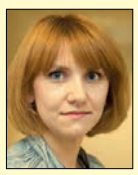
Samorządy i szpitale lekceważą hakerów. A mogą za to słono zapłacić

Zofia Jóźwiak
zofia.jozwiak@infor.pl

Październikowy raport, przygotowany przez jedną z kancelarii prawnych, pokazuje, jak bardzo kuleje cyberochrona w służbie zdrowia i w samorządach. Niby wszyscy wiedzą o wchodzącym wiosną rozporządzeniu w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (RODO), to jednak nowe obowiązki w tym zakresie traktowane są po macoszemu. Za wiedzą nie idą bowiem żadne działania, choć niedopatrzenia w tym zakresie będą słono kosztować. Co więcej, wiosną 2018 r. powinna też zostać wdrożona do polskiego prawa dyrektywa w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (NIS).

Skąd ten marazm? Jeśli chodzi o samorządy, które często są też organami założycielskimi dla placówek służby zdrowia, to – jak wynika z raportu – wina leży przede wszystkim w mentalności urzędników, którzy twierdzą, że ich sieci są bezpieczne? Uważają, że dostatecznie je chronią np. programy... antywirusowe. Tymczasem zabezpieczanie e-danych jest o wiele bardziej skomplikowane. Co więcej, nowe europejskie akty nie narzucają konkretnego sposobu ich ochrony. Ma być ona taka, by dane były bezpieczne, a podejmowane działania nadążały za pomysłami cyberprzestępców. A to jest znacznie trudniejsze niż dostosowanie się do dzisiejszych przepisów. Bo trzeba na bieżąco śledzić działania hakerów. To duże wyzwanie, szczególnie dla placówek służby zdrowia. Wprawdzie cyfryzacja w tej branży postępuje u nas obecnie powoli, to danych medycznych gromadzonych w sieci będzie coraz więcej. A to m.in. za sprawą ustawy o systemie informacji w ochronie zdrowia, która nakłada na placówki konkretne terminy posługiwania się e-dokumentacją. Te dane są wyjątkowo narażone na ataki hakerów, którzy ze skradzionych plików dowiadują się nie tylko o wieku czy adresie danej osoby, ale również o zażywanych lekach, zabiegach czy nałogach. Niebezpieczeństwo jest tym większe, że tego typu danych nie da się zmienić, tak jak np. numeru konta bankowego. ©℗



SYLWIA CZUBKOWSKA
sylwia.czubkowska@infor.pl

Dane z publicznych instytucji cennym łupem dla cyberprzestępców

Przez lokalne urzędy, a także szpitale czy przychodnie zdrowia przepływają miliardy złotych i wrażliwe dane milionów ludzi. Trudno się więc dziwić, że i one, podobnie jak banki czy firmy energetyczne, są narażone na cyberataki. Ale często zamiast dbać o bezpieczeństwo, oszczędzają na nim

Szokiem dla dziesiątek firm i instytucji w całej Europie był 12 maja 2017 r. To właśnie tego dnia na własnej skórze doświadczyły one działania ransomware, które dotychczas znały tylko z doniesień medialnych. Wykorzystując to złośliwe oprogramowanie zaszyfrowujące dyski do momentu zapłacenia przez właściciela urządzenia okupu (ransome), przestępcy uderzyli naprawdę na masową skalę. Przy czym nie mieli skrupułów – wśród zaatakowanych znalazły się bowiem nawet publiczne brytyjskie szpitale. „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" – opisuje w raporcie dotyczącym zagadnienia cyberbezpieczeństwa w sektorze ochrony zdrowia oraz w samorządach kancelaria prawna Domański Zakrzewski Palinka oraz spółka Microsoft.

Ataki hakerów bynajmniej nie omijają Polski. Styczeń 2016 r. – prokuratura zakończyła kilkumiesięczne śledztwo w sprawie cyberoszustw, przez które pięć śląskich gmin straciło w sumie ponad 2 mln zł. Przestępcy stworzyli specjalny program podmieniający numer rachunku, na który samorządy wysyłały przelewy. W efekcie pieniądze zamiast docierać do adresata, przepadały jak kamień w wodę. Ta historia nie jest wyjątkiem. Samorządy i służba zdrowia regularnie i w coraz większej skali stają się celem e-przestępców. I jak przewidują specjaliści, to dopiero początek problemów w tych instytucjach. A ostatnim momentem, by przygotowały się na taką rzeczywistość, jest obowiązek wdrożenia w maju przyszłego roku dwóch ważnych unijnych aktów prawnych: rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 (RODO), czyli reformy ochrony danych osobowych, a także dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (dyrektywa NIS), która – jak informuje resort cyfryzacji – powinna być implementowana polską ustawą wiosną przyszłego roku.

> **W przypadku kradzieży danych medycznych doprowadzenie do stanu sprzed kradzieży jest wręcz niemożliwe. Dzięki statycznej naturze zawartych w nich informacji przestępcy mają sporo czasu, aby je przeanalizować, przetwarzać, a następnie z nich korzystać**
>
> **Jolanta Malak**
> regionalna dyrektor sprzedaży Fortinet

Połowa bez szkoleń

– Przedsiębiorcy i administracja przygotowują się na odpieranie cyberataków. I choć świadomość wśród nich nie jest może powszechna, to powoli rośnie. Coraz więcej firm i instytucji zaczyna faktycznie przejmować się ochroną danych głównie z powodu RODO – zauważa Katarzyna Szymielewicz z Fundacji Panoptykon. – Ale rzeczywiście w służbie zdrowia i samorządach jest dużo gorzej. Nie ma dla nich ani specjalnie jakichś rozbudowanych akcji informacyjnych, ani szkoleń. A to ogromny błąd, bo przecież przepisy RODO jak i dyrektywy NIS też je obejmą. A cyberzagrożenia przecież magicznie ich nie ominą – dodaje Szymielewicz.

Faktycznie samorządy nie są na nie przygotowane, o czym kilka miesięcy temu informował Jan Maciej Czajkowski z Komisji Wspólnej Rządu i Samorządu Terytorialnego w trakcie konferencji „Cyberbezpieczeństwo w jednostkach samorządu terytorialnego". – Pracownicy połowy samorządów nie przechodzą żadnego przeszkolenia w obszarze cyberbezpieczeństwa. Powodem jest brak środków – dodał.

