Fot. J. Persa

Czasem muszę chować głowę w piasek

Z dr. praw Wojciechem Rafałem Wiewiórowskim, Generalnym Inspektorem Ochrony Danych Osobowych, rozmawia Krzysztof Nyczaj.

Czy dane medyczne polskich pacjentów są dobrze chronione?

– Eufemistycznie mówiąc: są różne problemy. Zależy, o jakich podmiotach leczniczych mówimy, czy dane medyczne przetwarzane są w ich systemach teleinformatycznych, czy mają postać papierową, czy mówimy o receptach, czy o dokumentacji medycznej.

Można zaobserwować prawidłowość: im większy stopień informatyzacji, tym mniej kłopotów z ochroną danych. To zresztą logiczne. Większość twórców systemów informatycznych przetwarzających dane medyczne zdaje sobie sprawę, że te systemy muszą sprostać wysokim wymaganiom stawianym nie tylko przepisami prawa, ale także regulacjami o charakterze normalizacyjnym. Duże, rozbudowane systemy teleinformatyczne cechują się więc najczęściej wysokim poziomem zabezpieczeń, z czym w przypadku danych przechowywanych w formie papierowej, np. u indywidualnego lekarza, bywa znacznie gorzej. Jeszcze gorzej jest z dokumentacją, którą sami przechowujemy – najłatwiej ją zgubić. W przypadku osobowych danych medycznych problemem jest nie tylko ich wyciek czy udostępnienie osobie nieuprawnionej, ale również ustalenie kręgu osób, które powinny mieć do nich dostęp.

Ogromnym problemem jest fakt „nachodzenia na siebie” przepisów o ochronie danych osobowych oraz przepisów o tajemnicy lekarskiej czy aptekarskiej. A tajemnica lekarska to również tajemnica lekarza w stosunku do innego lekarza. Nie każdy lekarz w Polsce powinien mieć dostęp do wszystkich danych każdego pacjenta. Odpowiedź na pytanie: jak zorganizować dostęp do danych medycznych, aby nie naruszyć przepisów o tajemnicy lekarskiej to obecnie jedno z największych wyzwań w służbie zdrowia.

Formalnie, w zgodzie z przepisami o tajemnicy zawodowej, trzeba by zakazać dostępu do danych wszystkim osobom, które nie są lekarzami czy pielęgniarkami, np. pracują w sekretariacie, recepcji, obsługują systemy IT, zajmują się rozliczeniami czy statystyką medyczną. Ale w praktyce to niemożliwe…

– Nie jestem specjalistą od wszystkich tajemnic prawnie chronionych, których w Polsce jest ok. 70. O poruszonej kwestii mogę więc mówić z punktu widzenia prawa do ochrony danych osobowych. Otóż najistotniejsze znaczenie ma tu fakt, czy dana osoba została prawidłowo upoważniona do przetwarzania danych medycznych i czy dokładnie wie, jakiego rodzaju czynności może podejmować w zakresie ich przetwarzania, »

» a jakich nie. Dla mnie oczywiste jest, że udostępnianie tego typu informacji w konkretnej potrzebie, np. osobom, które serwisują sprzęt czy oprogramowanie, bywa nieuniknione, np. w przypadku serwisowania tomografu komputerowego, który przechowuje przecież dane pacjentów. Inny przykład to sytuacja, w której w związku z przetwarzaniem danych wielu pacjentów o identycznych nazwiskach, konieczne jest uporządkowanie bazy tak, by nie dochodziło do pomyłek. Oczywiście, informatyk, który problem ma usunąć, musi mieć dostęp do danych osobowych. Istotne jest tu jednak, by administrator danych, czyli zazwyczaj kierownik jednostki, w prawidłowy sposób upoważnił taką osobę do dostępu do danych medycznych, poinformował ją, jakie czynności może wykonywać na danych i by w odpowiedniej chwili odebrał jej te uprawnienia. Pamiętajmy też, że w zinformatyzowanym świecie czynności na danych coraz częściej dokonuje się on-line. Z punktu widzenia ochrony danych osobowych działania takie są dopuszczalne, jednak wymagają wdrożenia stosownych procedur, w tym nadania i cofnięcia upoważnień.

