

Należyte zabezpieczanie danych osobowych pacjentów

wywiad z ministrem Michałem Serzyckim - Generalnym Inspektorem Ochrony Danych Osobowych

Jak wygląda dzisiaj ochrona danych, ochrona informacji w polskich szpitalach? Na jakim jest poziomie?

Ze skarg, które do nas wpłynęły i z kontroli, jakie przeprowadziliśmy w zakładach opieki medycznej, wynika, że stosowany tam sposób zabezpieczenia danych medycznych nie jest zadowalający. Wydaje się, że przedstawiciele sektora medycznego nie mają wystarczającej świadomości tego, że administrator danych osobowych w każdym zakładzie ma obowiązek należytego zabezpieczenia gromadzonych tam danych osobowych. A dane medyczne są danymi szczególnie chronionymi, ponieważ należą to kategorii danych tzw. wrażliwych. Dlatego ich udostępnianie jest obwarowane nie tylko przepisami ustawy o ochronie danych osobowych, ale także przepisami branżowymi, na mocy których wprowadzono m.in. tajemnicę lekarską.

Czy ze względu na to, że są to dane wrażliwe i mają ogromną wartość, jest dużo przypadków ich kradzieży?

Nasze dane osobowe, nie tylko te dotyczące stanu zdrowia, ale w ogóle wszystkie dotyczące nas informacje, mają – z czego nie wszyscy zdajemy sobie sprawę – dużą wartość rynkową. Z tego powodu są narażone m.in. na kradzież. Dlatego powinny być należycie zabezpieczone. Zwłaszcza dane tzw. wrażliwe – czyli te dotyczące informacji m.in. o stanie naszego zdrowia, wśród których mogą znajdować się niekiedy nawet informacje intymne.

Czy to, że w medycynie coraz powszechniej są wykorzystywane nowoczesne technologie, np. zaczyna

być stosowana telemedycyna, przed osobami zajmującymi się bezpieczeństwem danych stawia nowe wyzwania?

Tak. Trzeba mieć świadomość tego, że nowe technologie są z jednej strony dobrodziejstwem, ale z drugiej rodzą nowe zagrożenia dla bezpieczeństwa danych osobowych. Natomiast ustawa o ochronie danych osobowych oraz wydane na jej podstawie rozporządzenie ministra spraw wewnętrznych i administracji w sposób dość ogólny określają zasady zabezpieczania danych osobowych. Na administratorów danych nakładają bowiem obowiązek zastosowania należytego ich zabezpieczenia. Oznacza to m.in. konieczność takiego dobrania zabezpieczeń, aby były odpowiednie do istniejących zagrożeń.

Rozporządzenie ministra spraw wewnętrznych i administracji w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych wprowadza trzy stopnie zabezpieczenia zależne od kategorii przetwarzanych danych i istniejących zagrożeń. Są to:

- podstawowy – który powinien być stosowany w firmach nieprzetwarzających danych szczególnie chronionych i niemających żadnych urządzeń systemu informatycznego służącego do przetwarzania danych osobowych połączonego z publiczną siecią internetową,
- podwyższony – który powinien być stosowany tam, gdzie przetwarzane są dane szczególnie chronione (np. o stanie zdrowia, kodzie genetycznym czy życiu seksualnym), ale żadne z urządzeń systemu informatycznego służącego do przetwarzania danych osobowych nie jest połączone z publiczną siecią internetową,
- wysoki – który powinien być stosowany wówczas, gdy przynajmniej jedno urządzenie systemu informatycznego służącego do przetwarzania danych osobowych jest połączone z publiczną siecią internetową.

Co ważne, obowiązek należytej ochrony danych osobowych zawsze spoczywa na administratorach danych osobowych. Przy czym mogą oni wykonywać go osobiście, stając się wówczas administratorami bezpieczeństwa informacji (ABI), albo robić to za pośrednictwem wyznaczonych przez siebie osób – wówczas to one będą pełniły funkcję ABI. Takie rozwiązanie organizacyjne nie zdejmuje jednak odpowiedzialności, jaka za bezpieczeństwo danych osobowych spoczywa na ich administratorach.

Osoby te, znając charakter przetwarzanych danych oraz istniejące zagrożenia, muszą dobrać takie formy zabezpieczenia, aby uchronić dane m.in. przed udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, niezgodnym z prawem przetwarzaniem, zmianą, utratą, uszkodzeniem lub zniszczeniem.

Czy wprowadzenie rozwiązań typu automatyczna identyfikacja, kody kreskowe, wpłynęłoby jakoś na odpowiedzialność administratorów?

