacjentów[8], potwierdziły istotne problemy z przestrzeganiem zasad prowadzenia dokumentacji medycznej i ochrony danych osobowych w szpitalach. NIK stwierdziła ponadto, że do czasu zakończenia kontroli **żaden z objętych kontrolą świadczeniodawców nie wdrożył systemu informatycznego dedykowanego prowadzeniu dokumentacji medycznej w postaci elektronicznej.** Jak wskazują szacunki w skali kraju, obecnie jedynie niewiele ponad 40 procent szpitali jest zinformatyzowanych[9].

W czerwcu 2017 r. do opinii publicznej trafiła informacja, że doszło do wycieku danych ok. 50 tys. pacjentów Samodzielnego Publicznego Zakładu Opieki Zdrowotnej w Kole. Wśród informacji udostępnionych publicznie w sieci miały znaleźć się, oprócz danych identyfikacyjnych takich jak nazwiska, adresy, numery PESEL, także dane medyczne – historia choroby czy grupa krwi. To najprawdopodobniej przypadek największego naruszenia zasad ochrony danych osobowych w sektorze ochrony zdrowia[10].

W wyniku doniesień prasowych interwencję podjął Rzecznik Praw Obywatelskich. Zwrócił się on do Ministra Zdrowia i GIODO z prośbą o wyjaśnienia oraz wskazanie czy resort systemowo interesuje się kwestią zabezpieczania danych[11].

Dotychczasowe problemy z zachowaniem standardów ochrony danych osobowych pacjentów oraz stosunkowo niski poziom przygotowania podmiotów leczniczych do prowadzenia dokumentacji medycznej w formie elektronicznej, wskazuje na potrzebę wykorzystania także pozaprawnych narzędzi regulacji, w szczególności instrumentów tzw. miękkiego prawa (z ang. *soft law*), czyli niewiążących reguł opracowywanych przez posiadające odpowiednią, specjalistyczną wiedzę instytucje publiczne lub organizacje branżowe.

4. Konsekwencje naruszeń

Warto podkreślić, że zapewnienie odpowiednio wysokiego poziomu bezpieczeństwa informacji o pacjencie to prawny obowiązek administratorów danych oraz osób za nie odpowiedzialnych, za którego nieprzestrzeganie przewidziane są sankcje karne, administracyjne, cywilne i zawodowe. Bardzo dotkliwe mogą być także wysokie kary finansowe, które zaczną obowiązywać wraz z przepisami RODO.

---

[8] Kontrola P/15/061 – „Tworzenie i udostępnianie dokumentacji medycznej", KZD.430.002.2015, Nr ewid. 199/2015/P/15/061/KZD

[9] http://www.rynekzdrowia.pl/Technologie-informacyjne/Radziwill-niewiele-ponad-40-procent-szpitali-jest-zinformatyzowanych,173509,7.html

[10] http://businessinsider.com.pl/technologie/nowe-technologie/spzoz-w-kole-wyciek-danych-pacjentow/dbk7zzf

[11] https://www.rpo.gov.pl/sites/default/files/Do%20Ministra%20Zdrowia%20ws.%20wycieku%20danych%20osobowych%20pacjent%C3%B3w%20szpitala.pdf

W świetle ogólnych zasad ochrony danych osobowych wskazanych w aktualnie obowiązującej ustawie o ochronie danych osobowych[12] szczególnej odpowiedzialności podlegają administrator danych oraz osoby odpowiedzialne za ich ochronę (osoba, która zarządza, zawiaduje zbiorem danych lub danymi w procesie ich przetwarzania[13]). W przypadku udostępnienia informacji lub umożliwienia dostępu do nich osobom nieupoważnionym, podlegają oni grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2 (w przypadku działania nieumyślnego do jednego roku)[14]. Kara ograniczenia wolności albo pozbawienia wolności do roku przewidziana jest także w przypadku naruszenia, choćby nieumyślnie, obowiązku zabezpieczenia danych osobowych przed zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem[15].

