Minister Zdrowia

Warszawa, 14 -07- 2017

DNW.051.209.2017.2.MK

Pan
Adam Bodnar
Rzecznik Praw Obywatelskich

Szanowny Panie Rzeczniku

W odpowiedzi na Pana pismo z dnia 19 czerwca 2017 r. o znaku VV.520.36.2017.AG, zawierające prośbę o udzielenie informacji na temat działań podjętych przez Ministra Zdrowia w celu wyjaśnienia sprawy dotyczącej wycieku danych osobowych z bazy zawierającej informacje o pacjentach Samodzielnego Publicznego Zakładu Opieki Zdrowotnej w Kole (zwanego dalej: SPZOZ w Kole), poniżej wskazuję co następuje.

Z informacji dostępnych w mediach wynika, że w przedmiotowej sprawie doszło do incydentu naruszenia bezpieczeństwa związanego z upublicznieniem danych osobowych, w tym danych osobowych wrażliwych. Analiza informacji prasowych wskazała, że brak jest możliwości jednoznacznego stwierdzenia, jaki był to zakres danych, jaki charakter dane te posiadały i jaki był ich wolumen. Dodatkowo na podstawie dostępnych informacji brak jest możliwości stwierdzenia, jak długo dane te były publicznie dostępne jak również co było bezpośrednią przyczyną ich ujawnienia. Niewykluczone, że tak jak podaje portal rynekzdrowia.pl, udostępnienie tych danych może być związane z działalnością hakerów.

Polska Agencja Prasowa na swojej stronie internetowej poinformowała, że Dyrekcja SPZOZ w Kole potwierdziła fakt, że mogło dojść do wycieku danych, a o sprawie powiadomiono policję i prokuraturę, która prowadzi stosowne czynności.

Ministerstwo Zdrowia
ul. Miodowa 15
00-952 Warszawa

Telefon: (22) 634 96 00
e-mail: kancelaria@mz.gov.pl
www.mz.gov.pl

Uprzejmie informuję, że zgodnie z art. 24 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta[1] (dalej jako: „ustawa o prawach pacjenta i Rzeczniku Praw Pacjenta"), podmiot udzielający świadczeń zdrowotnych jest obowiązany zapewnić ochronę danych zawartych w dokumentacji medycznej.

Należy również zaznaczyć, że szczegółowa informacja dotycząca przetwarzania danych osobowych zawartych w dokumentacji medycznej znajduje się w art. 23 – 30a ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta. Reguluje ona zagadnienia prowadzenia dokumentacji medycznej, jej przechowywania, udostępniania oraz niszczenia. Warto zwrócić uwagę, że zgodnie z art. 24 ust. 2 tej ustawy do przetwarzania danych zawartych w dokumentacji medycznej, w celu ochrony zdrowia, udzielania oraz zarządzania udzielaniem świadczeń zdrowotnych, utrzymania systemu teleinformatycznego, w którym przetwarzana jest dokumentacja medyczna, i zapewnienia bezpieczeństwa tego systemu, są uprawnione:

1) osoby wykonujące zawód medyczny,
2) inne osoby wykonujące czynności pomocnicze przy udzielaniu świadczeń zdrowotnych, a także czynności związane z utrzymaniem systemu teleinformatycznego, w którym przetwarzana jest dokumentacja medyczna, i zapewnieniem bezpieczeństwa tego systemu, na podstawie upoważnienia administratora danych.

Bezpieczeństwo systemów informatycznych należy rozpatrywać pod kątem atrybutów przypisanych informacjom w nich przetwarzanym. Możemy tutaj mówić o poufności, integralności i dostępności, dodatkowo uzupełniając je o rozliczalność, a także niezaprzeczalność informacji. Na podstawie przeprowadzanych analiz ryzyka przetwarzania informacji, które bezpośrednio wykonuje się na wypadek utraty powyżej wspomnianych atrybutów, podmiot powinien wprowadzić zabezpieczenia w warstwach systemowej, organizacyjnej i technicznej.

Bardzo często wprowadzone są zabezpieczenia nieadekwatne do przetwarzanych informacji lub też pomija się atrybuty przypisane informacjom np. ich dostępność i tak mogło być w badanym przypadku. Jednak bez analizy sytuacji w tym podmiocie tj. zbadanie jakie kroki w warstwach bezpieczeństwa były podejmowane, nie można wywieść, czy Administrator Danych Osobowych czyli osoby zarządzające podmiotem dokonał wszystkich wymaganych czynności i zabezpieczył odpowiednio dane.