Wystarczające jest umieszczenie w umowie o pracę z osobą niebędącą lekarzem czy pielęgniarką zobowiązania do przestrzegania tajemnicy medycznej?

– To jedno z rozwiązań, przy czym przyznanie uprawnień dostępu do danych medycznych musi być ściśle związane z obowiązkami pracowniczymi. Znam jednak przypadek nadania upoważnień do przetwarzania danych osobowych osobom… sprzątającym w placówce medycznej, dyrekcja wyszła bowiem z założenia, że skoro mają one dostęp do wszelkich pomieszczeń, a co za tym idzie przechowywanej tam dokumentacji, to należy je formalnie upoważnić do takiego dostępu. Takie podejście jest oczywistą bzdurą.

Problemu, jaki sprawia właściwe zabezpieczenie dokumentacji medycznej, nie można rozwiązać poprzez nadanie wszystkim zatrudnionym uprawnienia do dostępu do niej. Zupełnie inny zakres dostępu do danych osobowych powinien mieć lekarz, pielęgniarka i położna, inny – osoba pracująca w sekretariacie, a jeszcze inny – pracownik ochrony. Nie wyobrażam sobie, by pracownik ochrony miał dostęp do takich danych, mimo że powinien mieć wiedzę, kto wchodzi do placówki lub korzysta z jej pomieszczeń. Powinien natomiast mieć uprawnienia dostępu do informacji, kto i jaką funkcję sprawuje w placówce, gdyż to może wpływać na obowiązki i prawa, np. prawo wejścia do magazynu z materiałami medycznymi i lekami.

A co z sytuacją, kiedy przetwarzanie danych medycznych realizowane jest w outsourcingu? Minister Zdrowia stoi na stanowisku, że outsourcing jest możliwy, a GIODO – że nie.

– My nie twierdzimy, że jest niemożliwy. Twierdzimy, że natura pewnych działań jest taka, że powinna istnieć możliwość ich wykonywania przez podmioty zewnętrzne. Nie mogą to jednak być działania dotykające *stricte* oceny stanu zdrowia pacjenta czy wprowadzania nowych danych medycznych, chyba że istnieje ku temu wyraźna podstawa prawna.

Jesteśmy poddawani szantażowi...

Nie wykonuję obowiązku, który na mnie spoczywa. Zgodnie z prawem powininem zakazać przetwarzania danych w rejestrach.

Problemem jest jednak brak podstaw prawnych do wielu czynności, które mogłyby być wykonywane w outsourcingu, jak np. działalność biobanków. Natomiast co do przekazywania danych medycznych na zewnątrz placówki w celu ich archiwizacji nie twierdzimy, że takie zdarzenia nie mają sensu. W wielu przypadkach dla bezpieczeństwa danych lepiej jest, aby były one składowane poza placówką opieki zdrowotnej. Jednak wówczas bardzo istotne jest zawarcie prawidłowej umowy powierzenia przetwarzania danych. Musi ona mieć formę pisemną, określać zakres i cel przetwarzania danych, zapewniając administratorowi kontrolę nad tym, w jaki sposób dane są przetwarzane.

Outsourcing przetwarzania danych medycznych, w związku z wejściem w życie w 2014 r. przepisów dotyczących prowadzenia dokumentacji medycznej w postaci elektronicznej, dla małych placówek może być sensownym rozwiązaniem, choćby ze względu na koszty. Jednak administratorzy w firmach informatycznych zajmujących się profesjonalnym przetwarzaniem danych też będą mieli dostęp do tych danych. Czy nie będzie to sprzeczne z prawem?

– Jeżeli outsourcing polega tylko na przechowywaniu danych medycznych poza placówką opieki zdrowotnej, czyli na klasycznym hostingu, a wszystkie czynności na danych dokonywane będą przez osoby z tej placówki, to nie ma problemu. Wystarczy dobrze skonstruowana umowa powierzenia przetwarzania danych. Tym bardziej że można zablokować dostęp do danych, np. poprzez ich szyfrowanie w jednostce. To bardzo bezpieczne rozwiązanie. Z kolei brak rozwiązań szyfrujących zwiększa prawdopodobieństwo, że osoby nieuprawnione będą wykorzystywały dane do innych celów, np. tworzenia profili pacjentów poprzez łączenie danych z jednostki A i B. Pamiętajmy, że najczęściej będziemy mieć do czynienia z firmami, które świadczą usługi outsourcingowe w sposób masowy, będą więc posiadać dostęp do danych z wielu placówek. Umowa powierzenia przetwarzania danych powinna więc wyraźnie stanowić, co może, a czego nie może robić firma zewnętrzna.