Konsekwencje potencjalnych naruszeń ochrony danych osobowych znacząco wzrosną po 25 maja 2018 r., kiedy zacznie obowiązywać RODO. Nowe przepisy przewidują kary pieniężne dochodzące do 20 mln EUR lub w przypadku przedsiębiorstwa w wysokości do 4 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego. Unijny prawodawca przewiduje przy tym, że każde państwo członkowskie może określić, czy i w jakim zakresie administracyjne kary pieniężne można nakładać na organy i podmioty publiczne ustanowione w tym państwie członkowskim. Projekt nowej ustawy o ochronie danych osobowych[16] zakłada, że na określone podmioty publiczne, w tym m.in. Narodowy Fundusz Zdrowia oraz samodzielne publiczne zakłady opieki zdrowotnej, można nakładać administracyjne kary pieniężne w maksymalnej wysokości do 100 tys. zł.

Dane medyczne obok ogólnych zasad odpowiedzialności za przetwarzanie danych osobowych zabezpieczone są również sankcjami szczególnymi wskazanymi w prawie medycznym. Osoby wykonujące zawody medyczne zobowiązane są do zachowania tajemnicy zawodowej. Udostępnienie danych pacjenta w formie cyfrowej może prowadzić do jej naruszenia, co grozi grzywną, karą ograniczenia wolności albo pozbawienia wolności do lat 2[17]. Takie naruszenie zasad wykonywania zawodu wiązać się będzie potencjalnie także z odpowiedzialnością zawodową, w tym m.in. pozbawieniem prawa wykonywania zawodu.

Na szczególną odpowiedzialność związaną z przetwarzaniem danych sensytywnych narażone są podmioty wykonujące działalność leczniczą. Naruszenie zasad bezpieczeństwa informacji o stanie zdrowia może zostać uznane za praktykę naruszającą zbiorowe prawa pacjentów, której dalsze występowanie w konsekwencji prowadzić może do nałożenia na placówkę kary pieniężnej do wysokości 500 000 zł[18].

Ujawnienie danych medycznych godzić będzie w prywatność pacjenta, która jest jego dobrem osobistym podlegającym ochronie prawa cywilnego. Pacjent będzie mógł więc dochodzić odszkodowania przed sądem.

---

12 Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2016 r. poz. 922 ze zm.). Należy zaznaczyć, że w momencie powstawania niniejszego materiału opublikowany został projekt nowej ustawy o ochronie danych osobowych, który dostosowuje krajowe normy do przepisów RODO.

13 Barta Paweł, Litwiński Paweł, *Ustawa o ochronie danych osobowych. Komentarz*, Wyd. 4, Warszawa 2016, Komentarz do art. 51, Legalis.

14 art. 51 ustawy o ochronie danych osobowych;

15 art. 52 ustawy o ochronie danych osobowych.

16 https://legislacja.rcl.gov.pl/projekt/12302950

17 art. 266 ustawy z dnia 6 czerwca 1997 r. Kodeks karny (t.j. Dz.U. z 2016 r. poz. 1137 ze zm.)

18 art. 68 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (t.j. Dz.U. z 2017 r. poz. 1318 ze zm.)

III. Standardy bezpieczeństwa

1. Twarde i miękkie prawo

Podstawowe wymogi dotyczące bezpieczeństwa przetwarzania informacji o pacjentach wynikają wprost z przepisów powszechnie obowiązującego prawa. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych określa minimalne standardy ochrony danych dotyczących osób fizycznych, natomiast przepisy prawa medycznego, w szczególności ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta, normują postępowanie z dokumentacją medyczną.

Należy jednak pamiętać, że regulacje prawne wyznaczają jedynie pewien minimalny standard bezpieczeństwa, często nie określając szczegółowych wymagań technicznych lub składników procedur bezpieczeństwa. Elementy te mogą zostać uzupełnione w ramach miękkiego prawa - wytycznych i rekomendacji opracowywanych przez kompetentne podmioty.

W związku z powyższym należy zwrócić uwagę na:

- Obecnie obowiązujące standardy ochrony wynikające wprost z przepisów prawa;
- Nowe zasady bezpieczeństwa danych wprowadzane przez RODO oraz dyrektywę NIS;
- Inne powszechnie stosowane normy – np. Ramy Cyberbezpieczeństwa NIST, normy ISO, oficjalne wytyczne strony publicznej.

2. Zasady ochrony danych osobowych - polityka bezpieczeństwa i instrukcja zarządzania

Zgodnie z ustawą o ochronie danych osobowych, administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Administrator danych prowadzi przy tym dokumentację opisującą sposób przetwarzania danych oraz powyższe środki.

