dr Wojciech R. Wiewiórowski

Zlecenie przetwarzania danych nie zwalnia z odpowiedzialności

Outsourcing przetwarzania danych medycznych w Polsce nie jest odpowiednio uregulowany. Mimo to dziesiątki tysięcy lekarzy prowadzących gabinety prywatne będzie przekazywało te informacje do przechowywania w instytucjach wyspecjalizowanych na własną odpowiedzialność – mówi dr Wojciech Rafał Wiewiórowski, generalny inspektor ochrony danych osobowych (GIODO).

Generalny inspektor ochrony danych osobowych jest uprawniony do kontroli zgodności przetwarzania danych z przepisami o ochronie danych osobowych.

W związku z obowiązkiem tworzenia, od 1 sierpnia 2014 r., dokumentacji medycznej wyłącznie w formie elektronicznej, znajdujemy się w okresie podwójnego przetwarzania danych – jeszcze papierowych i już cyfrowych. Co powinny robić placówki medyczne, by ze zdwojoną uwagą dbać o ochronę tych danych?

Z pewnością znajdujemy się w okresie, gdy tzw. wrażliwe dane osobowe, dotyczące stanu zdrowia, są bardziej narażone na niewłaściwe przetwarzanie, aczkolwiek nie jest to zapewne ani pierwszy, ani ostatni moment w historii ochrony zdrowia, kiedy takie zmiany następują. Ochrona zdrowia nie jest też jedynym sektorem, w którym takie zdarzenie wystąpiło. Dla wielu placówek medycznych nie jest to zresztą nowość, bo wiele z nich od lat pracuje z komputerami i systemami teleinformatycznymi, które umożliwiają przekazywanie danych osobowych i dzielenie się nimi. One już zetknęły się z problemem gromadzenia i wykorzystywania danych medycznych w postaci elektronicznej i papierowej. Oprócz danych, które miały w swoich systemach elektronicznych, pozyskiwały bowiem dane zawarte w dokumentach papierowych przekazywanych przez pacjentów, np. wynikach badań z laboratoriów zewnętrznych. Jednak do tej pory dane te były wykorzystywane wyłącznie w obrębie tej samej placówki medycznej udzielającej świadczeń poprzez swoich specjalistów rozproszonych w różnych oddziałach. Powszechne zinformatyzowanie zasobów sektora opieki zdrowotnej spowoduje zaś, że dostęp do danych będzie możliwy online z dowolnego miejsca na świecie.

Podobna zmiana następuje też w administracji publicznej – w wielu urzędach wprowadzono już tzw. elektroniczny obieg dokumentów, ale część danych,

z których urząd wciąż korzysta, to historyczne dane papierowe, czasem sprzed wielu lat.

Jednak między systemami administracji publicznej a systemami ochrony zdrowia istnieje poważna różnica. O ile bowiem błąd w sztuce polegający na tym, że ktoś skorzysta z niewłaściwego dokumentu, popełni urzędnik, to zapewne w którejś instancji odwoławczej sprawę będzie można naprawić, o tyle błąd taki popełniony przez pracownika placówki ochrony zdrowia może spowodować śmierć pacjenta lub nieodwracalną utratę zdrowia.

Opinie specjalistów wskazują jednak, że w dużych systemach teleinformatycznych dane wrażliwe są lepiej chronione niż w przypadku ich zapisu na papierze.

Jest to jedna z tez, która faktycznie ma mocne podstawy. Z założenia, jeżeli tworzy się duży, rozbudowany i kosztowny system, to również większe nakłady przeznacza się na jego zabezpieczenie. Można też doprowadzić do sytuacji, w której zespół specjalistów od zabezpieczeń w jednym miejscu pracuje nad bezpieczeństwem bazy jako całości. Skutkuje to tym, że nie trzeba tych specjalistów wysyłać do każdej przychodni z osobna, aby tam zabezpieczyli lokalne komputery czy lokalne serwery. Duże, scentralizowane systemy gwarantują pewną wygodę, ale trzeba pamiętać, że takie rozwiązanie łączy się z dwoma rodzajami problemów.