[1] Dz. U. z 2016 r. poz.186 z późn. zm.;

Warto jednak zaznaczyć, że zgodnie z wykonaną w 2016 roku przez Centrum Systemów Informacyjnych Ochrony Zdrowia (zwanym dalej: CSIOZ) II edycją „Badania stopnia przygotowania podmiotów wykonujących działalność leczniczą do obowiązków wynikających z Ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia[2]" 82% szpitali oraz 63% stacjonarnych i całodobowych świadczeniach zdrowotnych innych niż szpitalne deklarowało posiadanie opracowanej oraz wdrożonej wewnętrznej polityki bezpieczeństwa. W przypadku podmiotów realizujących świadczenia w ramach ambulatoryjnej opieki zdrowotnej – 56% posiada wdrożoną politykę bezpieczeństwa w swoich placówkach. W porównaniu do danych otrzymanych w toku I edycji badania z 2014 r. znacznie poprawiły się wyniki w tym zakresie, biorąc pod uwagę stacjonarne i całodobowe świadczenia zdrowotne inne niż szpitalne. Jednocześnie, zgodnie z wynikami ankiety, w roku poprzedzającym badanie praktycznie nie wystąpiły istotne awarie systemów informatycznych, w skutek których nastąpiłaby utrata jednostkowych danych medycznych, o których mowa w ustawie o systemie informacji w ochronie zdrowia. Do utraty danych doszło jedynie w niecałym 1% ankietowanych podmiotów, realizujących świadczenia w ramach ambulatoryjnej opieki zdrowotnej, niecałym 0,5% stacjonarnych i całodobowych świadczeniach zdrowotnych innych niż szpitalne oraz 3% szpitali. Przyczyną ww. utraty były: uszkodzenia dysku twardego, uszkodzenia bazy danych, bądź też awaria sprzętowa serwera, na którym działała baza danych. Jednak jak wynika z doświadczenia zapisy zawarte w Wewnętrznych Politykach Bezpieczeństwa Informacji często są nieaktualne, a w niektórych przypadkach Polityka Bezpieczeństwa Informacji w ogóle nie została wdrożona i nie jest stosowana.

Na tej podstawie można stwierdzić, że stan zabezpieczeń systemów informatycznych w polskich placówkach ochrony zdrowia jest zróżnicowany i zależy od czynników takich jak :

- świadomości, zarówno kadry zarządzającej, jak i osób zajmujących się bezpieczeństwem i administrowaniem systemami i infrastrukturą IT w tych placówkach,
- brakami kadrowymi oraz wysoką fluktuacją informatyków,
- możliwościami finansowymi tych podmiotów,

[2] Dz. U. z 2016 r., poz. 1535, z późn. zm.;

- brakiem dostępnych wytycznych i rekomendacji w zakresie stosowania rozwiązań w zakresie zabezpieczeń systemów informatycznych.

CSIOZ podejmowało szereg działań edukacyjnych skierowanych, zarówno do informatyków ze szpitali, jak i kadry zarządzającej podmiotami leczniczymi w celu podniesienia poziomu wiedzy w zakresie strategicznego charakteru zagadnienia jakim jest odpowiednie zabezpieczenie systemów informatycznych w placówkach ochrony zdrowia. Należy zauważyć, że na organizowane przez CSIOZ szkolenia dla kadry zarządzającej (obejmujące m.in. kwestie bezpieczeństwa) de facto przychodzą osoby zajmujące się bezpieczeństwem w tych podmiotach lub informatycy, a nie kadra zarządzająca podmiotami leczniczymi.

W przypadku incydentu w SPZOZ w Kole można przypuszczać, że to zbieg kilku zdarzeń i czynników spowodował wyciek danych pacjentów. Jednak jak wskazano wyżej, należy zwrócić uwagę na czynniki, które mogą mieć wpływ na przedmiotową sytuację. I tak brak świadomości, zarówno kadry zarządzającej, jak i pracowników odpowiedzialnych za bezpieczeństwo, brak środków finansowych, brak szkoleń i zwiększania kompetencji zespołów odpowiedzialnych za bezpieczeństwo powoduje, że dane mogą nie być zabezpieczone w sposób wystarczający.

Ilość ataków ransomware i typu phishing jakie można obserwować w sieci jest znacząca i można zaobserwować ich systematyczny wzrost, a ostatnie ataki Wonna Cry i Petya pokazują, że staje się to poważnym globalnym problemem wymagającym koordynacji centralnej w danym obszarze.

Bezpieczeństwo danych medycznych jest kluczowym zagadnieniem w kontekście prowadzenia dokumentacji medycznej przez podmioty udzielające świadczeń zdrowotnych. Dlatego też każdy podmiot leczniczy powinien posiadać Wewnętrzną Politykę Bezpieczeństwa, a ponadto systematycznie aktualizować jej założenia i kontrolować przestrzeganie przez pracowników określonych w niej zasad.

Przede wszystkim wymaga podkreślenia, że administratorem danych osobowych przetwarzanych w dokumentacji medycznej jest podmiot wykonujący działalność leczniczą. Normy prawne nakładają na administratora szereg obowiązków, w szczególności powinien on zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem (art. 36 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, dalej

jako: „ustawa o ochronie danych osobowych" [3]). Ponadto zgodnie z art. 37 ustawy o ochronie danych osobowych, do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych. Obowiązkiem administratora danych jest także zapewnienie kontroli nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane.