Na wspomnianą dokumentację składa się polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, które prowadzi się w formie pisemnej. Wymagany przez ustawodawcę minimalny zakres treści tych dokumentów obrazuje poniższa tabela:

Polityka bezpieczeństwa

- wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe;
- wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych;
- opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi;
- sposób przepływu danych pomiędzy poszczególnymi systemami;
- określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

Instrukcja zarządzania systemem informatycznym

- procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności;
- stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem;
- procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu;
- procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania;
- sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych;
- sposób zabezpieczenia systemu informatycznego przed działalnością szkodliwego oprogramowania;
- postanowienia dotyczące odnotowywania sposobu realizacji informacji o odbiorcach;
- procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

Zawsze gdy przynajmniej jedno urządzenie systemu informatycznego szpitala, służącego do przetwarzania danych osobowych pacjentów lub personelu placówki, połączone jest z siecią publiczną, konieczne jest także spełnienie wymagań przewidzianych dla wysokiego poziomu bezpieczeństwa przetwarzania danych osobowych określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. Nr 100, poz. 1024). Obejmują one m.in. mechanizmy kontroli dostępu do danych, stosowanie oprogramowania antywirusowego czy stosowanie bezpiecznych haseł.

3. Standardy informatyzacji podmiotów realizujących zadania publiczne

Ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne określa m.in. zasady ustalania minimalnych wymagań dla systemów teleinformatycznych używanych do realizacji zadań publicznych, wymiany informacji w postaci elektronicznej z podmiotami publicznymi oraz ustalania Krajowych Ram Interoperacyjności systemów teleinformatycznych. Znajduje ona zastosowanie m.in. do samodzielnych publicznych zakładów opieki zdrowotnej oraz spółek wykonujących działalność leczniczą w rozumieniu przepisów o działalności leczniczej. W praktyce oznacza to, że powyższe podmioty muszą spełniać normy dotyczące m.in. specyfikacji formatów danych oraz protokołów komunikacyjnych i szyfrujących oraz sposobów zapewnienia bezpieczeństwa przy wymianie informacji.

4. Przepisy prawa medycznego dotyczące bezpieczeństwa danych medycznych

Szczegółowe zasady przetwarzania danych zawartych w dokumentacji medycznej wynikają z norm prawa medycznego. Podmiot udzielający świadczeń zdrowotnych jest obowiązany zapewnić ochronę danych zawartych w dokumentacji, co następuje m.in. poprzez ograniczenie kręgu osób mających dostęp do danych, obowiązek zachowania w tajemnicy informacji związanych z pacjentem czy spełnienie dodatkowych warunków związanych z umową powierzenie przetwarzania danych.

Szczególne wymagania dotyczące dokumentacji prowadzonej w postaci elektronicznej zawierają ponadto przepisy wykonawcze do ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta, w szczególności rozporządzenie Ministra Zdrowia z dnia 9 listopada 2015 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania (Dz.U. z 2015 r. poz. 2069). Zgodnie z nim, dokumentację prowadzoną w postaci elektronicznej, uważa się za zabezpieczoną, jeżeli w sposób ciągły są spełnione łącznie następujące warunki:

1) jest zapewniona jej dostępność wyłącznie dla osób uprawnionych;
2) jest chroniona przed przypadkowym lub nieuprawnionym zniszczeniem;
3) są zastosowane metody i środki ochrony dokumentacji, których skuteczność w czasie ich zastosowania jest powszechnie uznawana.

5. RODO i zatwierdzone kodeksy postępowania

Ogólne rozporządzenie o ochronie danych osobowych wymaga, by administrator wdrażał odpowiednie środki techniczne i organizacyjne uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia. Unijny prawodawca wskazuje, że spełnienie tych wymogów może nastąpić np. poprzez pseudonimizację i szyfrowanie danych osobowych, zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania, zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego czy regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania. Oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Narzędziem mającym ułatwić wywiązanie się z obowiązków dotyczących bezpieczeństwa oraz pomóc w stworzeniu odpowiedniego, proporcjonalnego standardu ochrony są kodeksy postępowania.