Zagadnieniem nurtującym środowisko medyczne jest możliwość zastrzegania przez pacjentów dostępu do swoich danych medycznych. Czy pacjenci mają prawo zastrzec dostęp do części swoich danych medycznych lekarzom, którzy formalnie się nimi opiekują, np. lekarzom poz lub pielęgniarkom środowiskowym?

– Moim zdaniem, generalnie z ustawy o ochronie danych osobowych możliwość tego typu wynika, chyba że istnieją przepisy szczególne, które to wykluczają, np. dotyczące chorób zakaźnych. Ustawa o ochronie danych osobowych stanowi zaś, że każdy ma prawo sprzeciwu wobec przetwarzania jego danych osobowych i odnosi się to także do danych medycznych. Prawdą jest natomiast to, że kiedy nie ma możliwości kontaktu z daną osobą, a ze względów medycznych jest to konieczne, ustawa o ochronie danych osobowych nie uniemożliwia zapoznania się przez każdego lekarza z danymi o jej stanie zdrowia.

Pan minister zwracał uwagę na konieczność prawnego uregulowania funkcjonowania wielu rejestrów medycznych. Czy ta sytuacja już się poprawiła?

– Około 90% rejestrów działa bez prawidłowej podstawy prawnej. Tak przynajmniej wynika z materiałów, które Ministerstwo Zdrowia przygotowało na potrzeby ustawy o systemie informacji w ochronie zdrowia. Dane te są przerażające. Od wejścia do Unii Europejskiej obowiązują nas

europejskie przepisy dotyczące ochrony danych osobowych, które wymagają, by przetwarzanie danych w rejestrach było uregulowane na gruncie ustawy.

Brak podstawy prawnej utrudnia działalność wielu podmiotom prowadzącym rejestry. Przykładem są rejestry nowotworów – o uregulowanie ich funkcjonowania toczymy bój od 2004 r., a kolejni Generalni Inspektorzy Ochrony Danych Osobowych zwracają się do kolejnych ministrów zdrowia o wprowadzenie podstaw prawnych działania tychże. Pragnę podkreślić, i nie boję się użyć tych słów, że jesteśmy poddawani szantażowi. Gdybyśmy chcieli postąpić tak, jak to jest wymagane przez ustawę o ochronie danych osobowych, to 1 stycznia 2004 r. powinniśmy zakazać przetwarzania danych w rejestrach nowotworowych, jako nie znajdujących podstaw prawnych w polskim prawie. Oczywiście, nie zrobiliśmy tego, gdyż byliśmy cały czas przekonywani przez Ministerstwo Zdrowia, że regulacja lada moment się pojawi. Ostatnia data, którą nam podano, to 1 stycznia 2012 r. Mamy maj, a regulacji znowu nie ma. A przecież wprowadzenie podstaw prawnych dla tych rejestrów umożliwiłoby m.in. automatyzację wymiany danych, np. z rejestrem PESEL, dzięki czemu rejestry nowotworowe mogłyby automatycznie badać tzw. przeżywalność pacjentów.

Czyli to dobra wola GIODO sprawiła, że rejestry nie zostały zamknięte?

– Raczej – chowanie głowy w piasek. Zdaję sobie jednak sprawę, że nie wykonuję obowiązku, który na mnie spoczywa, skoro zgodnie z prawem powinienem zakazać przetwarzania danych w tych rejestrach, i to natychmiast.

Ustawa o systemie informacji w ochronie zdrowia wprowadziła konieczność informowania osób, których dane są przetwarzane w rejestrach. Trudno jednak wyobrazić sobie sytuację, że administrator rejestru prowadzi stosowną korespondencję z kilkudziesięcioma tysiącami osób. To także olbrzymie wydatki. Czy Pan minister ma jakiś pomysł w tej sprawie?