Optymistycznie nie nastrajają także wyniki ubiegłorocznego badania przeprowadzonego na 200 urzędnikach odpowiedzialnych za informatykę w mniejszych i większych urzędach samorządowych. Zostały one przygotowane na zlecenie firmy Fortinet. Wynika z nich, że co trzecia jed-

nostka nie ma na wyposażeniu nawet podstawowego zabezpieczenia przed cyberatakami, jakim jest firewall. Jeśli urzędnicy już sięgają po jakieś tego rodzaju oprogramowanie, to jest to zwyczajny antyspam. Przy czym samorządowcy oczywiście zapewniają, że jest u nich bezpiecznie (tak twierdzi aż dwie trzecie z nich), ale już odpowiedź na pytanie o to, jak urząd zadbał o to bezpieczeństwo, niestety pokazuje smutną prawdę: lokalne urzędy na swoim cyberbezpieczeństwie niebezpiecznie oszczędzają.

Niewiele lepiej jest w służbie zdrowia. Owszem jej placówki coraz lepiej dbają o to, by działały w nich systemy do elektronicznego obiegu dokumentacji (zresztą wymaga od nich tego prawo), ale niestety o wiele słabiej jest w przypadku ochrony danych zawartych w tej dokumentacji. Potwierdza to choćby kontrola przeprowadzona w ubiegłym roku przez Najwyższą Izbę Kontroli „Tworzenie i udostępnianie dokumentacji medycznej". Wynika z niej, że szpitale mają problemy z przestrzeganiem zasad prowadzenia dokumentacji medycznej i ochrony danych osobowych. Przy czym izba stwierdziła, że do czasu zakończenia kontroli żaden z objętych nią 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). Niestety, te, które posługują się e-dokumentacją, mają problemy z jej ochroną. Jak wynika z raportu kancelarii DZP oraz spółki Microsoft, dotyczącego zagadnienia cyberbezpieczeństwa w sektorze ochrony zdrowia oraz w samorządach, w czerwcu 2017 r. doszło do wycieku danych ok. 50 tys. pacjentów Samodzielnego Publicznego Zakładu Opieki Zdrowotnej w Kole. Oprócz danych identyfikacyjnych (nazwiska, adresy, numery PESEL) wyciekły także dane medyczne – historia choroby czy grupa krwi. W wyniku doniesień prasowych interwencję podjął rzecznik praw obywatelskich. Zwrócił się on do ministra zdrowia i generalnego inspektora ochrony danych osobowych z prośbą o wyjaśnienia oraz wskazanie, czy resort systemowo interesuje się kwestią zabezpieczania danych.

Kluczowe instytucje

To, że bankowość (instytucje finansowe), a także energetyka, transport czy komunikacja są elementami infrastruktury krytycznej państwa, nie podlega dyskusjom. A czy w świadomości decydentów (zarówno na szczeblu rządowym, jak i lokalnym) należą do niej także placówki służby zdrowia i urzędy np. gmin? Teoretycznie tak, jednak w praktyce różnie to bywa.

– Samorządy przetwarzają nie tylko ogromne ilości szczególnie wrażliwych danych osobowych, włącznie z numerami PESEL, danymi z dowodów osobistych, adresami zameldowania, czyli z kompletem informacji, dzięki którym przestępca może np. stworzyć fałszywy dowód osobisty i wyłudzić kredyt, ale również obracają dużymi sumami publicznych pieniędzy. Dlatego jakiekolwiek wdrożenie infrastruktury zabezpieczającej powinno być w nich przeprowadzane szczególnie starannie i z odpowiednim planowaniem oraz rozeznaniem potrzeb – podkreśla Jolanta Malak, regionalna dyrektor sprzedaży Fortinet. Dodaje jednak, że główną barierą rozwoju cyberbezpieczeństwa w JST jest brak funduszy, a w dalszej kolejności niska świadomość problemu na wyższych szczeblach administracyjnych. Niewystarczające jest też wykorzystanie środków unijnych na informatyzację – aż 87 proc. urzędów badanych przez Fortinet finansowało inwestycje w infrastrukturę zabezpieczającą ze środków własnych.

W przypadku ochrony zdrowia należy z kolei pamiętać, że tego typu placówki gromadzą wiele wrażliwych danych pacjentów, na tyle cennych, że na czarnym rynku są one bardziej wartościowe niż np. dane dostępu do konta czy karty kredytowej. – O ile te ostatnie mają krótki okres przydatności dla przestępców, tak dane z rejestrów medycznych mogą być przetwarzane przez o wiele dłuższy czas. Kiedy oszust wykorzystuje do popełnienia przestępstwa informacje z konta bankowego lub karty kredytowej, ukrócenie tego procederu z reguły jest stosunkowo proste. Instytucja finansowa po prostu blokuje kartę czy możliwość wykonywania operacji na koncie i wydaje nowe dokumenty – tłumaczy Malak. – W przypadku kradzieży danych medycznych doprowadzenie do stanu sprzed kradzieży jest wręcz niemożliwe. Dzięki statycznej naturze zawartych w nich informacji przestępcy mają sporo czasu, aby je przeanalizować, przetworzyć, a następnie z nich korzystać – tłumaczy ekspertka.

Jaki może być tego efekt? „Przeprowadzone w Stanach Zjednoczonych badania wskazują, że co dziesiąty podmiot leczniczy doświadcza próby włamania każdego dnia. Branża medyczna, pomimo rosnącej liczby cyberataków, wciąż wydaje się być zapóźniona w porównaniu z sektorem finansowym, również przetwarzającym olbrzymie ilości danych wrażliwych i poufnych. Banki posiadają osobne działy IT/cyberbezpieczeństwa zatrudniające niejednokrotnie kilkudziesięciu profesjonalistów, a także zatrudniają zewnętrze firmy specjalizujące się w zapewnianiu wysokiego poziomu cyberbezpieczeństwa" – czytamy w raporcie DZP.

Termin się zbliża

Katalizatorem zmian może być coraz bliższy termin wejścia w życie dwóch wspomnianych już europejskich aktów prawnych. W końcu oba nakładają na wszystkich uczestników rynku konkretne obowiązki. Przede wszystkim wymagają, by administrator wdrażał odpowiednie środki techniczne i organizacyjne tak, by jak najbardziej ograniczyć ryzyko naruszenia praw lub wolności osób fizycznych (zarówno pacjentów, jak i pacjentów). – Niemal 13 proc. osób odpowiedzialnych za IT w większych jednostkach samorządu dostrzega problem braku centralnej strategii i standardów bezpieczeństwa informatycznego. Należy pamiętać, że cyberbezpieczeństwo jest procesem, który wymaga stałego odpowiadania na nowo pojawiające się zagrożenia. Idealnym rozwiązaniem byłoby, gdyby polityki samorządów dotyczące cyberbezpieczeństwa były na bieżąco weryfikowane pod kątem nowych potrzeb – podkreśla ekspertka Fortinet.