Zgodnie z art. 40 ust. 1 ogólnego rozporządzenia o ochronie danych osobowych, państwa członkowskie, organy nadzorcze, Europejska Rada Ochrony Danych oraz Komisja **zachęcają do sporządzania kodeksów postępowania mających pomóc we właściwym stosowaniu RODO** – z uwzględnieniem specyfiki różnych sektorów dokonujących przetwarzania oraz szczególnych potrzeb mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw.

Podmioty chcące opracować kodeks postępowania (lub zmienić lub rozszerzyć zakres dotychczas obowiązujący kodeks), zobowiązane są przedłożyć projekt kodeksu organowi nadzorczemu. W przypadku kodeksu branżowego obowiązującego wyłącznie na terytorium Polski organem tym będzie GIODO, a po wejściu w życie nowej ustawy o ochronie danych osobowych, Prezes Urzędu Ochrony Danych Osobowych. Po przedłożeniu projektu, organ nadzorczy wydaje opinię o zgodności projektu kodeksu z RODO i zatwierdza projekt, jeśli uzna, że stanowi on odpowiednie zabezpieczenie. Następnie organ nadzorczy rejestruje i publikuje kodeks.

Zatwierdzony kodeks postępowania podlega monitorowaniu przez podmiot, który dysponuje odpowiednim poziomem wiedzy w dziedzinie będącej przedmiotem kodeksu i został akredytowany w tym celu przez organ ochrony danych osobowych. Ponadto, zgodnie z art. 41 ust. 4 RODO, podmiot monitorujący musi podejmować aktywne działania wobec sygnatariuszy kodeksu, którzy nie przestrzegają jego zapisów, w tym zawieszać lub wykluczać sygnatariuszy, którzy dopuszczają się najpoważniejszych naruszeń z grona podmiotów stosujących kodeks.

Kodeks branżowy dla ochrony zdrowia, stanowiący instrument miękkiego prawa osadzony (jednak mocno w normach rozporządzenia) będzie więc wyznaczał nowy, powszechny standard ochrony danych osobowych pacjentów, doprecyzowując zasady wynikające wprost z RODO.

Branża medyczna dostrzegła potrzebę przygotowania kodeksu branżowego. W dniu 26 lipca 2017 roku w siedzibie CSIOZ odbyło się spotkanie inaugurujące prace nad kodeksem branżowym dla sektora ochrony zdrowia. Działania na rzecz przygotowania kodeksu branżowego wspierają m.in. Centrum Systemów Informacyjnych Ochrony Zdrowia, Ministerstwo Zdrowia, Centrum Monitorowania Jakości w Ochronie Zdrowia, Polska Federacja Szpitali, Fundacja Telemedyczna Grupa Robocza, Pracodawcy Medycyny Prywatnej, Konfederacja Lewiatan, Polska Izba Informatyki i Telekomunikacji, Federacja Związków Pracodawców Ochrony Zdrowia Porozumienie Zielonogórskie. Ponadto inicjatywa powstania kodeksu uzyskała poparcie Województwa Wielkopolskiego, Naczelnej Izby Pielęgniarek i Położnych, Fundacji My Pacjenci, Fundacji Urszuli Jaworskiej, Naczelnej Izby Aptekarskiej, Krajowej Izby Diagnostów Laboratoryjnych, Krajowej Rady Fizjoterapeutów. Inicjatorem i głównym partnerem merytorycznym prac nad kodeksem jest kancelaria DZP. Inicjatywa ma wsparcie merytoryczne spółki Microsoft Polska.

6. Normy ISO

Niezależnie od wymogów prawnych podstawowe standardy postępowania z danymi osobowymi pacjentów wyznaczają takie powszechnie normy jak ISO/IEC 27001, ISO/IEC 27002 czy ISO/IEC 27018.

Norma ISO/IEC 27001 dotyczy zarządzania bezpieczeństwem informacji. Odnosi się m.in. do takich kwestii jak polityka bezpieczeństwa, organizacja bezpieczeństwa informacji, zarządzanie ciągłością działania czy zgodność z wymaganiami prawnymi. Europejski Komitet Ekonomiczno – Społeczny wskazał na konieczność wdrożenia normy ISO 27001 na szczeblu międzynarodowym w celu zapewnienia bezpieczeństwa danych przetwarzanych w ramach tzw. m-zdrowia.

Norma ISO/IEC 27002 wyznacza zasady ustanowienia, wdrażania, eksploatacji, monitorowania, przeglądu, utrzymania i doskonalenia Systemu Zarządzania Bezpieczeństwem Informacji. Rozwija merytorycznie wytyczne zawarte w normie ISO/IEC 27001.