Dostrzegając problem zarządzania w podmiotach leczniczych danymi o stanie zdrowia pacjentów oraz możliwości wykorzystywania przez nie systemów teleinformatycznych do przetwarzania danych osobowych, Minister Zdrowia w nowelizacji ustawy z dnia 9 października 2015 r. o zmianie ustawy o systemie informacji w ochronie zdrowia oraz niektórych innych ustaw[4] kompleksowo uregulował zagadnienia zawierania przez podmioty udzielające świadczeń zdrowotnych umów o powierzenie przetwarzania danych osobowych z podmiotami wyspecjalizowanymi w utrzymaniu systemu teleinformatycznego (tzw. outsourcing danych medycznych).

Możliwość zawierania przez podmioty udzielające świadczeń zdrowotnych umów o powierzeniu przetwarzania danych osobowych jest zawsze uwarunkowana koniecznością zapewnienia bezpieczeństwa danych powierzonych do przetwarzania. W przypadku zaprzestania przetwarzania danych osobowych zawartych w dokumentacji medycznej przez podmiot, któremu powierzono przetwarzanie, w szczególności w związku z jego likwidacją, jest on zobowiązany do przekazania danych osobowych podmiotowi wykonującemu działalność leczniczą, który powierzył mu takie dane[5].

W planowanej kolejnej nowelizacji ustawy o systemie informacji w ochronie zdrowia przewiduje się przyznanie CSIOZ kompetencji do określania w formie wytycznych wymagań dla systemów lokalnych usługodawców.

Jednocześnie, mając na uwadze ewentualne następstwa naruszania bezpieczeństwa ochrony danych osobowych, w tym danych wrażliwych, Minister Zdrowia skierował do kierowników wszystkich podmiotów leczniczych w Polsce pismo, zalecające szczególne zainteresowanie się problematyką ochrony danych osobowych, w tym medycznych, pozyskiwanych podczas procesu leczenia, a także zastosowanie odpowiednich środków technicznych i organizacyjnych w celu ich zabezpieczenia przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną,

---

[3] Dz. U. z 2016 r., poz. 922;
[4] Dz. U. z 2015 r., poz. 1991, z późn. zm.;
[5] Por. art. 24 ust. 2- 7 ustawy o prawach pacjentach i Rzeczniku Praw Pacjenta;

przetwarzaniem z naruszeniem przepisów prawa oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

Ponadto zważywszy na fakt, iż podmiotem tworzącym dla Samodzielnego Publicznego Zakładu Opieki Zdrowotnej w Kole jest Powiat Kolski, Minister Zdrowia wystąpił do Pana Wieńczysława Oblizajka Starosty Kolskiego o podjęcie stosownych działań weryfikacyjnych i nadzorczych, celem ustalenia przyczyn wycieku danych osobowych oraz dokonania oceny prawidłowości zastosowanych w tym podmiocie leczniczym środków technicznych i organizacyjnych zapewniających ochronę danych osobowych przed ich udostępnieniem osobom nieuprawnionym[6]. Zgodnie bowiem z art. 121 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej[7], nadzór nad podmiotem leczniczym niebędącym przedsiębiorcą sprawuje podmiot tworzący.

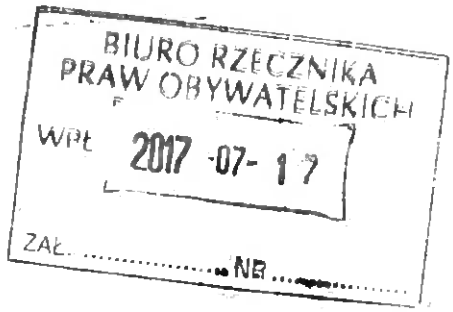
Ponadto z uwagi na przedmiot sprawy, Minister Zdrowia wystąpił do Pani Edyty Bielak – Jomaa Generalnego Inspektora Ochrony Danych Osobowych z prośbą o podjęcie stosownych działań w ramach posiadanej właściwości, w tym o przeprowadzenie kontroli, w szczególności w zakresie zastosowanych w Samodzielnym Publicznym Zakładzie Opieki Zdrowotnej w Kole środków technicznych i organizacyjnych zapewniających ochronę danych osobowych przed ich udostępnieniem osobom nieuprawnionym[8].

z poważaniem

Z upoważnienia
MINISTRA ZDROWIA
SEKRETARZ STANU
Józefa Szczurek-Żelazko

[6] Pismo z dnia 28 czerwca 2017 r. o znaku DNW.051.209.2017.1.MG;
[7] Dz. U. z 2016 r., poz. 1638, z późn. zm.;
[8] Pismo z dnia 28 czerwca 2017 r. o znaku DNW.051.209.2017.1.MG.

MINISTERSTWO ZDROWIA
Departament Nadzoru, Kontroli i Skarg
00-952 Warszawa
ul. Miodowa 15



DNW.051.209.2017

431282 2017-07-14 05

Adam Bodnar
Rzecznik Praw Obywatelskich - Biuro
Al. Solidarności 77
00-090 Warszawa

412002