– Nie mam. W trakcie prac legislacyjnych byliśmy zwolennikami innego rozwiązania, bardziej praktycznego, choć trudniejszego legislacyjnie, co mogłoby wydłużyć prace nad ustawą. Proponowaliśmy, by dane osobowe zawarte w rejestrach były przetwarzane z mocy prawa, a wówczas nie trzeba byłoby dopełniać obowiązku informacyjnego. Przeważyły względy polityczne, a przyjęte rozwiązania są efektem daleko idącego kompromisu z naszej strony. W obecnym kształcie ustawa jest dla nas akceptowalna. Nadal podtrzymujemy, że pewne zapisy są trudne do wykonania: konieczność dopełnienia obowiązku informacyjnego to tylko jeden z przykładów takich zapisów.

System Informacji Medycznej (SIM) stanowi jeden z centralnych systemów wprowadzonych przez tę ustawę. Mają być w nim gromadzone dane osobowe, jak imię i nazwisko, PESEL, jednostkowe dane medyczne. Jak interpretować pojęcie „jednostkowe dane medyczne"? Czy to informacja o zastosowanej procedurze medycznej bądź problemie zdrowotnym pacjenta, czy też – cała dokumentacja medyczna pacjenta?

– Biorąc pod uwagę definicję zawartą w tej ustawie, obawiam się, że jedyną prawidłową interpretacją jest ta druga. Jednostkowe dane medyczne to całość informacji medycznej dotyczącej konkretnej osoby, a więc całość dokumentacji medycznej.

I na podstawie tego przepisu CSIOZ może gromadzić dokumentację medyczną wszystkich pacjentów w Polsce?

– Obawiam się, że tak. Myślę nawet, że taki właśnie był zamiar. Jednak proszę zauważyć, że z przepisów ustawy nie wynika wcale przymus umieszczania informacji w systemie informacji medycznej.

CSIOZ twierdzi, że dane będą umieszczane za zgodą pacjenta…

– Jeśli miałoby się to odbywać za zgodą pacjenta, to nie bardzo wiem, w jaki sposób taka zgoda miałaby zostać udzielona. Proszę pamiętać, że zgoda musi być świadoma i dobrowolna. Pacjent nie może mieć poczucia zależności pomiędzy udzieleniem zgody a udzieleniem świadczenia zdrowotnego.

Wśród modułów SIM ma być moduł zleceń, gromadzący m.in. elektroniczne recepty. Czy zasadne jest archiwizowanie ich wszystkich w centralnym systemie danych? Czy nie powinny być zeń usuwane zaraz po ich zrealizowaniu? Wiele zawierać będzie przecież dane wrażliwe, np. informacje o przepisaniu leków psychotropowych. Czy chęć otrzymywania szczegółowych statystyk dotyczących gospodarki lekiem uprawnia do archiwizowania tak szczegółowych danych?

– Przetwarzanie danych wrażliwych należy określać pod kątem celów, które mają zostać zrealizowane. W każdym systemie, czy to teleinformatycznym, czy tradycyjnym, dane wrażliwe powinny być przechowywane tylko tak długo, jak to konieczne do zrealizowania celu, który wymagał ich przechowywania. Trudno mi jednak odpowiedzieć, czy we wszystkich przypadkach statystyk zdrowotnych odizolowanie danych medycznych od danych identyfikujących osobę jest możliwe.

Anonimizacja danych rozwiązałaby ten problem?

– Dane do celów statystycznych powinny być wykorzystywane w wersji zanonimizowanej. Jednak w przypadku niektórych danych medycznych, np. dotyczących genomu, może być z tym kłopot. Po prostu – od pewnego momentu pojawia się fizyczna niemożliwość anonimizacji i dane, które pozostaną w systemie, a dotyczą genomu, nawet po odłączeniu od osoby nie będą anonimowe, ponieważ kolejne zebrane dane będą w 100% odpowiadały wcześniejszym, więc łatwo będzie można zidentyfikować tę osobę. Nawet jeśli dane osobowe trwale oddzielimy od danych medycznych, to wystąpią sytuacje, gdy identyfikacja pacjenta będzie możliwa po samych danych medycznych. Przykładowo, jeżeli osoba była hospitalizowana w związku z chorobą rzadko występującą w danym szpitalu, to będzie ona zawsze możliwa do zidentyfikowania po danych medycznych, chociażby dlatego, że była jedynym pacjentem hospitalizowanym z tą chorobą. Nie należy więc fetyszyzować problemu anonimizacji danych, gdyż nie zawsze będzie to możliwe.