Norma ISO/IEC 27018 stosowana jest w połączeniu z normą ISO/IEC 27001 i podobnie jako ona odnosi się do procesu zarządzania bezpieczeństwem informacji. Konkretyzuje standardy dotyczące bezpiecznego wykorzystywania publicznej chmury obliczeniowej.

7. Oficjalne wytyczne

W dniu 28 września 2017 roku Centrum Systemów Informacyjnych Ochrony Zdrowia opublikowało finalną wersję dokumentu pt. „Rekomendacje Centrum Systemów Informacyjnych Ochrony Zdrowia w zakresie bezpieczeństwa oraz rozwiązań technologicznych stosowanych podczas przetwarzania dokumentacji medycznej w postaci elektronicznej”[19].

Zgodnie z intencjami autorów, Rekomendacje są przeznaczone dla usługodawców podejmujących decyzję dotyczącą wyboru rozwiązania wykorzystywanego do elektronicznego przetwarzania dokumentacji medycznej, w tym decyzję dotyczącą sposobu zapewnienia bezpieczeństwa przetwarzanych danych. Dokument może być również wykorzystywany przez dostawców, którzy podejmują się projektowania i budowy systemów informatycznych dedykowanych dla ochrony zdrowia. Dokument ten zawiera wiele istotnych wskazówek w zakresie zapewnienia bezpieczeństwa danych medycznych. Rekomendacje podkreślają możliwość zastosowania dowolnych rozwiązań IT, w tym chmurowych w ramach organizacji, jednocześnie jednak autorzy Rekomendacji zwracają uwagę na zasadność zwrócenia uwagi na spełnienie przez dostawców usług IT norm ISO oraz innych relewantnych – jest to istotny element, który należy brać pod uwagę przy podejmowaniu decyzji co do wyboru dostawców IT przez podmioty wykonujące działalność leczniczą. Rekomendacje w osobnym rozdziale odnoszą się również bezpośrednio do zagadnienia cyberbezpieczeństwa.

8. Ramy cyberbezpieczeństwa NIST

Ramy Bezpieczeństwa Cybernetycznego, opracowane przez amerykański Krajowy Instytut Standaryzacji i Technologii (National Institute of Standards and Technology – NIST) to przykład dobrych praktyk, które mogłyby zostać zaadaptowane także przez sektor ochrony zdrowia w Polsce.

Ramy NIST są przykładem określenia minimów bezpieczeństwa, których skuteczność została potwierdzona i które zostały szybko przyjęte powszechnie. Co ważne, Stany Zjednoczone nie są jedynym krajem wykorzystującym Ramy. W Europie w 2015 roku rząd Włoch przyjął nowe Ramy Bezpieczeństwa Cybernetycznego oparte na NIST. Włochy dostosowały Ramy do specyfiki sektora małych i średniej wielkości przedsiębiorstwach.[20] Podobnie, w 2015 roku Australia zachęcała swoich przedsiębiorców do wykorzystania Ram Bezpieczeństwa Cybernetycznego NIST do oszacowania i ograniczenia zagrażających im ryzyk cybernetycznych lub do inwentaryzacji stosowanych przez nich praktyk zarządzania cyber ryzykiem. Zdaniem rządu, zalety Ram to ich skalowalność i możliwość budowania odporności cybernetycznej przedsiębiorstw na jej podstawie w sposób proporcjonalny.[21]

---

[19] https://www.csioz.gov.pl/aktualnosci/szczegoly/rekomendacje-w-zakresie-bezpieczenstwa-oraz-rozwiazan-technologicznych-stosowanych-podczas-przetw/ (dostęp 3 października2017)

[20] Raport o Cyberbezpieczeństwie Włoch, 2015 http://www.cybersecurityframework.it/sites/default/files/CSR2015_ENG.pdf

[21] http://download.asic.gov.au/media/3062900/rep429-published-19-march-2015-1.pdf

Przyjmowanie na świecie Ram Cyberbezpieczeństwa najprawdopodobniej będzie postępowało. Niedawno wydany Dekret Prezydencki na temat Bezpieczeństwa Cybernetycznego[22] nakłada obowiązek stosowania Ram Bezpieczeństwa Cybernetycznego przez wszystkie agendy rządu USA. Ponadto, niedawno Międzynarodowa Organizacja Normalizacyjna (ISO) zatwierdziła podjęcie prac nad raportem technicznym „Bezpieczeństwo cybernetyczne normy ISO i IEC", mających na celu dostosowanie Ram Bezpieczeństwa Cybernetycznego NIST do środowiska międzynarodowego.