Pierwszy dotyczy tego, że kiedy baza jest scentralizowana albo stworzony zostaje system z centralnym dostępem do wielu zasobów, to jednorazowe włamanie się do takiego zasobu oznacza możliwość dostępu do wszystkich danych tam zgromadzonych.

Drugi typ problemów, który zapewne będzie niemożliwy do wyeliminowania, to kopiowanie danych – przez lekarzy, pielęgniarki, położne czy też informatyków – na różnego rodzaju nośniki. Ponieważ dostęp do danych będzie możliwy z wielu źródeł, coraz częściej będziemy chcieli część tych danych zachować dla siebie, przynajmniej na jakiś czas, choćby po to, żeby je przejrzeć w przyszłości. Tutaj oczywiście pojawia się pytanie – jakie będą uprawnienia poszczególnych grup osób, czyli lekarzy, pielęgniarek, rejestratorek czy informatyków w szpitalu, do przetwarzania danych, które pochodzą z takich scentralizowanych systemów.

> Dobrze przygotowana polityka bezpieczeństwa informacji opisująca aktualny stan placówki medycznej jest pierwszym świadectwem dla GIODO, że ktoś panuje nad tym przedsiębiorstwem.

Takie uprawnienia personelu powinny być określone w polityce bezpieczeństwa. Mówi się, że gdy GIODO przeprowadza kontrolę ochrony danych osobowych, to pierwsze pytanie dotyczy właśnie opracowania tego dokumentu. Dlaczego jest on tak ważny?

To prawda, zaczynamy od kontroli dokumentacji. Polityka bezpieczeństwa jest ważna przede wszystkim dlatego, że pokazuje, czy w placówce medycznej zastanawiano się, jak zająć się bezpieczeństwem danych. To, czy ktoś ma opracowaną Politykę bezpieczeństwa, która opisuje aktualny stan instytucji i jej jednostek, a także osób tam pracujących i ich uprawnienia oraz stosowane systemy teleinformatyczne, jest dla GIODO pierwszym świadectwem, że dana placówka panuje nad kwestią ochrony danych. Świadectwem jedynie na papierze, ale już pokazującym, że w ogóle problem był rozważany. Oczywiście nie oznacza to, że jeżeli takiej polityki nie ma, to dane są niezabezpieczone. Ale jej brak oznacza dla nas jedno – że trzeba będzie sprawdzić wszystko, a więc każdą jednostkę w tej instytucji, i zobaczyć, co się w niej dzieje, ponieważ z dokumentacji to nie wynika.

Oczywiście fakt, że opracowano politykę bezpieczeństwa oraz instrukcję zarządzania systemem teleinformatycznym, nie przesądza, że dokumentacja ta jest kompletna i oddaje stan faktyczny oraz że uwzględniono w niej wszystkie niezbędne elementy.

Małe gabinety i indywidualne praktyki lekarskie, pielęgniarskie, dentystyczne zapewne zdecydują się na outsourcing i przekażą przetwarzanie tworzonych przez siebie danych medycznych firmom zewnętrznym. Na co muszą zwrócić uwagę?

Jestem w trudnej sytuacji, odpowiadając na to pytanie. Zdaję sobie bowiem sprawę z tego, że owe kilkadziesiąt tysięcy osób, które w różnej formie wykonują działalność w sektorze ochrony zdrowia, będzie musiało prowadzić dokumentację medyczną w postaci elektronicznej. To rzeczywiście ogromna grupa rozproszonych podmiotów. Ministerstwo Zdrowia uznało jednak, że sektor ten jest już wystarczająco dojrzały do takiej zmiany. Ja muszę tę decyzję uszanować.