Jeżeli będziemy myśleli o odpowiedzialności karnej wynikającej z nienależytego zabezpieczenia, to nie. Za to grożą konkretne kary, które są wymienione w ustawie o ochronie danych osobowych. Jeżeli natomiast słowo „odpowiedzialność”

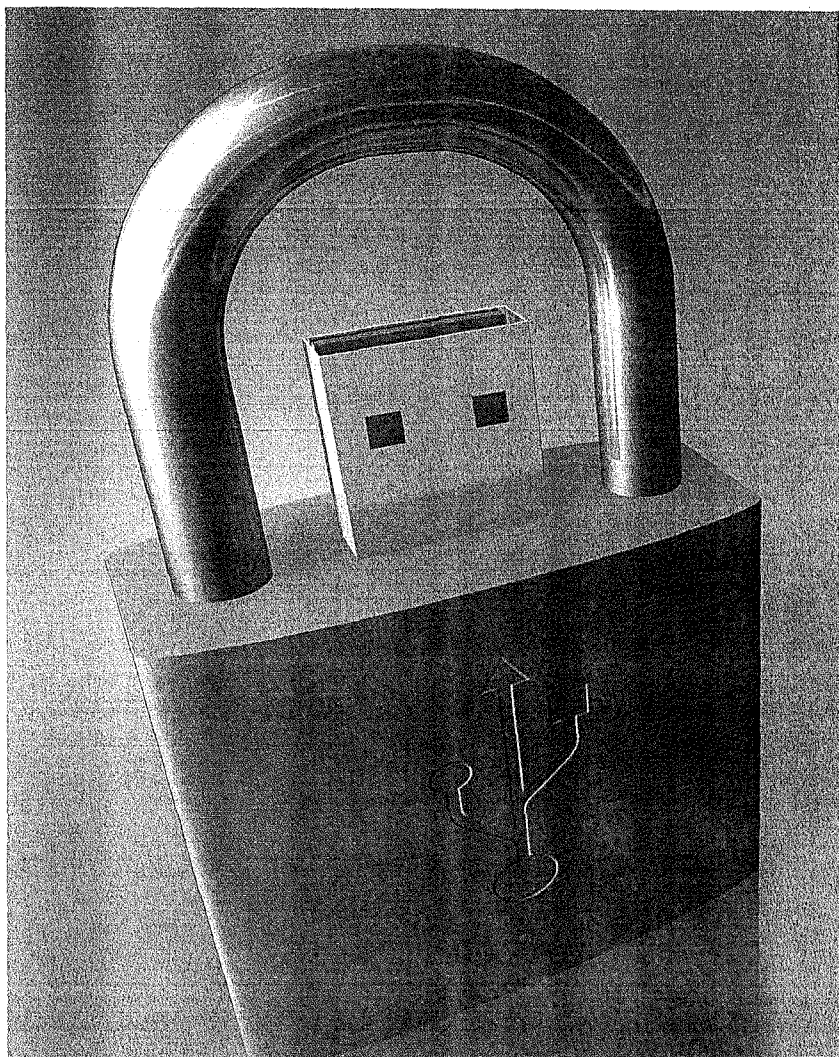
będziemy rozumieli jako dołożenie jeszcze większej staranności przy zabezpieczaniu danych osobowych, to tak.

Według Pana lepsza jest tradycyjna dokumentacja papierowa czy nowoczesna elektroniczna? Jeżeli chodzi o bezpieczeństwo oczywiście.

Jeśli sprawę tę będziemy rozpatrywać pod kątem dobrej usługi dla pacjenta, to nowe technologie dają ogromne możliwości jej usprawnienia – szybszej analizy, wymiany informacji. Zresztą dla lekarzy to również duże ułatwienie, z czego zapewne lepiej ode mnie zdają sobie sprawę. Jeśli zaś chodzi o kwestię zabezpieczenia danych osobowych, to na pewno łatwiej to zrobić, gdy dokumentacja ma formę papierową. W przypadku przetwarzania danych osobowych w zintegrowanych systemach informatycznych z pewnością rośnie liczba zagrożeń, np. zwiększa się niebezpieczeństwo wycieku. Choć zdaję sobie sprawę, że z punktu widzenia szybkości i jakości obsługi pacjenta, to duże ułatwienie.

A gdyby wprowadzić jednolity system gromadzenia danych we wszystkich placówkach? Chodzi o wyznaczniki, wymagane do spełnienia dla systemu gromadzenia danych osobowych w danej placówce.

Taka standaryzacja pośrednio na pewno wpłynęłaby na bezpieczeństwo danych osobowych. Dzięki temu placówkom opieki zdrowotnej łatwiej byłoby wdrażać np. zasadę adekwatności, która mówi, że nie wolno zbierać większej liczby danych niż jest to



niezbędne ze względu na cel, w jakim się to robi. To jest jedna z najistotniejszych zasad zawartych w ustawie o ochronie danych osobowych. Jednak nie mnie się wypowiadać, ile informacji lekarz musi zdobyć, żeby skutecznie pomóc pacjentowi.