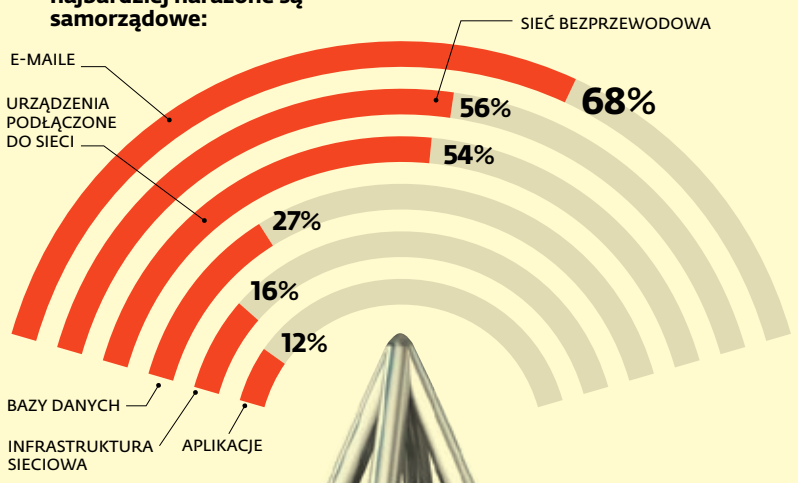
Takie właśnie spojrzenie na kwestie bezpieczeństwa proponuje RODO. – Dyrektywa RODO to tak naprawdę regulacja cyberbezpieczeństwa z konkretnym deadlinem, a NIS to taki „rolling forcast", czyli prognoza, której wdrożenie przesuwa się nieustannie w przyszłość. I dlatego wprowadzenie obu dokumentów będzie trudnym procesem zarówno dla samorządów, jak i placówek ochrony zdrowia. Przy czym nie są tylko jakieś grupy nowych przepisów. Tutaj kluczowe jest to, że RODO I NIS wymagają przeprowadzania nieustającej analizy ryzyka, czyli ich wdrażanie nie kończy się za jednym zamachem, cały czas trzeba będzie się dostosowywać do zmieniającego się otoczenia – podkreśla Michał Jaworski, dyrektor ds. polityki korporacyjnej Microsoftu. I dodaje: – Nikt nie pisze na twardo, że wystarczające jest jakieś konkretne zabezpieczenie, bo przecież za chwilę może ono okazać się nieaktualne. Zamiast tego nakładane są po prostu obowiązki dochowania bezpieczeństwa. Dla polskich instytucji to bardzo trudne do przetrawienia. U nas wszyscy potrzebują dokładnej wy-

> **Unijne akty nie określają twardo, że wystarczające jest konkretne zabezpieczenie, bo za chwilę może okazać się ono nieaktualne. Zamiast tego nakładane są obowiązki dochowania bezpieczeństwa. Dla polskich instytucji to bardzo trudne do przetrawienia. U nas wszyscy potrzebują dokładnej wykładni. Stąd choćby ciągłe odkładanie wdrażania RODO**
>
> **Michał Jaworski**
> dyrektor ds. polityki korporacyjnej Microsoft

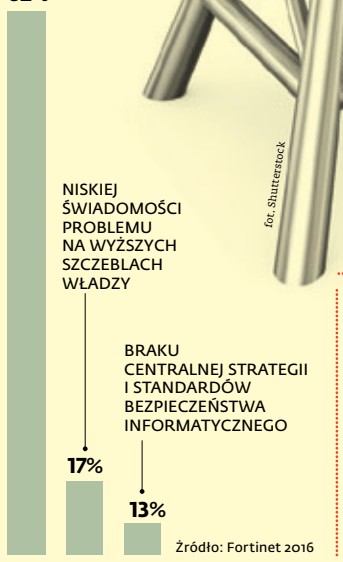
CYBERATAKI PRZYNOSZĄ MILIARDOWE STRATY

SAMORZĄDOWI INFORMATYCY O ZAGROŻENIACH

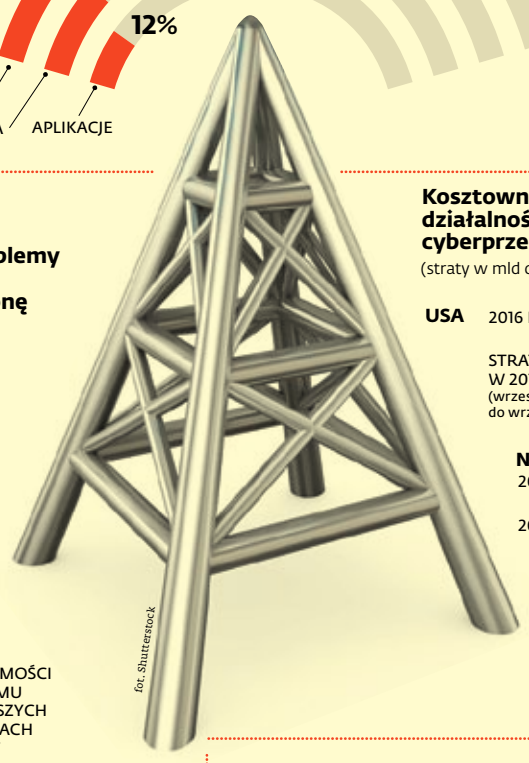
Zdaniem respondentów na ataki hakerów najbardziej narażone są samorządowe:



Zdaniem urzędników JST mają problemy z dbaniem o cyberochronę z powodu:

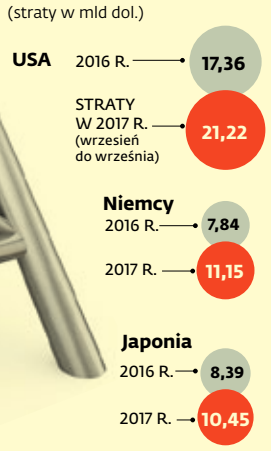


Źródło: Fortinet 2016



fot. Shutterstock

Kosztowna działalność cyberprzestępców
(straty w mld dol.)

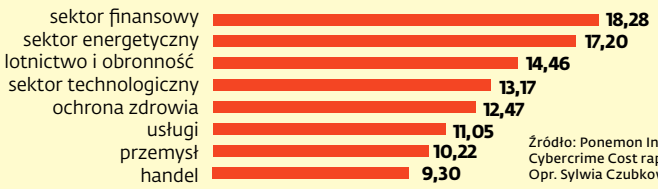


Kto ponosi największe koszty

11,7 mln dol.

TYLE ŚREDNIO ROCZNIE Z POWODU CYBERPRZESTĘPSTW TRACI FIRMA W USA

Średni roczny koszt strat amerykańskiej firmy w zależności od tego, czym się zajmuje, wynosi:
(mln dol.)