Niemniej, moim zdaniem, outsourcing w tym sektorze to poważny problem. Jako generalny inspektor ochrony danych osobowych stoję bowiem na stanowisku, że nie jest on odpowiednio uregulowany. Przepisy w tym zakresie stworzono np. w sektorze bankowym czy telekomunikacyjnym. O ich opracowanie dla sektora ochrony zdrowia dopominamy się już od dłuższego czasu. Z taką sugestią wystąpiliśmy do Ministerstwa Zdrowia w sierpniu 2011 r. Jest to ważne choćby z tego powodu, że te tysiące lekarzy będzie przekazywało dane medyczne do przechowywania w wyspecjalizowanych podmiotach. To jest, oczywiście, dobre rozwiązanie, trzeba jednak pamiętać, że dane medyczne różnią się od przeciętnych danych składowanych na serwerach firm outsorcingowych. Biorąc zaś pod uwagę to, że zawsze może pojawić się jakiś problem techniczny, np. niedziałający *software* albo kłopoty z uruchomieniem się bazy danych, powstaje pytanie, kto będzie ponosił za to odpowiedzialność. Mogę odpowiedzieć wprost, że tę odpowiedzialność będzie ponosił wyłącznie lekarz. Umowa outsourcingu nie zdejmuje z lekarza odpowiedzialności za to, w jaki sposób dane są przetwarzane. Każdy błąd, który nastąpi w systemie, będzie błędem lekarza. To, że będzie miał on prawo regresu wobec informatyka zajmującego się składowaniem jego danych, będzie tak naprawdę wtórne. Bez wyraźnego wskazania na to, jakiego rodzaju standardy muszą być spełnione przy przetwarzaniu danych medycznych, myślę, że sobie nie poradzimy. Zdziwiło mnie więc stanowisko ministra zdrowia, który uznał, że sprawa ta nie wymaga regulacji. Według mnie wymaga.

Jakiej rady udzieliłby Pan pracownikom ochrony zdrowia prowadzącym własne gabinety, decydującym się na powierzenie przetwarzania danych medycznych firmom zewnętrznym?

Z pewnością muszą zwrócić uwagę na bezpieczeństwo samego systemu, do którego przenoszą dane – na jego dostępność, a także to, jakimi drogami ta dostępność będzie realizowana. Muszą samodzielnie ocenić, czy zalogowanie do systemu będzie bezpieczne. Patrząc na dzisiejszy rozwój technologii, zdajemy sobie sprawę z tego, że zapewne będą to systemy, które będą umożliwiały połączenie z różnych urządzeń, nie tylko komputera stacjonarnego w gabinecie, ale też z prywatnego laptopa, smartfona czy tabletu itd. Wiemy, że zalogowanie się z każdego z tych urządzeń wygląda trochę inaczej, co od razu sugeruje, żeby nie utrudniać tego procesu za bardzo. Im natomiast słabszy mechanizm logowania się do systemu, tym łatwiej można go przełamać i albo dokonać złośliwej zmiany danych, albo te dane po prostu wykraść.

GIODO: Wystąpiliśmy do Ministerstwa Zdrowia z sugestią, żeby przygotować przepisy dotyczące outsourcingu danych medycznych i rozwiązać pewne problemy, które już widzimy.

Bardzo istotną sprawą jest również to, co może zrobić hoster, czyli podmiot przechowujący dane. Oczywiste jest, że będzie on składował nie tylko dane, ale także bazy danych, w których te dane będą tworzone. Będzie też przechowywał *software*, za pomocą którego będą one obrabiane. Natomiast wszystkie przypadki, w których te dane będą mieszane z danymi innego lekarza, są niewskazane. Mogą być jednak pożądane, co może nastąpić na przykład w odniesieniu do spółdzielni lekarskiej, w której lekarze razem przekazują dane do tego samego outsourcera. Istnieje jednak pytanie, komu z pozostałych lekarzy te dane będą mogły być udostępniane i jak to się ma do tajemnicy lekarskiej. ■

Ale kwestia tajemnicy lekarskiej to już temat na osobną rozmowę.

Dziękuję za rozmowę.
Rozmawiał: Mariusz Jendra