Ustawa o systemie informacji w ochronie zdrowia wprowadza również pojęcie systemu informacji w ochronie zdrowia (SIOZ), który ma się składać m.in. z SIM-u oraz rejestrów. SIOZ ma być także zarządzany przez CSIOZ. Czy to oznacza, że Centrum będzie zarządzało w sposób scentralizowany danymi medycznymi wszystkich pacjentów w Polsce?

– Oddzielmy pojęcie systemu informacyjnego od składowanej gdzieś bazy danych. To, że istnieje system informacji w ochronie zdrowia, a ośrodkiem zarządzającym jest CSIOZ, nie oznacza, że wszystkie bazy mają się znaleźć w systemie centralnym.

Z systemem informacyjnym mamy do czynienia wtedy, kiedy z danego miejsca możemy wydobyć informacje z innego miejsca. Taki system może być rozproszony. Ustawa o ochronie danych osobowych już w 1997 r. mówiła, co jest zbiorem danych osobowych, niezależnie od tego, czy jest on scentralizowany czy rozproszony.

System informacji w ochronie zdrowia opisany w ustawie niekoniecznie musi być systemem, który korzysta wyłącznie z baz znajdujących się w CSIOZ. Większość rejestrów będzie zlokalizowana w innych miejscach, natomiast będą połączone z systemem centralnym tak, że będzie można zajrzeć do nich z konkretnego »

» miejsca. W tym sensie będą częścią systemu informacji w ochronie zdrowia.

Zgodnie z ustawą, od połowy 2014 r. wszystkie podmioty lecznicze powinny prowadzić dokumentację medyczną wyłącznie w postaci elektronicznej. Dla placówek, zwłaszcza mniejszych, będzie to kosztowne przedsięwzięcie. Najtańsze byłoby więc wejście w rozwiązania typu cloud computing. Czy tzw. przetwarzanie danych medycznych w „chmurze" jest bezpieczne? Jaki rodzaj „chmury" dla placówek byłby Pana zdaniem odpowiedni?

– Nie da się odpowiedzieć w kilku zdaniach. Najpierw trzeba by przeanalizować koncepcję różnego rodzaju chmur. Zupełnie inaczej będzie to wyglądało w przypadku klasycznych chmur publicznych udostępnianych wszelkim podmiotom, inaczej w przypadku chmury prywatnej, zbliżonej do klasycznego hostingu. A pomiędzy tymi biegunami leżą wszystkie inne możliwe rozwiązania chmurowe, które mogą być mniej lub bardziej bezpieczne. Bardzo prosta jest natomiast zależność pomiędzy kosztami rozwiązania chmurowego a zakresem jego bezpieczeństwa. Im jest bezpieczniejsze, tym na pewno droższe. Jeżeli chcielibyśmy przechowywać dane osobowe, szczególnie wrażliwe, w chmurze publicznej, co wiąże się z możliwością ich przetwarzania gdzieś na świecie, bez precyzyjnego określenia lokalizacji centrów przetwarzania danych – to takie rozwiązanie niewątpliwie jest sprzeczne z zasadami ochrony danych osobowych. Co do tego nie mam żadnych wątpliwości, nie ma bowiem możliwości uzyskania zezwolenia na przekazanie danych do kraju trzeciego. Przy typowej umowie adhezyjnej na korzystanie z chmury publicznej zezwolenia GIODO więc by nie wydał. Ale nawet jeśli umowa zakładałaby, że dane będą przechowywane na terenie któregoś z państw UE, to pozostaje problem zapewnienia administratorowi danych, czyli kierownikowi placówki opieki zdrowotnej, możliwości kontroli sposobu przetwarzania danych. Część dostawców rozwiązań chmurowych umożliwia wprawdzie dokonywanie np. inspekcji on-line, ale oczywiście to też kosztuje. Tak więc, im bardziej umowa dotycząca przetwarzania danych będzie dostosowana specjalnie do naszych potrzeb, tym bardziej będzie to kosztowne.