Porady on-line, zdalny dostęp lekarzy do wyników swojej pracy, dostęp firm ubezpieczeniowych do danych... Kto według Pana powinien mieć dostęp do danych tzw. wrażliwych?

W dobie rozwoju nowoczesnych technologii dostęp do baz danych staje się jednym z istotniejszych problemów, jeśli chodzi o ochronę danych osobowych. Coraz częściej bowiem tworzymy ogromne megabazy. Przy czym problemem nie jest gromadzenie danych osobowych, lecz ich właściwe zabezpieczenie i udostępnianie. W takich sytuacjach można mieć wątpliwości, czy kiedyś ktoś nie wpadnie na pomysł, żeby inaczej wykorzystać zebrane dane.

Wracając zaś do tego, czy firmy ubezpieczeniowe powinny mieć dostęp do naszych danych medycznych, to wydaje się, że dla dokładnego wyliczenia ryzyka ubezpieczeniowego wystarczyłby dostęp do danych statystycznych określonej populacji. Dlatego protestowałbym przeciwko zapewnieniu ubezpieczycielom nieograniczonego dostępu do danych jednostkowych – z zastrzeżeniem możliwości ich pozyskania na potrzeby konkretnego postępowania odszkodowawczego, co zresztą gwarantują obecne przepisy.

Trzeba bowiem pamiętać, że podmiot, który dysponuje danymi może je wykorzystywać tylko do tego celu, w jakim je zebrał. Nie powinien też bez naszej wiedzy i zgody udostępniać ich innym firmom i instytucjom, chyba że zezwala na to np. przepis prawa.

Jednak atrakcyjność wielu danych, a zwłaszcza tych, które zgromadzone są w obszernych bazach, powoduje, że przedstawiciele różnych środowisk próbują uzyskać do nich dostęp. Moim zadaniem – jako organu ochrony danych osobowych – jest zaś przeciwdziałanie takim niebezpiecznym praktykom i pomaganie obywatelom w zagwarantowaniu im ich podstawowego prawa – prawa do ochrony ich danych osobowych.

Czy pacjenci mają możliwość kontroli bezpieczeństwa swoich danych? Czy mogą jakoś zareagować na ich złe zabezpieczenie.

Ustawa o ochronie danych osobowych w art. 27 stanowi, że co do zasady zabronione jest przetwarzanie danych szczególnie chronionych, do których zaliczane są dane m.in. o stanie zdrowia, kodzie genetycznym, nałogach czy życiu seksualnym.

Jednak przetwarzanie tych danych jest dopuszczalne pod pewnymi warunkami, m.in. po wyrażeniu pisemnej zgody osoby, której dane dotyczą, albo w przypadku, gdy przepis szczególny innej ustawy zezwala na przetwarzanie takich danych bez zgody osoby, której dane dotyczą, i stwarza pełne gwarancje ich ochrony.

Nierozłącznym prawem każdej osoby, której dane są przetwarzane, jest uprawnienie do kontroli swoich danych zawartych w zbiorze. Katalog tych praw znajduje się w art. 32 ustawy o ochronie danych osobowych. Wśród nich są m.in. prawo do uzyskania wyczerpującej informacji, czy taki zbiór istnieje, oraz ustalenia administratora danych, jego adresu i pełnej nazwy, a także uzyskania informacji o źródle, z którego pochodzą dane dotyczące osoby.

Natomiast w sytuacji, gdy osoba, której dane dotyczą, stwierdzi, że jej dane przetwarzane są w sposób naruszający jej prawo do ochrony, może zwrócić się z pisemną skargą na takie postępowanie do administratora danych, a o ile to nie wystarczy - do Generalnego Inspektora Ochrony Danych Osobowych.

Czy rozwój nowoczesnych technologii wpłynie jakoś lub powinien wpłynąć na zmianę ustawodawstwa?

Przepisy nie nadążają za szybkim rozwojem nowoczesnych technologii, bo postęp odbywa się w zawrotnym tempie. Trzeba też pamiętać, że nie zawsze szybka zmiana prawa rozwiąże wszystkie problemy; często też zaraz pojawiają się nowe. Każdy przypadek trzeba analizować indywidualnie. Przykładem może być definicja danych osobowych z ustawy o ochronie danych osobowych.