RM

Źródło: Ponemon Institute, Cybercrime Cost raport 2017. Opr. Sylwia Czubkowska

Jak poprawić cyberbezpieczeństwo
– rekomendacje z raportu DZP i Microsoft

- Wdrożenie przepisów RODO.
- Analiza i w jej wyniku zmiana struktury organizacyjnej oraz mechanizmów zarządczych mająca na celu przygotowanie organizacji do działań po poważnym incydencie naruszającym cyberbezpieczeństwo.
- Stworzenie koncepcji samorządowego klastra cyberbezpieczeństwa zgodnie z zaleceniami Krajowych Ram Cyberbezpieczeństwa.
- Dokonanie przeglądu i wdrożenie aktualnych rekomendacji przygotowanych przez CSIOZ, w tym zwrócenie uwagi na wiarygodność podmiotów przetwarzających, z których usług korzysta placówka medyczna.
- 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.
- Przyjęcie branżowego kodeksu postępowania dotyczącego ochrony danych osobowych tak dla samorządów jak i kodeksu dla dla sektora ochrony zdrowia i złożenie deklaracji o przestrzeganiu kodeksu branżowego (oraz poddawanie się ocenie przez niezależny podmiot monitorujący przestrzeganie kodeksu.
- Wypracowanie dobrych praktyk w zakresie cyberochrony, opartych na doświadczeniach zdobytych dotychczas przez JST, doświadczeniach firm prywatnych.

kładni. Stąd choćby to ciągłe odkładanie wdrażania RODO, bo „czekamy na ustawy, na rozporządzenia – stwierdza Jaworski.

By udało się takie zapisane dosyć płynnie zasady wdrożyć, eksperci wskazują kilka ścieżek działania. Jedną z nich jest opracowanie, a potem pilnowanie branżowego kodeksu postępowania. „Kodeks branżowy jednostek samorządu terytorialnego lub kodeksy przedsiębiorstw komunalnych różnych branż, stanowiące instrumenty miękkiego prawa, osadzone jednak mocno w normach rozporządzenia, wyznaczałyby nowy, powszechny standard ochrony danych, doprecyzowując zasady wynikające wprost z RODO – przekonują prawnicy z kancelarii Domański Zakrzewski Palinka. Dodają, że należy jednak pamiętać, że regulacje prawne wyznaczają jedynie pewien minimalny standard bezpieczeństwa, często nie określając szczegółowych wymagań technicznych lub składników procedur bezpieczeństwa. – W przypadku RODO katalizatorem do podjęcia prac i poprawiania zabezpieczeń oraz procedur są bardzo wysokie kary, sięgające nawet 4 proc. globalnego obrotu instytucji. Tyle że w przypadku instytucji publicznych mają być one o wiele łagodniejsze – projekt mówi o 100 tys. zł kary za wyciek danych. To jednak powoduje, że sektor publiczny podchodzi do wielkiej reformy ochrony danych ze znacznie silniejszym poczuciem „jakoś to będzie” – podkreśla Michał Jaworski. – To oczywiście ogromny błąd – dodaje.

Jak ogromny – pokażą kolejne cyberataki.

Od kiedy obowiązkowe e-dokumenty

Dokumentacja medyczna w formie elektronicznej*	od 1 stycznia 2019 r.
E-recepty	od 1 stycznia 2020 r.
E-skierowania	od 1 stycznia 2021 r.
Udostępnianie EDM za pośrednictwem SIM	od 1 stycznia 2021 r.

* Skierowany do konsultacji publicznych projekt rozporządzenia ministra zdrowia w sprawie rodzajów elektronicznej dokumentacji medycznej na chwilę obecną wskazuje trzy rodzaje elektronicznej dokumentacji medycznej: informację o rozpoznaniu choroby, problemu zdrowotnego lub urazu, wynikach przeprowadzonych badań, przyczynie odmowy przyjęcia do szpitala, udzielonych świadczeniach zdrowotnych oraz ewentualnych zaleceniach - w przypadku odmowy przyjęcia pacjenta do szpitala, informację dla lekarza kierującego świadczeniobiorcę oraz kartę informacyjną z leczenia szpitalnego, która stanowi dokumentację indywidualną zewnętrzną.

E-zdrowie pełne zalet, ale trzeba uważać

Gromadzenie danych w sieci i telemedycyna to wielka szansa dla leczących i pacjentów. Jednak pod warunkiem, że nikt tych danych w bezprawny sposób nie usunie lub nie wykradnie.

PIOTR NAJBUK
prawnik i lekarz, Domański Zakrzewski Palinka sp. k.

PAWEŁ KAŹMIERCZYK
prawnik, Domański Zakrzewski Palinka sp. k.

WOJCIECH DZIOMDZIORA
radca prawny

Coraz więcej informacji gromadzonych i wykorzystywanych przez podmioty wykonujące działalność leczniczą przybiera postać cyfrową. Wśród nich znajdują się dane o różnym charakterze, w tym m.in. identyfikacyjne pacjentów i dotyczące ich stanu zdrowia, przebiegu leczenia czy zażywanych leków. System obiegu elektronicznej dokumentacji medycznej, świadczenia telemedyczne czy wirtualne konta pacjenta, to tylko przykłady rozwiązań, które mają usprawnić komunikację na linii pacjent – podmiot leczniczy. O ile sam kierunek, jakim jest e-zdrowie, jest powszechnie akceptowany i wydaje się koniecznością, o tyle problemem może się okazać droga do niego. Cyfrowe dane obywateli – w tym w szczególności wrażliwe dane zdrowotne – narażone są na nowe niebezpieczeństwa, przed którymi placówki lecznicze muszą być w stanie skutecznie się bronić.

Znaczące ułatwienie

Jednym z największych wyzwań stojących przed medycyną w XXI w. jest pełne wykorzystanie możliwości oferowanych przez nowe technologie. I nie chodzi jedynie o bardzo zaawansowane, specjalistyczne projekty medyczne. Przemyślane wdrożenia takich rozwiązań jak komunikatory internetowe, aplikacje analityczne, chmura obliczeniowa czy elektroniczna dokumentacja pozwala znacznie usprawnić proces leczenia i zarządzania placówką medyczną. Tym bardziej że codzienna praca szpitala generuje bardzo dużą ilość różnych informacji, które nie są zazwyczaj do końca wykorzystywane. Utrwalane w formie papierowego dokumentu po wypisaniu pacjenta trafiają do archiwum. Dlatego priorytetem procesu informatyzacji systemu ochrony zdrowia jest wprowadzenie elektronicznej dokumentacji medycznej, która zawiera cyfrowe informacje o stanie zdrowia pacjentów. Mogą być łatwo poddane operacjom przez specjalnie w tym celu zaprojektowane aplikacje analityczne, które szybko zauważą w nich to, co nieuchwytne dla człowieka. Technologie umożliwiają także przełamanie barier, które ograniczały dotąd możliwość kontaktu z lekarzem lub pielęgniarką. Dzięki telemedycynie w znacznym stopniu może być rozwiązany problem niewystarczającej liczby specjalistów oraz niskiej dostępności do opieki zdrowotnej na terenach wiejskich. Lekarz udzielając świadczenia za pośrednictwem systemu teleinformatycznego lub innego systemu łączności, może bowiem zbadać pacjenta bez konieczności bezpośredniego kontaktu z nim. Co więcej, komunikatory internetowe poza możliwością widzenia i słyszenia osoby znajdującej się po drugiej stronie, umożliwiają przesyłanie także bardziej zaawansowanych informacji, np. danych obrazowych (takich jak zdjęcia EKG czy USG) czy osłuchowych (transmisja zapisu dźwięku z elektronicznego stetoskopu).