Komisja Europejska skierowała niedawno do konsultacji projekt nowego Rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony danych. Jak duży wpływ będzie ono miało na kwestię ochrony danych medycznych?

– Spory. Wprowadza bowiem reguły ustanawiania przepisów krajowych związanych z przetwarzaniem danych dotyczących zdrowia nie tylko dla celów związanych z procesem leczenia konkretnej osoby, ale również dla celów związanych z medycyną pracy, medycyną prewencyjną, zarządzaniem opieką zdrowotną, ochroną epidemiologiczną, wreszcie koniecznością zapewnienia wysokich standardów jakości i bezpieczeństwa produktów leczniczych. Rozporządzenie definiuje również ramy umożliwiające przetwarzanie danych osobowych do celów dokumentacji, statystyki, badań naukowych, prowadzenia rejestrów pacjentów.

Ministerstwo Zdrowia proceduje tymczasem projekty rozporządzeń do tej ustawy. Czy GIODO zgodzi się na wykorzystywanie numeru PESEL jako identyfikatora lekarza?

– Każda sytuacja, w której PESEL jest wykorzystywany poza systemem administracji, a tym bardziej jako login czy hasło do jakiegokolwiek systemu – zawsze jest dla nas niepokojąca. Wielokrotnie kwestionowaliśmy wykorzystywanie numeru PESEL w celach komercyjnych, np. przy programach lojalnościowych. Dlaczego mielibyśmy się zgodzić na takie rozwiązanie w przypadku lekarzy? Wydaje się, że istnieje możliwość stworzenia innego identyfikatora niż numer PESEL dla celów identyfikacyjnych grup pracowników medycznych. Naszym zdaniem, PESEL jest w Polsce zbyt często stosowanym identyfikatorem wewnątrz baz administracyjnych. ■

Przetwarzanie danych medycznych poza placówką

Polemika GIODO z Ministrem Zdrowia

Pomiędzy Głównym Inspektorem Ochrony Danych Osobowych a Ministrem Zdrowia trwa spór dotyczący możliwości prawnego uregulowania zlecania przez placówki opieki zdrowotnej przetwarzania danych medycznych podmiotom wyspecjalizowanym w profesjonalnym ich przetwarzaniu. GIODO wezwał ministra do niezwłocznego podjęcia prac nad prawnym uregulowaniem tej kwestii – Minister Zdrowia stoi jednak na stanowisku, że istniejące ramy prawne są wystarczające. Na razie w sprawie mamy pat. Jakie są najważniejsze argumenty stron?

Zdaniem GIODO

W sierpniu 2011 r. GIODO wystąpił do MZ o podjęcie prac legislacyjnych mających na celu wprowadzenie podstaw prawnych dla zlecania informatycznej obsługi procesu przetwarzania danych osobowych przez administratorów przetwarzających dane osobowe pacjentów w związku z udzielaniem świadczeń zdrowotnych innym wyspecjalizowanym podmiotom. Wg GIODO, w obecnym stanie prawnym nie jest to dopuszczalne ze względu na istnienie tajemnicy zawodowej (art. 13 i 14 ustawy z 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta). GIODO zwrócił uwagę, że co do zasady ustawa o ochronie danych osobowych przewiduje możliwość powierzenia przetwarzania danych osobowych wyspecjalizowanym podmiotom, nie zawiera też zastrzeżeń co do możliwości powierzenia do przetwarzania także danych szczególnie chronionych. Jednak może to budzić wątpliwości w odniesieniu do informacji objętych zakresem ustawowych tajemnic wynikających z przepisów dotyczących wykonywania zawodów medycznych. Jeżeli bowiem ustawy szczególne przewidują dalej idącą ochronę, niż wynika to z ustawy o ochronie danych osobowych, stosuje się przepisy tych pierwszych.