8.1 Ramy Bezpieczeństwa Cybernetycznego NIST: Struktura

Ramy Bezpieczeństwa Cybernetycznego NIST oparto na istniejących normach, wytycznych oraz praktykach i zaprojektowano tak, by różne organizacje mogły je wykorzystywać do oceny swoich zagrożeń dla działalności, a następnie wdrażać je w sposób ekonomiczny. Składają się z trzech części:

- **Szkielet ram:** Szkielet jest zbiorem działań i stosownych informacyjnych źródeł odniesienia[23], (czyli norm) podzielonych na pięć funkcji: Rozpoznanie, Ochrona, Wykrywanie, Reagowanie i Odbudowa. Szkielet wskazuje, jak organizacje powinny podchodzić do swoich praktyk w obszarze bezpieczeństwa cybernetycznego w zakresie: 1) określania swoich najbardziej krytycznych zasobów, 2) wdrażania procedur ich ochrony, 3) uwzględniania zasobów niezbędnych do rozpoznawania potencjalnych naruszeń bezpieczeństwa, 4) utrzymywania procedur reagowania na naruszenia oraz 5) tworzenia procedury umożliwiającej im odbudowanie się po ataku.

- **Profil Ram:** Profil zapewnia metodę wspomagającą organizacje w zgrywaniu działań w zakresie bezpieczeństwa cybernetycznego z wymaganiami ich zasadniczej działalności, najlepszymi praktykami branżowymi, zakresem tolerancji ryzyka i zasobami oraz w jasnym wyartykułowaniu celów firmowego programu ochrony bezpieczeństwa cybernetycznego. Umożliwia także ustalenie pożądanych rezultatów ochrony cybernetycznej oraz luk występujących w aktualnych procedurach z tego obszaru.

- **Warstwy Wdrażania Ram:** opisują stopień zaawansowania stosowania w organizacji praktyk z obszaru bezpieczeństwa cybernetycznego. Rozróżnia się cztery poziomy klasyfikujące podejście do zarządzania ryzykiem ataków cybernetycznych, od poziomu „nieformalnego" do „adaptacyjnego":

[22] https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal

[23] Normy uwzględnione w Ramach Bezpieczeństwa Cybernetycznego NIST obejmują:
- CIS Critical Security Controls: https://www.cisecurity.org/critical-controls/
- Control Objectives for Information and Related Technology (COBIT): http://www.isaca.org/cobit/pages/default.aspx
- ISA/IEC-62443: https://www.isa.org/training-and-certifications/isa-certification/isa99iec-62443/isa99iec-62443-cybersecurity-certificate-programs/
- ISO/IEC 27001:2013: http://www.iso.org/iso/catalogue_detail?csnumber=54534
NIST SP 800-53 Rev.4: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.

Warstwa 1 (nieformalnie): organizacja podchodzi do bezpieczeństwa cybernetycznego na zasadach doraźnych. Ma minimalną świadomość zagrożeń cybernetycznych dla organizacji.

Warstwa 2 (ze świadomością ryzyka): organizacja ma politykę zarządzania ryzykiem dla bezpieczeństwa cybernetycznego i prowadzi aktualnie działania mające na celu opracowanie celów zarządzania tym ryzykiem i zrozumienie zagrożeń, jakie niesie ono dla organizacji.

Warstwa 3 (powtarzalnie): organizacja działa zgodnie z formalnymi procedurami dotyczącymi bezpieczeństwa cybernetycznego, które regularnie aktualizuje, dysponuje dobrze przeszkolonym personelem i rozumie współzależności oraz otoczenie swoich partnerów biznesowych.