Najczęstsze błędy zakładów opieki zdrowotnej dotyczące przetwarzania danych osobowych:

- brak środków zabezpieczających dane przed ich udostępnieniem osobom nieupoważnionym, zabranie przez osobę nieuprawnioną przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;
- brak zabezpieczeń papierowej dokumentacji medycznej (przechowywanie jej na biurkach, w szafkach czy odkrytych regałach);
- zabieranie przez pielęgniarki po zakończeniu dnia pracy kluczy do pomieszczeń, zamiast pobierania i zdawania ich na portierni;
- brak zainstalowania w systemach służących do przetwarzania danych osobowych oprogramowania antywirusowego;
- brak ochrony danych osobowych pacjentów zamieszczonych w systemie informatycznym przed zagrożeniami pochodzącymi z sieci publicznej (z Internetu);
- brak odnotowania, kiedy i przez kogo dane osobowe zostały wprowadzone do systemu informatycznego;
- brak identyfikatora osoby, która wprowadziła dane, oraz daty ich pierwszego wprowadzenia do systemu informatycznego.

Zgodnie z jej zapisami, danymi osobowymi są wszelkie informacje dotyczące konkretnej osoby, za pomocą których bez większego wysiłku można tę osobę zidentyfikować, chociaż nie jest ona wyraźnie wskazana. Większość z nas wie, że imię i nazwisko, adres zamieszkania, dane o cechach fizjologicznych to dane osobowe.

Jednak postęp technologiczny powoduje, że zakres informacji, które można zaliczyć do danych osobowych, coraz bardziej się rozszerza. Dziś należało by mówić chyba o „informacji osobowej”, a nie tylko o „danych osobowych”. Uważam bowiem, że do danych osobowych należy obecnie zaliczyć m.in.: numer IP komputera, loginy, nicki, a nawet pliki cookie. Trudno jednak wszystkie możliwe sytuacje przewidzieć i zawrzeć w ustawie.


Czy Unia Europejska narzuca nam jakieś wymagania dotyczące ochrony danych osobowych?

Jeżeli chodzi o ochronę danych osobowych to najważniejszym unijnym aktem prawnym jest Dyrektywa 95/46/WE Parlamentu Europejskiego. Każde państwo, które przystąpiło lub ma zamiar przystąpić do Unii Europejskiej, musi jej postanowienia wdrożyć do swojego porządku prawnego. A dyrektywa ta zawiera definicje podstawowych terminów, ustala zasady zbierania, gromadzenia, przechowywania i udostępniania danych osobowych.

Określa też zasady i warunki zgodności przetwarzania danych osobowych z prawem oraz prawa osób, których dane dotyczą. Jej niemalże lustrzanym odzwierciedleniem są zaś ustawy o ochronie danych osobowych w poszczególnych krajach

członkowskich. Dzięki temu poziom ochrony danych osobowych w całej Unii Europejskiej jest taki sam.

Badania Harvardu wykazują, że lekarze korzystający z elektronicznej dokumentacji medycznej są mniej narażeni na błędy lekarskie. Czy jeżeli dalsze badania potwierdzą te proporcje, jest szansa na wymóg stosowania dokumentacji elektronicznej?

Jeżeli dane rozwiązanie jest dobre, skuteczne, to samo się obrotu i zacznie być powszechnie stosowane. To mniej więcej tak, jak z teorią, że dobry pieniądz wypiera zły. Dobre rozwiązania wyprą rozwiązania gorsze. Natomiast muszę jeszcze raz podkreślić, że postęp technologiczny stawia przed administratorami nowe wyzwania co do odpowiedniego zabezpieczenia danych. 

Dziękuję za rozmowę
Małgorzata Dziurzyńska

Ważniejsze akty prawne regulujące ochronę danych osobowych w służbie zdrowia

Europejskie

- Dyrektywa 95/46/WE z 24 października 1995 r. o ochronie osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych
- Konwencja Nr 108 Rady Europy z 28 stycznia 1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych
- Rekomendacja R(97)5 dotycząca ochrony danych medycznych
- Dokument roboczy w sprawie przetwarzania danych osobowych dotyczących zdrowia w elektronicznej dokumentacji zdrowotnej (EHR) przyjęty 15 lutego 2007 r.

Krajowe

- Ustawa z 29 sierpnia 1997 r. o ochronie danych osobowych
- Ustawa z 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (zwłaszcza art. 188 i nast.)
- Ustawa z 30 sierpnia 1991 r. o zakładach opieki zdrowotnej (zwłaszcza art. 18, 32e i f)
- Rozporządzenie ministra zdrowia z 21 grudnia 2006 r. w sprawie rodzajów i zakresu dokumentacji medycznej w zakładach opieki zdrowotnej oraz sposobu jej przetwarzania
- Ustawa z 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty (przepisy rozdziału regulującego zasady wykonywania zawodu lekarza)
- Rozporządzenie ministra zdrowia z 30 lipca 2001 r. w sprawie rodzajów indywidualnej dokumentacji medycznej, sposobu jej prowadzenia oraz szczegółowych warunków jej udostępniania
- Ustawa z 5 lipca 1996 r. o zawodach pielęgniarstwa i położnej (przepisy rozdziału regulującego zasady wykonywania zawodów pielęgniarstwa i położnej)