GIODO podkreśla, że chociaż co do zasady powierzenie przetwarzania danych osobowych następuje bez konieczności uzyskiwania zgody osób, których danych dotyczą, to w razie związania tajemnicą zawodową – każdy przypadek posłużenia się podwykonawcą w związku z przetwarzaniem danych wymaga istnienia przepisu rangi ustawy, który na takie działanie wprost zezwala. Analogiczna relacja, zdaniem GIODO, zachodzi pomiędzy przepisami ustawy o ochronie danych osobowych a regulacjami sektorowymi uwzględniającymi szczególne zagrożenia dla sfery prywatności i wprowadzającymi tajemnice zawodowe, np. ustawą Prawo bankowe, ustawą o działalności ubezpieczeniowej, ustawą Prawo telekomunikacyjne. Na gruncie przepisów ustawowych – podkreśla GIODO –

przewidziano możliwość przekazywania danych niezbędnych do prowadzenia działalności bankowej, ubezpieczeniowej czy telekomunikacyjnej innym podmiotom przez podmioty prowadzące te działalności, jednocześnie rozciągnięto na podmioty współpracujące z nimi obowiązek zachowania ustawowej tajemnicy.

Ustawa o działalności leczniczej ani ustawa o systemie informacji w ochronie zdrowia nie przewidują podobnych rozwiązań – przypomina GIODO. Również żaden z przepisów ustawy o informatyzacji podmiotów realizujących zadania publiczne (np. spzozów) nie odnosi się bezpośrednio do informacji dotyczących pacjentów i objętych tajemnicą na podstawie przepisów szczególnych, chociaż dotyka kwestii technicznego udostępniania danych zgromadzonych w rejestrach, w tym m.in. w ewidencji świadczeń zdrowotnych w zozach.

Przepisy ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne nie stanowią, zdaniem GIODO, wyjątku od zasady przyjętej w art. 14 ust. 2 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta, zobowiązującej do zachowania w tajemnicy przez osoby wykonujące zawód medyczny i udzielające pacjentowi świadczeń zdrowotnych informacji z tym związanych, a uzyskanych w związku z wykonywaniem zawodu medycznego. GIODO podkreśla również, że prawidłowo skonstruowana podstawa prawna dla przekazywania danych pacjenta objętych tajemnicą zawodową powinna w sposób wyraźny określać krąg podmiotów uprawnionych do dostępu do informacji objętych tajemnicą, ponadto cel i zakres tego udostępnienia. Niezbędne jest również, zdaniem GIODO, wprowadzenie dodatkowego przepisu rozciągającego obowiązek zachowania powyższej tajemnicy na podmioty, którym informacje te będą powierzane. Tylko w taki sposób można bowiem zapewnić ochronę prywatności pacjentów i zachowania tajemnicy informacji uzyskiwanych w związku z wykonywaniem zawodu medycznego.

Minister Zdrowia odpowiada

Minister Zdrowia nie podzielił powyższego stanowiska. Stwierdził, że ustawa o ochronie danych osobowych stanowi wystarczającą podstawę prawną do zlecenia przetwarzania danych medycznych podmiotom zajmującym się ich profesjonalnym przetwarzaniem. Podmiot przetwarzający dane na podstawie umowy powierzenia zawartej z administratorem danych nie staje się ich administratorem, a do powierzenia przetwarzania danych osobowych przez ich administratora nie jest wymagana zgoda osoby, której dotyczą.

Minister przywołując przepisy ustawy o ochronie danych osobowych stwierdził, że umowa o powierzenie przetwarzania danych osobowych określa szczegółowo zakres i cel ich przetwarzania. Zdaniem MZ, obostrzenia dotyczące technicznego zabezpieczenia danych zawarte w ustawie o ochronie danych osobowych są więc wystarczające. Niewłaściwe natomiast jest powoływanie się GIODO na przykłady z prawa bankowego i innych ustaw. Według prawa bankowego dane są udostępniane, np. w celu sprawdzenia zdolności kredytowej klienta. Powierzenie przetwarzania danych osobowych pacjentów przez podmioty udzielające świadczeń zdrowotnych dotyczy natomiast jedynie przechowywania dokumentacji medycznej sporządzonej w postaci elektronicznej. Podmiot, który przetwarzanie danych powierza, nie udostępnia ich – podkreśla MZ.