W kierunku e-zdrowia ewoluuje także polski system ochrony zdrowia. Jednak w procesie cyfryzacji danych medycznych należy pamiętać, że niezbędnym warunkiem osiągnięcia korzyści jest zapewnienie niezawodnych i odpornych systemów, które gwarantują szybki i niezakłócony dostęp do danych.

Gdzie jesteśmy i co nas czeka?

Niestety, polski system ochrony zdrowia zmaga się z wieloma poważnymi problemami, dlatego dokonująca się w nim rewolucja cyfrowa jest jeszcze trudno dostrzegalna i przesuwana na później – wynika z przedstawionego przez DZP i firmy Microsoft raportu. Wyraźne zmiany widać jednak w zakresie prawa medycznego, którego otwartość na nowe technologie może być stawiana jako wzorzec dla innych podobnych regulacji w Europie i na świecie.

Jednym z pierwszych kroków w kierunku zapewnienia sprawnego i bezpiecznego systemu elektronicznej informacji o pacjencie była przyjęta 28 kwietnia 2011 r. ustawa o systemie informacji w ochronie zdrowia (t.j. Dz.U. z 2017 r. poz. 1845). Akt ten reguluje system informacji w ochronie zdrowia, który jest wykorzystywany do prowadzenia polityki zdrowotnej państwa, podnoszenia jakości i dostępności świadczeń opieki zdrowotnej oraz finansowania zadań z zakresu ochrony zdrowia. Niestety obowiązek wprowadzenia elektronicznej dokumentacji medycznej, zaplanowany pierwotnie na 31 lipca 2014 r., był jednak kilkukrotnie przesuwany w czasie – najpierw do 31 lipca 2017 r., potem 31 grudnia 2017 r. Ostatnia nowelizacja, wprowadzona ustawą z 20 lipca 2017 r. o zmianie ustawy o systemie informacji w ochronie zdrowia oraz niektórych innych ustaw, przesunęła pełną funkcjonalność systemu na 1 stycznia 2021 r.

Kolejnym krokiem milowym w kierunku e-zdrowia była nowelizacja woe;wielu ustaw z zakresu prawa medycznego, która weszła w życie 15 grudnia 2015 r. Ustawodawca wskazał w niej wyraźnie, że dopuszczalne jest udzielanie świadczeń telemedycznych – w ustawie o działalności leczniczej doprecyzowano, że działalność lecznicza polega na udzielaniu świadczeń zdrowotnych, a te mogą być zaś udzielane za pośrednictwem systemów teleinformatycznych lub systemów łączności. Również lekarze zyskali możliwość orzekania o stanie zdrowia określonej osoby po zbadaniu jej za pośrednictwem narzędzi telemedycznych.

W ramach przywołanej nowelizacji wprowadzono też często niewidoczne dla lekarzy i pacjentów rozwiązanie, które znacząco usprawnia proces informatyzacji – możliwość outsourcingu danych medycznych. Obecnie podmioty wykonujące działalność leczniczą mogą zawierać z dostawcami usług IT umowę powierzenia przetwarzania tego typu danych.

Na podstawie tego typu kontraktów zlecają wykonywanie części zadań związanych z gospodarowaniem informacją. Dzięki outsourcingowi możliwe jest np. wykorzystanie najnowocześniejszej infrastruktury oferowanej m.in. przez dostawców usług chmurowych. Nie dziwi więc, że także krajowa polityka z zakresu ochrony zdrowia podąża w tym kierunku. Pod koniec września 2017 r. w siedzibie Ministerstwa Zdrowia odbyło się spotkanie rozpoczynające prace nad Strategią e-Zdrowia w Polsce na lata 2018–2020. Eksperci mają opracować plan działań przybliżających polski system ochrony zdrowia do nowych, cyfrowych standardów do końca 2017 roku. Planując rozwój e-zdrowia, należy pamiętać, że związane z nim korzyści mogą być osiągnięte, jeśli odpowiedni zakres danych medycznych będzie gromadzony i przetwarzany w odpowiedzialny sposób, a także udostępniany tylko upoważnionym podmiotom i to w uzasadnionych przypadkach. Kluczem do sprawnego działania systemu jest bezpieczeństwo – każda utrata lub opóźnienie w dostępie do danych medycznych może stanowić zagrożenie zdrowia lub życia. Wyciek danych dotyczących przebytych chorób lub zażywanych leków może także oznaczać osobiste problemy dla pacjenta, którego dotyczą informacje.

Nowe szanse, nowe ryzyka

Cyfryzacja danych, o ile niesie ze sobą wiele korzyści dla podmiotów wykonujących działalność leczniczą i pacjentów, wiąże się także z szeregiem nowych zagrożeń, na które trzeba się odpowiednio przygotować. Dla przetwarzania informacji w tradycyjnej, papierowej formie największym zagrożeniem były incydenty grożące jej fizycznym zniszczeniem (pożary, podtopienia, próby zniszczenia czy wykradzenia przez włamanie do archiwum czy też często spotykany bałagan, który skutkował niemożnością uzyskania dostępu do danych we właściwym czasie). Stosowane środki były i nadal są dostosowane przede wszystkim do tego typu zagrożeń – systemy przeciwpożarowe, przechowywanie najcenniejszych materiałów w sejfach, wewnętrzne procedury obiegu dokumentów, ochrona monitorująca budynek, w którym przechowywane są dane.

Dane w formie cyfrowej, oprócz tradycyjnych zagrożeń (pożar serwerowni, kradzież dysku twardego) narażone są ponadto na zupełnie nowy obszar ryzyka, jakim jest podłączenie do sieci publicznej i działanie złośliwego oprogramowania. Podmioty wykonujące działalność leczniczą mogą stać się ofiarą ataków o podłożu terrorystycznym, których celem jest paraliż funkcjonowania państwa i stworzenie realnego zagrożenia dla życia i zdrowia obywateli (np. zablokowanie systemów informatycznych w szpitalach wojskowych), jak również e-przestępstw o podłożu majątkowym. Celem tych drugich jest wykradzenie informacji, które mogą być dalej odsprzedane lub posłużyć jako podstawa szantażu.