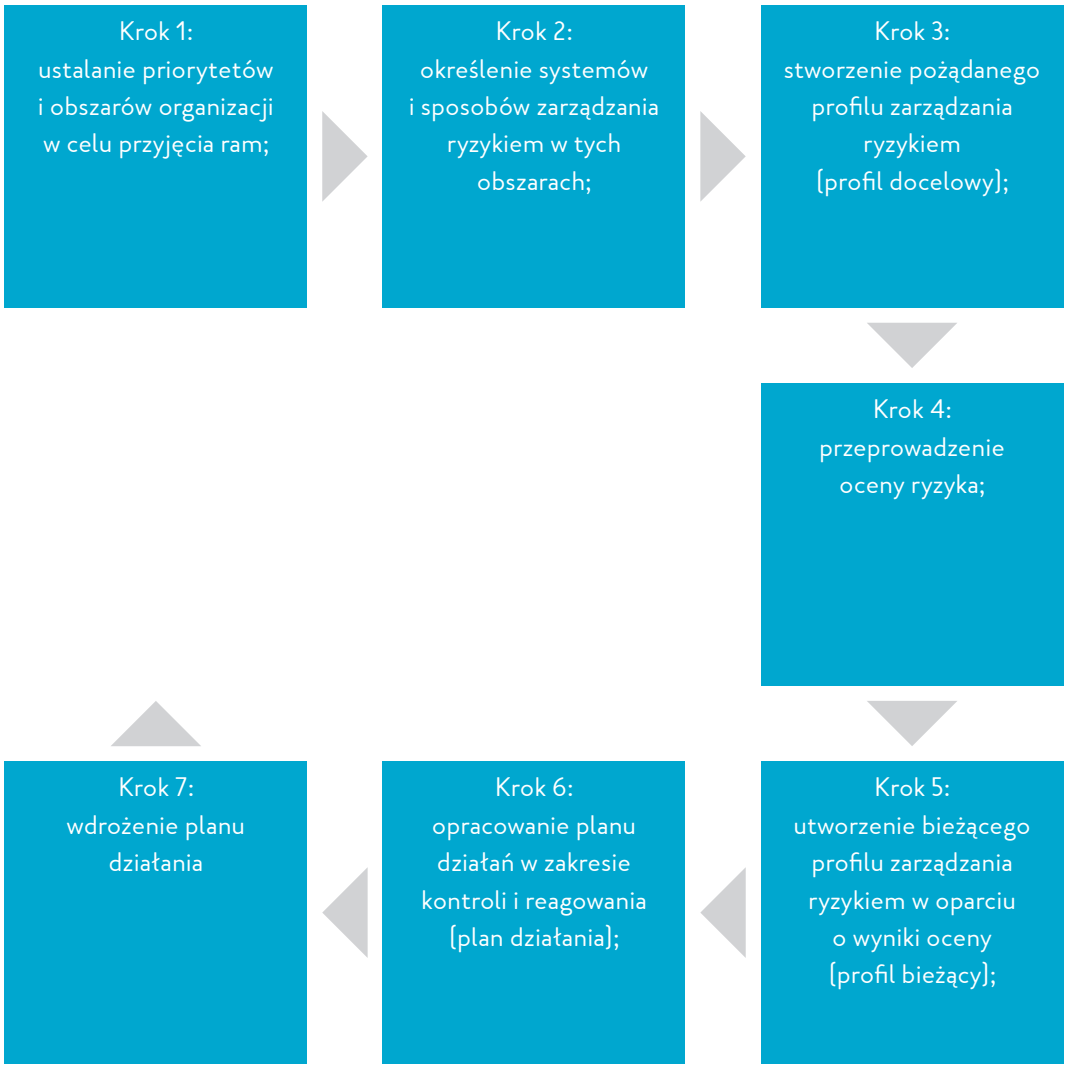
Warstwa 4 (adaptacyjnie): dostosowuje swoje praktyki w obszarze bezpieczeństwa cybernetycznego na bieżąco w oparciu o zachodzące zdarzenia i wskaźniki predykcyjne tworzone na podstawie poprzednich i aktualnych działań w tym obszarze.

8.2 Wdrażanie Ram Bezpieczeństwa Cybernetycznego NIST w sektorze ochrony zdrowia

Działająca w Stanach Zjednoczonych organizacja The Health Information Trust Alliance (HITRUST), współpracując z przedstawicielami sektora ochrony zdrowia, nowych technologii oraz ochrony danych, opracowała wytyczne wdrożeniowe[24], mające wspomóc sektor ochrony zdrowia w tworzeniu lub dostosowaniu istniejących w nim programów ochrony przed zagrożeniami cybernetycznymi do celów Ram Bezpieczeństwa Cybernetycznego NIST. Przy opracowywaniu wytycznych prowadzono konsultacje m.in. z Radą Koordynacji Sektora *(Sector Coordinating Council, SCC)* oraz Departamentem Bezpieczeństwa Wewnętrznego *(Department of Homeland Security, DHS)*.