GIODO podtrzymuje…

W grudniu 2011 r. GIODO stanowczo odrzucił tę argumentację Ministra Zdrowia, która jego zdaniem pomija rzeczywiste źródła problemu oraz wskazuje na niezrozumienie argumentów natury prawnej: znaczenie wzajemnego stosunku przepisów o ochronie danych osobowych i ustaw względem niej szczególnych, które należy oceniać na gruncie art. 5 ustawy o ochronie danych osobowych. (Stanowi on, iż jeżeli przepisy odrębnych ustaw odnoszących się do przetwarzania danych przewidują dalej idącą ochronę, niż ta ustawa, stosuje się przepisy tychże ustaw). W razie związania tajemnicą zawodową – podkreśla ponownie GIODO – każdy przypadek posłużenia się podwykonawcą w związku z przetwarzaniem danych wymaga istnienia przepisów rangi ustawy, które na takie działanie wprost zezwalają. Skoro zaś przepisy zapewniające informacjom dalej idącą ochronę wyłączają stosowanie przepisów ustawy o ochronie danych osobowych, to błędem jest powoływanie się na jej art. 31 traktujący o możliwości powierzenia przetwarzania danych innemu podmiotowi.

GIODO podkreślił również, że problem powierzenia przetwarzania danych osobowych dotyczy w wielu przypadkach przetwarzania danych związanych z obsługą procesu przetwarzania danych w systemach informatycznych czy specjalistycznego sprzętu diagnostycznego rejestrującego dane osobowe na rzecz podmiotów świadczących usługi zdrowotne. I może tu chodzić o różne operacje na danych (zbieranie, utrwalenie, przechowywanie, opracowywanie, zmienianie i usuwanie), nie zaś, jak wskazuje Minister Zdrowia, jedynie przechowywanie dokumentacji medycznej. GIODO ponownie zwrócił uwagę, że obecnie obowiązujące przepisy dotyczące przechowywania dokumentacji medycznej nie odnoszą się do kwestii możliwości delegowania powyższych zadań na inne podmioty.

Rada dla placówek opieki zdrowotnej

W świetle tej polemiki – placówki opieki zdrowotnej powinny przyjąć stanowisko „ostrożnościowe". GIODO jest wszak głównym organem w kwestii ochrony danych osobowych. Jego instytucjonalizacja i zakres kompetencji, określone w ustawie o ochronie danych osobowych, wynikają wprost z art. 28 Dyrektywy 95/46/WE Parlamentu Europejskiego i Rady WE z 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych.

Jak zatem zorganizować gromadzenie osobowych danych medycznych poza placówką opieki zdrowotnej, aby mogły one stracić status medycznych danych osobowych, a tym samym – przestały podlegać reżimowi tajemnicy lekarskiej?

Można tego dokonać poprzez anonimizację, pseudonimizację lub separację danych.

Anonimizacja to takie przekształcenie danych osobowych, po którym nie można już przyporządkować poszczególnych informacji osobistych lub rzeczowych do określonej lub możliwej do zidentyfikowania osoby fizycznej albo można tego dokonać jedynie niewspółmiernie dużym nakładem czasu, kosztów i sił. Przez pseudonimizację należy rozumieć proces, w którym dane osobowe zostają usunięte z rekordu danych i zastąpione przez „pseudonim", przy czym pseudonim pozwala powrócić do zapisu danych źródłowych. Separacja danych z kolei polega na podzieleniu danych na dwie części: odseparowaniu danych wrażliwych od pozostałych. Związek pomiędzy odseparowaną częścią identyfikacyjną a pozostałą częścią danych realizowany jest przy pomocy pseudonimów.

Sposobem zapewnienia przestrzegania tajemnicy lekarskiej w przypadku outsourcingu przetwarzania danych medycznych może być również szyfrowanie danych składowanych w zewnętrznym archiwum. Szyfrowanie odbywa się na terenie placówki opieki zdrowotnej przy wykorzystaniu certyfikatów niekwalifikowanych. Odczyt danych jest wtedy możliwy przez personel medyczny placówki. Administrator IT z firmy zewnętrznej obsługującej archiwum elektroniczne widzi jedynie nic nie mówiący ciąg znaków. ■