WAŻNE Podmioty wykonujące działalność leczniczą mogą stać się ofiarą ataków terrorystycznych. Ich celem może być paraliż funkcjonowania państwa i stworzenie realnego zagrożenia dla życia i zdrowia obywateli (np. zablokowanie systemów informatycznych w szpitalach wojskowych), jak również e-przestępstw o podłożu majątkowym.

W stronę wspólnej cyfrowej opieki

Korzyści związane z cyfryzacją danych, nie tylko w ochronie zdrowia, ale szerzej w administracji publicznej, dostrzegła m.in. Komisja Europejska. W komunikacie z 19 kwietnia 2016 r. przedstawiła plan działania UE na rzecz administracji elektronicznej na lata 2016-2020 – przyspieszenie transformacji cyfrowej w administracji, który zakłada modernizację funkcjonowania administracji publicznych w całej Unii Europejskiej. Zgodnie z założeniami Komisji „do 2020 r. administracje publiczne i instytucje publiczne w Unii Europejskiej powinny być otwarte, efektywne i powszechne (...) Administracje publiczne wykorzystają możliwości, jakie oferuje nowe środowisko cyfrowe, aby ułatwić nawiązywanie kontaktów z zainteresowanymi podmiotami i ze sobą nawzajem”.

KE zwraca uwagę, że wdrażając inicjatywy w ramach planu, w tym m.in. przejście państw członkowskich na e-zamówienia i stosowanie przez nie rejestrów umów, identyfikacji elektronicznej i podpisu elektronicznego czy też wspieranie państw członkowskich w rozwijaniu transgranicznych usług w zakresie e-zdrowia, kluczowymi wartościami mają być niezawodność i bezpieczeństwo. Oznacza to potrzebę zapewnienia wyższego poziomu ochrony danych osobowych, prywatności i bezpieczeństwa informatycznego, niż wynikałoby to ze zwykłej zgodności z ramami prawnymi w tych dziedzinach.

W ślad za planami strategicznymi idzie prawodawstwo wspólnotowe. Unia Europejska zmierza do wyznaczenia wspólnych, minimalnych standardów cyberbezpieczeństwa. Wśród najważniejszych inicjatyw z tego zakresu należy wymienić rozporządzenie RODO, którego normy zaczną obowiązywać od 25 maja 2018 r. Wyznacza ono nowy, wyższy standard ochrony danych dotyczących osób fizycznych, w tym m.in. danych dotyczących ich stanu zdrowia. Od 1 lipca 2016 r. stosuje się już przepisy rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z 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 NIS.

W kontekście cyberbezpieczeństwa szczególnie istotny jest ostatni akt. U podstaw jego przyjęcia legły dwa stwierdzenia: pierwsze – państwa nie są obecnie w stanie zapewnić wysokiego poziomu bezpieczeństwa sieci i systemów informatycznych w Unii, drugie – poszczególne kraje różnią się pod względem poziomu gotowości na zagrożenia związane z cyfryzacją, to zaś powoduje niejednolite podejście w ramach całej UE. Dlatego też dyrektywa NIS ustanawia środki, które mają doprowadzić do osiągnięcia wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych w unii. Dyrektywa NIS nie nakłada samodzielnie sankcji za niewywiązywanie się z jej postanowień. Zobowiązuje natomiast państwa członkowskie do przyjęcia regulacji dotyczących sankcji, które mają zastosowanie w przypadku naruszeń krajowych przepisów (przyjętych na podstawie dyrektywy) i podjęcia wszystkich niezbędnych środków w celu zapewnienia ich wykonania. Na powiadomienie komisji o przyjętych regulacjach prawnych i podjętych środkach Polska, czas do 9 maja 2018 r.

WAŻNE **Zakładane przez Komisję Europejską przyspieszenie transformacji cyfrowej w administracji oznacza potrzebę zapewnienia wyższego poziomu ochrony danych osobowych, prywatności i bezpieczeństwa informatycznego, niż wynikałoby to ze zwykłej zgodności z ramami prawnymi w tych dziedzinach.**

ZADANIA DYREKTYWY NIS

Dyrektywa w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii:

- ✓ zobowiązuje wszystkie państwa członkowskie do przyjęcia krajowej strategii w zakresie bezpieczeństwa sieci i systemów informatycznych;
- ✓ tworzy grupę współpracy, po to, by wspierać i ułatwiać m.in. wymianę informacji między państwami członkowskimi oraz rozwijać wśród nich zaufanie i pewność;
- ✓ tworzy sieć zespołów reagowania na incydenty bezpieczeństwa komputerowego (sieć CSIRT – z ang. Computer Security Incident Response Team);
- ✓ ustanawia wymogi dotyczące bezpieczeństwa i zgłaszania incydentów dla operatorów usług kluczowych i dostawców usług cyfrowych;
- ✓ ustanawia obowiązki dla państw członkowskich dotyczące wyznaczania właściwych organów krajowych, pojedynczych punktów kontaktowych oraz CSIRT, mających zadania związane z bezpieczeństwem sieci i systemów informatycznych. ©℗

P1SZ

2018
9
maja

Do tego dnia Polska ma powiadomić Komisję Europejską o regulacjach dotyczących sankcji, które będą stosowane w przypadku naruszeń krajowych przepisów przyjętych na podstawie dyrektywy NIS

Także RODO wyraźnie akcentuje kwestie bezpieczeństwa przetwarzania danych osobowych. Administrator danych (i ewentualnie podmiot przetwarzający, np. dostawca rozwiązań IT) musi wdrożyć odpowiednie środki techniczne i organizacyjne, aby zapewnić odpowiedni stopień bezpieczeństwa. Muszą przy tym uwzględnić stan wiedzy technicznej, koszt wdrażania, a także charakter, zakres, kontekst, cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia. Oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności ryzyko wiążące się z przetwarzaniem. W szczególności będące efektem przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych, przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

WAŻNE **W rozumieniu RODO dane dotyczące zdrowia oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia.**

Ze względów bezpieczeństwa podmiot wykonujący działalność leczniczą powinien zachowywać zdolność do ciągłego zapewnienia poufności, integralności, dostępności oraz odporności systemów i usług przetwarzania, a także zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego. Powinien również zapewnić regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych, których celem jest zapewnienie bezpieczeństwa przetwarzania. Ponadto konieczna może okazać się pseudonimizacja i szyfrowanie danych osobowych. Ogólne rozporządzenie o ochronie danych osobowych wymaga ponadto, by zarówno administrator, jak i podmiot przetwarzający wyznaczyli inspektora ochrony danych zawsze wtedy, gdy ich główna działalność polega na przetwarzaniu na dużą skalę danych medycznych. Podstawowym zadaniem inspektora ochrony danych jest zapewnienie zgodnego z prawem, a co za tym idzie – bezpiecznego przetwarzania danych pacjentów.