Proces implementacji w ochronie zdrowia składa się z siedmiu etapów, które ilustruje poniższy diagram. Wdrożenie powinno obejmować, w ramach swojego programu zarządzania ryzykiem, plan przekazywania informacji o postępach właściwym gremiom, takim jak kierownictwo wyższego szczebla. Ponadto każdy krok procesu powinien dostarczać informacji zwrotnych i umożliwiać walidację poprzednich kroków.

[24] https://www.us-cert.gov/sites/default/files/c3vp/framework_guidance/HPH_Framework_Implementation_Guidance.pdf


Krok 1:
ustalanie priorytetów
i obszarów organizacji
w celu przyjęcia ram;
Krok 2:
określenie systemów
i sposobów zarządzania
ryzykiem w tych
obszarach;
Krok 3:
stworzenie pożądanego
profilu zarządzania
ryzykiem
(profil docelowy);
Krok 4:
przeprowadzenie
oceny ryzyka;
Krok 5:
utworzenie bieżącego
profilu zarządzania
ryzykiem w oparciu
o wyniki oceny
(profil bieżący);
Krok 6:
opracowanie planu
działań w zakresie
kontroli i reagowania
(plan działania);
Krok 7:
wdrożenie planu
działania

IV. Podsumowanie i rekomendacje

Zapewnienie wysokiego poziomu bezpieczeństwa danych zawartych w elektronicznej dokumentacji medycznej jest niezmiernie ważne dla poprawnego funkcjonowania systemu ochrony zdrowia. Informacje te są narażone nie tylko na standardowe zagrożenia związane z siecią, ale także zaplanowane i wycelowane bezpośrednio w nie ataki hakerskie. W świetle dotychczasowych problemów polskich szpitali w tym zakresie bardzo ważne będzie właściwe przygotowanie się do nowych standardów wynikających z prawodawstwa unijnego, w szczególności z RODO. Właściwym uzupełnieniem nowych zasad będzie wdrożenie bardziej szczegółowych rozwiązań wynikających z sektorowych kodeksów postępowania oraz ram cyberbezpieczeństwa NIST.

Zarządzający podmiotami wykonującymi działalność leczniczą powinni podjąć wysiłek dla podniesienia poziomu cyberbezpieczeństwa. Dotyczy to oczywiście kwestii informatycznych i technicznych, ale również proceduralnych i regulacyjnych. Rekomendujemy w szczególności następujące działania:

1. Wdrożenie przepisów RODO, z uwzględnieniem zapisów opracowywanego przez branżę kodeksu branżowego dla sektora ochrony zdrowia i złożenie deklaracji o przestrzeganiu kodeksu branżowego (oraz poddawanie się ocenie przez niezależny podmiot monitorujący przestrzeganie kodeksu).

2. Dokonanie przeglądu i wdrożenie aktualnych Rekomendacji przygotowanych przez CSIOZ, w tym zwrócenie uwagi na wiarygodność podmiotów przetwarzających, z których usług korzysta placówka medyczne.

3. Analiza i w jej wyniku zmiana struktury organizacyjnej oraz mechanizmów zarządczych oraz procedur mająca na celu przygotowanie organizacji do działań po poważnym incydencie naruszającym cyberbezpieczeństwo.

4. Rozważenie wprowadzenia zasad i polityk w ramach organizacji opartych na dobrych praktykach, obowiązujących przepisach a także na standardach międzynarodowych takich jak NIST.

Biuro w Warszawie
Rondo ONZ 1
00-124 Warszawa
T +48 22 557 76 00
F +48 22 557 76 01

Biuro w Poznaniu
ul. Paderewskiego 8
61-770 Poznań
T +48 61 642 49 00
F +48 61 642 49 50

Biuro we Wrocławiu
ul. Gwiaździsta 66
53-413 Wrocław
T +48 71 712 47 00
F +48 71 712 47 50

Domański Zakrzewski Palinka sp.k.
www.dzp.pl