Jeden cel: bezpieczeństwo

Działania w zakresie cyberbezpieczeństwa w służbie zdrowia przyspieszyły po londyńskim ataku hakerów. Wiele krajów uświadomiło sobie, że korzystanie z nowoczesnych technologii w medycynie wymaga wielomilionowych nakładów

Na początku sierpnia 2017 r. amerykański senator Richard Blumenthal zaproponował przyjęcie zmian prawnych – Medical Device Cybersecurity Act – mających na celu większą ochronę danych o stanie zdrowia pacjentów. Nie jest to odosobniona inicjatywa. Po przykrych doświadczeniach ostatnich ataków hakerskich także władze Wielkiej Brytanii zamierzają zainwestować ok. 50 mln funtów na zwiększenie cyberbezpieczeństwa w ochronie zdrowia. Stało się bowiem jasne, że odpowiedzialne korzystanie z możliwości oferowanych przez technologie wiąże się w służbie zdrowia z koniecznością zapewnienia najwyższego możliwego poziomu ochrony danych.

Polska też świadoma

W podobnym kierunku zmierzają polskie władze. Ministerstwo Cyfryzacji i Najwyższa Izba Kontroli są w pełni zgodne co do tego, że konieczne jest rozszerzenie działań w zakresie ochrony systemów przetwarzających dane istotne dla funkcjonowania państwa. Przygotowywana obecnie przez resort ustawa o krajowym systemie cyberbezpieczeństwa powinna wejść w życie, zgodnie z deklaracjami urzędników, wiosną 2018 r. (z ostatnich deklaracji strony rządowej wynika, że projekt zostanie przekazany do konsultacji publicznych w ciągu najbliższych tygodni). Przy czym już 9 maja 2017 r. strona rządowa – realizując obowiązek wynikający z dyrektywy NIS – przyjęła krajową strategię w zakresie bezpieczeństwa systemów teleinformatycznych, czyli „Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022". Dokument został opracowany przez grupę ekspertów – przedstawicieli resortów cyfryzacji, obrony narodowej, spraw wewnętrznych i administracji oraz osoby reprezentujące Agencję Bezpieczeństwa Wewnętrznego, Rządowe Centrum Bezpieczeństwa i Biuro Bezpieczeństwa Narodowego.

I tak jednym z planowanych w ramach strategii działań jest też dostosowanie otoczenia prawnego do potrzeb i wyzwań w obszarze cyberbezpieczeństwa. W tym celu zostanie przeprowadzony przegląd istniejących regulacji prawnych, który ma nie tylko pozwolić na zharmonizowanie przepisów, ale też zwiększyć efektywność podejmowanych działań i poprawić przepływ informacji pomiędzy wszystkimi podmiotami zaangażowanymi w aktywne budowanie krajowego systemu cyberbezpieczeństwa.

Problemy z przepisami

Obecne normy dotyczące cyberbezpieczeństwa są rozproszone po różnych aktach prawnych. Do tego dochodzą wytyczne, zalecenia i wskazania.

USTAWOWE MINIMUM OCHRONY

Ustawa z 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz.U. z 2017 r. poz. 570) określa m.in. zasady ustalania minimalnych wymagań dla systemów teleinformatycznych, używanych do realizacji zadań publicznych, oraz dla rejestrów publicznych i wymiany informacji w postaci elektronicznej z podmiotami publicznymi. Przepisy muszą stosować m.in. samodzielne publiczne zakłady opieki zdrowotnej oraz spółki wykonujące działalność leczniczą w rozumieniu przepisów o działalności leczniczej. Wydane na podstawie upoważnienia z ww. ustawy rozporządzenie Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (t.j. Dz.U. z 2016 r. poz. 113) zawiera szczegółowe normy techniczne i organizacyjne zapewniające minimalny poziom bezpieczeństwa. Zgodnie z nim zarządzanie bezpieczeństwem informacji powinno być realizowane w szczególności przez zapewnienie przez kierownictwo podmiotu leczniczego warunków umożliwiających realizację i egzekwowanie wielu wskazanych w rozporządzeniu działań, w tym m.in. utrzymywanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji, przeprowadzanie okresowych analiz ryzyka, zapewnienie szkoleń osób zaangażowanych w proces przetwarzania informacji, zapewnienie ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami czy też zawieraniem w umowach serwisowych, podpisanych ze stronami trzecimi, zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji.

Wymagania te uznaje się za spełnione, jeżeli system zarządzania bezpieczeństwem informacji został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001, a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie polskich norm związanych z tą normą, w tym

SAMORZĄD I ADMINISTRACJA

PN-ISO/IEC 27002 (w odniesieniu do ustanawiania zabezpieczeń), PN-ISO/IEC 27005 (w odniesieniu do zarządzania ryzykiem), PN-ISO/IEC 24762 (w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania).

Obowiązująca jeszcze ustawa z 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2016 r. poz. 922) w podobny sposób zobowiązuje administratora danych osobowych (którym jest co do zasady podmiot leczniczy) do stosowania środków technicznych i organizacyjnych, które zapewniają ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną. Administrator powinien więc zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. W tym celu powinna być prowadzona dokumentacja opisująca sposób przetwarzania danych, na którą składają się polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym.

Należy jednak pamiętać, że zupełnie nowa wersja ustawy o ochronie danych, która została udostępniona do konsultacji publicznych, nie zawiera norm dotyczących bezpieczeństwa przetwarzania danych, odsyłając w tym zakresie do RODO.

Podstawowe zasady dotyczące bezpieczeństwa dokumentacji medycznej wskazuje w sposób stosunkowo ogólny ustawa z 6 listopada 2008 r. o prawach pacjenta i rzeczniku praw pacjenta (t.j. Dz.U. z 2017 r. poz. 1318 ze zm.). Stanowi ona, że podmiot udzielający świadczeń zdrowotnych jest obowiązany zapewnić ochronę danych zawartych w dokumentacji. Konkretniejsze i dostosowane do cyfrowej formy danych wymogi sformułowane zostały w rozporządzeniu ministra zdrowia z 9 listopada 2015 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania (Dz.U. poz. 2069).

WYTYCZNE, ZALECENIA, WSKAZANIA

Niezależnie od wymogów prawnych, podstawowe standardy postępowania z danymi osobowymi pacjentów wyznaczają instrumenty miękkiego prawa – czyli oficjalne wskazówki publikowane przez stronę publiczną lub uznane organizacje branżowe – wskazujące jak należy postępować, by spełnić ustawowe obowiązki. Choć dokumenty takie nie mają mocy wiążącej i nikt nie może być pociągnięty do odpowiedzialności w związku z brakiem ich zastosowania, stanowią one cenny drogowskaz w gąszczu różnych nakazów i zakazów.

Rekomendacje CSIOZ

28 września 2017 r. 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".

Zgodnie z intencjami autorów rekomendacje są przeznaczone dla usługodawców podejmujących decyzję dotyczącą wyboru rozwiązania wykorzystywanego do elektronicznego przetwarzania dokumentacji medycznej, w tym 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. Materiał prezentuje wiele istotnych wskazówek w zakresie zapewnienia bezpieczeństwa danych medycznych. Rekomendacje podkreślają możliwość zastosowania dowolnych rozwiązań IT, w tym technologii chmurowych w ramach organizacji. Jednocześnie autorzy rekomendacji uczulają na zasadność zwrócenia uwagi na spełnienie przez dostawców usług IT norm ISO oraz innych relewantnych standardów. Jest to istotny element, który należy brać pod uwagę przy podejmowaniu decyzji co do wyboru kontrahentów. Rekomendacje odnoszą się również bezpośrednio do zagadnienia cyberbezpieczeństwa.

Kodeks postępowania dla ochrony zdrowia

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. Mają one pomóc we właściwym stosowaniu RODO – z uwzględnieniem specyfiki różnych sektorów dokonujących przetwarzania oraz szczególnych potrzeb mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw.

Z kolei branża medyczna w Polsce dostrzegła potrzebę przygotowania kodeksu branżowego. 26 lipca 2017 r. w siedzibie CSIOZ odbyło się spotkanie inaugurujące prace nad kodeksem branżowym dla sektora ochrony zdrowia. Działania na rzecz przygotowania kodeksu branżowego wspiera wiele instytucji, organizacji zawodowych i społecznych zajmujących się szeroko pojętą ochroną zdrowia.

Normy ISO

Standardy bezpieczeństwa danych wyznaczają także normy. 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 e-zdrowia.

Norma ISO/IEC 27002 wyznacza zasady ustanowienia, wdrażania, eksploatacji, monitorowania, przeglądu, utrzymania i doskonalenia Systemu Zarządzania Bezpieczeństwem Informacji. 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. ©℗

Tekst powstał przy wsparciu merytorycznym **Piotra Marczuka,** dyrektora ds. polityki korporacyjnej w Microsofcie

WAŻNE **Nowa wersja ustawy o ochronie danych, która została udostępniona do konsultacji publicznych, nie zawiera norm dotyczących bezpieczeństwa przetwarzania danych, odsyłając w tym zakresie do RODO.**

Co nakazuje minister zdrowia ©℗

Jeśli chodzi o cyberbezpieczeństwo, należy zwrócić uwagę, że dokumentacja może być prowadzona w postaci elektronicznej, pod warunkiem prowadzenia jej w systemie teleinformatycznym zapewniającym:

- zabezpieczenie dokumentacji przed uszkodzeniem lub utratą;
- integralność treści dokumentacji i metadanych, polegającą na zabezpieczeniu przed wprowadzaniem zmian, z wyjątkiem zmian wprowadzanych w ramach ustalonych i udokumentowanych procedur;
- stały dostęp do dokumentacji dla osób uprawnionych oraz zabezpieczenie przed dostępem osób nieuprawnionych;
- identyfikację osoby dokonującej wpisu oraz osoby udzielającej świadczeń zdrowotnych i dokumentowanie dokonywanych przez te osoby zmian w dokumentacji i metadanych;

Dokumentację prowadzoną w postaci elektronicznej uważa się za zabezpieczoną, jeżeli w sposób ciągły są spełnione łącznie następujące warunki:

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

Ramy Bezpieczeństwa Cybernetycznego NIST

Przykładem dobrych praktyk, które mogłyby zostać zaadaptowane także w Polsce, są Ramy Bezpieczeństwa Cybernetycznego opracowane przez amerykański Krajowy Instytut Standaryzacji i Technologii – wskazuje raport DZP i Microsoftu

Ramy przygotowane przez amerykańskich ekspertów (National Institute of Standards and Technology – NIST) określają minima bezpieczeństwa, których skuteczność została potwierdzona i które zostały powszechnie przyjęte w USA. Co ważne, Stany Zjednoczone nie są jedynym krajem wykorzystującym ramy. Ramy Bezpieczeństwa Cybernetycznego oparte na NIST w 2015 roku przyjął rząd Włoch. Zostały one dostosowane do specyfiki sektora małych i średniej wielkości przedsiębiorstw. Do korzystania przez przedsiębiorców z NIST zachęcała także – w 2015 r. – Australia. Przyjmowanie ram cyberbezpieczeństwa na świecie najprawdopodobniej będzie postępowało. Także wydany niedawno w USA dekret prezydencki na temat bezpieczeństwa cybernetycznego nakłada obowiązek stosowania ram przez wszystkie agendy rządu Stanów Zjednoczonych. Ponadto Międzynarodowa Organizacja Normalizacyjna (ISO) zatwierdziła podjęcie prac nad raportem technicznym „Bezpieczeństwo cybernetyczne normy ISO i IEC", mającym na celu dostosowanie Ram Bezpieczeństwa Cybernetycznego NIST do środowiska międzynarodowego. ©℗

Na czym polegają ©℗

Oparto je 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:

1. **SZKIELET RAM:** jest to zbiór działań i stosownych informacyjnych źródeł odniesienia (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 określania swoich najbardziej krytycznych zasobów, wdrażania procedur ich ochrony, uwzględniania zasobów niezbędnych do rozpoznawania potencjalnych naruszeń bezpieczeństwa, utrzymywania procedur reagowania na naruszenia oraz tworzenia procedury umożliwiającej im odbudowanie się po ataku.
2. **PROFIL RAM:** 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.
3. **WARSTWY WDRAŻANIA RAM:** opisują stopień zaawansowania stosowania w organizacji praktyk z obszaru bezpieczeństwa cybernetycznego. Rozróżnia się cztery poziomy klasyfikujące podejście organizacji do zarządzania ryzykiem ataków cybernetycznych, od poziomu „nieformalnego" do „adaptacyjnego":
   - ✓ **Warstwa 1** (nieformalnie): podchodzi do bezpieczeństwa cybernetycznego na zasadach doraźnych. Ma minimalną świadomość zagrożeń cybernetycznych dla organizacji.
   - ✓ **Warstwa 2** (ze świadomością ryzyka): 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): działa zgodnie z formalnymi procedurami dotyczącymi bezpieczeństwa cybernetycznego, które regularnie aktualizuje, dysponuje dobrze przeszkolonym personelem i rozumie współzależności oraz otoczenie swoich partnerów.
   - ✓ **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.

PiSZ

Pisaliśmy o tym...

„Branża medyczna już pisze własny kodeks ochrony danych osobowych" – Tygodnik Gazeta Prawna z 8 sierpnia 2017 r. (DGP nr 159)